Object Storage Service

API Reference (Kuala Lumpur Region)

Issue 01

Date 2022-08-16

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

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

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

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process.* For details about this process, visit the following web page:
https://www.huawei.com/en/psirt/vul-response-process
For vulnerability information, enterprise customers can visit the following web page:
https://securitybulletin.huawei.com/enterprise/en/security-advisory

Contents

1 Before You Start

1.1 Overview

Welcome to the *Object Storage Service API Reference*. Object Storage Service (OBS) provides massive, secure, reliable, and cost-effective data storage capabilities for users to store data of any type and size. It is suitable for scenarios such as enterprise backup/archiving, video on demand (VoD), and video surveillance.

This document describes how to use application programming interfaces (APIs) to perform operations on OBS, such as creating, modifying, and deleting bucket, as well as uploading, downloading, and deleting objects. For details about all supported operations, see **API Overview**.

Before calling OBS APIs, ensure that you have fully understood relevant concepts. For details, see **Basic Concepts**.

1.2 API Calling

OBS provides Representational State Transfer (REST) APIs, allowing you to use HTTP or HTTPS requests to call them. For details, see **Calling APIs**.

1.3 Endpoints

An endpoint is the **request address** for calling an API. Endpoints vary depending on services and regions.

Table 1-1 OBS endpoints

Region Name	Region	Endpoint	Protocol
AP-Kuala Lumpur-OP6	my-kualalumpur-1	obs.my-kualalumpur-1.alphaedge.tmone.com.my	HTTPS/HTTP

OBS provides a second-level domain name for each region. You can use the domain name provided by OBS or a custom domain name to access OBS.

1.4 Basic Concepts

Basic Concepts Related to OBS APIs

- Domain

  You can register a domain with the cloud service. The domain has full access permissions for all the resources and cloud services that are subscribed under it. The domain can also reset user passwords and grant permissions to users. A domain is a payment entity. To keep the domain secure, it is recommended that you create users under the domain to perform routine management operations.

- User

  A user is created using a domain on Identity and Access Management (IAM) to use cloud services. Each IAM user has its own identity credentials (password and access keys).

  On the **My Credentials** page on the console, you can view the domain ID and user ID, you can also manage the access keys of the domain and IAM users.

  Access keys of the domain and its IAM users are required for authentication when calling APIs.

- Bucket

  A bucket is a container where objects are stored. It is the top namespace in OBS. Each object must reside in a bucket. For example, if the object named **picture.jpg** is stored in the **photo** bucket, you can use the following URL to access the object: **http://photo.obs.*region*.*example*.com/picture.jpg**.

- Objects

  An object is a basic data unit on OBS. A bucket can store multiple objects, and OBS does not distinguish between object types. Objects are serialized in OBS. An object may be a text, a video, or any other types of files. In OBS, the size of a file can range from 0 bytes to 48.8 TB. However, when an object is uploaded through the **PutObject** operation, it cannot exceed the maximum size of 5 GB. Use the multipart upload method, if the object size is larger than 5 GB.

- Region

  A region is a geographic area in which cloud resources are deployed. Availability zones (AZs) in the same region can communicate with each other over an intranet, while AZs in different regions are isolated from each other. Deploying cloud resources in different regions can better suit certain user requirements or comply with local laws or regulations.

  Each bucket in OBS must reside in a region. You can specify the region when creating the bucket. Once a bucket is created, its region cannot be changed. Select the most appropriate region for a bucket based on the location, cost, and regulatory compliance requirements. For details about regions, see **Endpoints**.

- AZ

An AZ comprises of one or more physical data centers equipped with independent ventilation, fire, water, and electricity facilities. Computing, network, storage, and other resources in an AZ are logically divided into multiple clusters. AZs within a region are interconnected using high-speed optical fibers to allow you to build cross-AZ high-availability systems.

2 API Overview

API Operations on Buckets

Table 2-1 API operations on buckets

Operation	Description
Listing Buckets	Queries the list of buckets created by the user.
Creating a Bucket	Creates a bucket. You can add different request headers to specify the region, storage class, and permission control policy.
Listing Objects in a Bucket	Lists objects in a bucket. You can add different request headers to obtain objects that match the specified prefix, identifier, and other requirements.
Obtaining Bucket Metadata	Checks whether the bucket metadata exists. You can query the information about the bucket region, storage class, OBS version number, enterprise project ID, and CORS configuration.
Obtaining Bucket Location	Obtains the bucket region information.
Deleting Buckets	Deletes a specified bucket. Before deleting a bucket, ensure that the bucket is empty.

API Operations on Advanced Bucket Settings

Table 2-2 API operations on advanced bucket settings

Operation	Description
Configuring a Bucket Policy	Creates or modifies a bucket policy. If the specified bucket already has a policy, the policy in the request will overwrite the existing one.
Obtaining Bucket Policy Information	Obtains the policy information of a specified bucket.
Deleting a Bucket Policy	Deletes the policy of a specified bucket.
Configuring a Bucket ACL	Configures the ACL of a specified bucket. You can control the read and write permissions of a bucket through ACL settings.
Obtaining Bucket ACL Information	Obtains the ACL information of a specified bucket.
Configuring Logging for a Bucket	Enables or disables the log management function of a bucket. When this function is enabled, a log record is generated for each operation on a bucket. Multiple log records are packed into a log file, which will be saved in a specified location.
Obtaining a Bucket Logging Configuration	Obtains the logging configuration of the current bucket.
Configuring Bucket Lifecycle Rules	Configures rules to automatically delete or migrate objects in a bucket.
Obtaining Bucket Lifecycle Configuration	Obtains the lifecycle rules configured for a specified bucket.
Deleting Lifecycle Rules	Deletes the lifecycle configuration of a bucket.
Configuring Versioning for a Bucket	Enables or disables versioning for a bucket. When this function is enabled, objects of different versions can be retrieved and restored, and data can be quickly restored in case of accidental operations or application faults.
Obtaining Bucket Versioning Status	Obtains the versioning status of a specified bucket.
Configuring Event Notification for a Bucket	Configures the event notification for a bucket to ensure that the bucket owner is notified about events occur on the bucket in a secure and timely manner.

Operation	Description
Obtaining the Event Notification Configuration of a Bucket	Obtains the notification configuration of a bucket.
Configuring Storage Class for a Bucket	Creates or updates the default storage class configuration of a bucket.
Obtaining Bucket Storage Class Information	Obtains the default storage class configuration of a bucket.
Configuring Tags for a Bucket	Adds a tag to an existing bucket. After tags are added to a bucket, all service detail records (SDRs) generated by the requests for this bucket will have the same tags. You can categorize the SDRs for detailed cost analysis.
Obtaining Bucket Tags	Obtains the tags of a specified bucket.
Deleting Tags	Deletes the tags of a specified bucket.
Configuring Bucket Storage Quota	Sets the bucket space quota to limit the maximum storage capacity of the bucket.
Querying Bucket Storage Quota	Obtains the bucket space quota.
Obtaining Storage Information of a Bucket	Obtains the number of objects in a bucket and the space occupied by the objects.
Configuring a Custom Domain Name for a Bucket	Configures a custom domain name for a bucket. Once a user-defined domain name is successfully configured, the bucket can be accessed through the user-defined domain name.
Obtaining the Custom Domain Name of a Bucket	Queries the custom domain name of a bucket.
Deleting the Custom Domain Name of a Bucket	Deletes the custom domain name of a bucket.
Configuring Bucket Encryption	Creates or updates the default server-side encryption configuration for a bucket. After encryption is enabled for a bucket, objects uploaded to the bucket are encrypted with the encryption configuration the bucket.
Obtaining Bucket Encryption Configuration	Queries the default server-side encryption configuration of a bucket.
Deleting the Encryption Configuration of a Bucket	Deletes the default server-side encryption configuration of a bucket.

API Operations for Static Website Hosting

Table 2-3 API Operations for Static Website Hosting

Operation	Description
Configuring Static Website Hosting for a Bucket	Creates or updates the website hosting configuration of a bucket. OBS allows you to store static web page resources such as HTML web pages, flash files, videos, and audios in a bucket. When a client accesses these resources from the website endpoint of the bucket, the browser can directly resolve and present the resources to the client.
Obtaining the Static Website Hosting Configuration of a Bucket	Obtains the website hosting configuration of a bucket.
Deleting the Static Website Hosting Configuration of a Bucket	Deletes the website hosting configuration of a bucket.
Configuring Bucket CORS	Configures the cross-origin resource sharing (CORS) configuration of a bucket. OBS allows static web page resources to be stored in buckets. The buckets can be used as website resources. A website hosted by OBS can respond to cross-domain requests from another website only after the CORS rule is configured.
Obtaining the CORS Configuration of a Bucket	Obtains the CORS configuration of a bucket.
Deleting the CORS Configuration of a Bucket	Deletes the CORS configuration of a bucket.
OPTIONS Bucket	Checks whether the client has the permission to perform operations on the server. It is usually performed before the cross-domain access.
OPTIONS Object	Checks whether the client has the permission to perform operations on the server. It is usually performed before the cross-domain access.

API Operations on Objects

Table 2-4 API operations on objects

Operation	Description
Uploading an Object - PUT	Uploads an object to a specified bucket.
Uploading an Object - POST	Uploads an object to a specified bucket based on tables.
Copying an Object	Creates a copy for an existing object in OBS.
Downloading an Object	Downloads an object.
Querying Object Metadata	Obtains the object metadata. Information such as object expiration time, version number, and CORS configuration is the object metadata.
Deleting an Object	Deletes a specified object. You can also carry the versionId field to delete the specified object version.
Deleting Objects	Deletes a batch of objects from a bucket permanently. Objects deleted in this way cannot be recovered.
Restoring Cold Objects	Restores objects in the Cold storage class. You can download these objects only after they are restored.
Appending an Object	Appends data to an object in a specified bucket. If no object with the same key value exists in the bucket, a new object will be created.
Configuring an Object ACL	Configures the ACL of a specified object. You can control the read and write permissions of objects through ACL settings.
Obtaining Object ACL Configuration	Obtains the ACL configuration of a specified object.
Modifying Object Metadata	Adds, modifies, or deletes metadata of uploaded objects.
Modifying an Object	Modifies the content of an object in a specified parallel file system from the specified location.
Truncating an Object	Truncates an object in a specified parallel file system to the specified size.
Renaming an Object	Renames an object in a specified parallel file system.

API Operations for Multipart Tasks

Table 2-5 API operations for multipart tasks

Operation	Description
Listing Initiated Multipart Uploads in a Bucket	Queries all the multipart upload tasks that have not been merged or canceled in a bucket.
Initiating a Multipart Upload	Initiates a multipart upload task, and obtains the globally unique multipart upload task ID for subsequent operations, such as uploading, merging, and listing parts.
Uploading Parts	Uploads parts for a specific multipart task.
Copying Parts	Copies an object or a part of the object as a part of a multipart task.
Listing Uploaded Parts	Queries information about all parts of a multipart task.
Completing a Multipart Upload	Merges the specified parts into a complete object.
Canceling a Multipart Upload Task	Cancels a multipart upload task.

3 Calling APIs

3.1 Constructing a Request

This section describes the structure of a REST API request.

Request URI

OBS uses URI to locate specific buckets, objects, and their parameters. Use URIs when you want to operate resources.

The following provides a common URI format. The parameters in square brackets [ ] are optional.

protocol://[bucket.]domain[:port][/object][?param]

Table 3-1 URI parameters

Parameter	Description	Mandatory
protocol	Protocol used for sending requests, which can be either HTTP or HTTPS. HTTPS is a protocol that ensures secure access to resources.	Yes
bucket	Resource path of a bucket, identifying only one bucket in OBS	No
domain	Domain name or IP address of the server for saving resources	Yes
port	Port enabled for protocols used for sending requests. The value varies with software server deployment. If no port number is specified, the protocol uses the default value. Each transmission protocol has its default port number. In OBS, the default HTTP port number is **80** and that of HTTPS is **443**.	No
object	An object path used in the request	No

Parameter	Description	Mandatory
param	A specific resource contained by a bucket or object. Default value of this parameter indicates that the bucket or object itself is obtained.	No

NOTICE

All API requests except those for the bucket list must contain the bucket name. Based on the DNS resolution performance and reliability, OBS requires that the bucket name must be placed in front of the **domain** when a request carrying a bucket name is constructed to form a third-level domain name, also mentioned as virtual hosting access domain name.

For example, you have a bucket named **test-bucket** in the **a1** region, and you want to access the ACL of an object named **test-object** in the bucket. The correct URL is **https://test-bucket.obs.a1.example.com/test-object?acl**.

Request Method

HTTP methods, which are also called operations or actions, specify the type of operations that you are requesting.

Table 3-2 HTTP request methods supported by the OBS

Method	Description
GET	Requests the server to return a specific resource, for example, a bucket list or object.
PUT	Requests the server to update a specific resource, for example, creating a bucket or uploading an object.
POST	Requests the server to add a resource or perform a special operation, for example, part uploading or merging.
DELETE	Requests the server to delete specified resources, for example, an object.
HEAD	Requests the server to return the digest of a specific resource, for example, object metadata.
OPTIONS	The request server checks whether the user has the operation permission for a resource. The CORS needs to be configured for the bucket.

Request Headers

Refers to optional and additional request fields, for example a field required by a specific URI or HTTP method. For details about the fields of common request headers, see **Table 3-3**.

Table 3-3 Common request headers

Header	Description	Mandatory
Authorization	Signature information contained in a request message Type: string No default value. Conditional: optional for anonymous requests and required for other requests.	Conditionally required
Content-Length	The message length (excluding headers) defined in RFC 2616 Type: string No default value. Conditional: optional for PUT requests, but mandatory for the requests that load XML content	Conditionally required
Content-Type	The content type of the requested resource, for example, **text/plain** Type: string No default value.	No
Date	Time when a request is initiated, for example, **Wed, 27 Jun 2018 13:39:15 +0000**. Type: string No default value. Conditional: optional for anonymous requests or those requests containing header **x-obs-date**, required for other requests.	Conditionally required
Host	The host address, for example, *bucketname*.**obs.***region*.**example.com**. Type: string No default value.	Yes

(Optional) Request Body

A request body is generally sent in a structured format (for example, JSON or XML). It corresponds to **Content-Type** in the request header and is used to transfer content other than the request header. If the request body contains full-width characters, these characters must be coded using UTF-8.

The request body varies according to the APIs. Certain APIs do not require the request body, such as the GET and DELETE APIs.

Sending a Request

There are two methods to initiate requests based on the constructed request messages:

- cURL

  cURL is a command-line tool used to perform URL operations and transmit information. cURL acts as an HTTP client that can send HTTP requests to the server and receive response messages. cURL is applicable to API debugging. For more information about cURL, visit **https://curl.haxx.se/**. cURL cannot calculate signatures. When cURL is used, only anonymous public OBS resources can be accessed.

- Coding

  You can use code to make API calls, and to assemble, send, and process request messages.

3.2 Authentication

3.2.1 User Signature Authentication

OBS signs a request using AK/SK. When a client is sending a request to OBS, the message header must contain the SK, request time, request type, and other information of the signature.

- AK: access key ID, which is a unique identifier associated with a secret access key (SK). The AK and SK are used together to obtain an encrypted signature for a request. Format example: **HCY8BGCN1YM5ZWYOK1MH**
- SK: secret access key, which is used together with the AK to sign requests, identify a request sender, and prevent the request from being modified. Format example: **9zYwf1uabSQY0JTnFqbUqG7vcfqYBaTdXde2GUcq**

A user can obtain the AK and SK from IAM. For details, see **Obtaining Access Keys (AK/SK)**.

OBS provides three signature calculation methods based on application scenarios: **Authentication of Signature in a Header**, **Authentication of Signature in a URL**, and **Authentication of Signature Carried in the Table Uploaded Through a Browser**.

Table 3-4 shows the user signature verification process in which a signature is carried in a header. For details about the parameters and code examples of authentication of signature in a header, see **Authentication of Signature in a Header**.

Table 3-4 Signature calculation and verification procedure

Procedure		Example
Signature calculation	1. Construct an HTTP message.	PUT /object HTTP/1.1 Host: bucket.obs.region.example.com Date: Tue, 04 Jun 2019 06:54:59 GMT Content-Type: text/plain Content-Length: 5913
	2. Calculate **StringToSign** based on the signature rule.	StringToSign = HTTP-Verb + "\n" + Content-MD5 + "\n" + Content-Type + "\n" + Date + "\n" + CanonicalizedHeaders + CanonicalizedResource
	3. Prepare the AK and SK.	AK: ****** SK: ******
	4. Calculate **Signature**.	Signature = Base64(HMAC-SHA1(**SecretAccessKeyID**, UTF-8-Encoding-Of(**StringToSign**)))
	5. Add a signature header and send the request to OBS.	PUT /object HTTP/1.1 Host: bucket.obs.region.example.com Date: Tue, 04 Jun 2019 06:54:59 GMT Content-Type: text/plain Content-Length: 5913 Authorization: OBS **AccessKeyID**:**Signature**
Signature authentication	6. Receive the HTTP message.	PUT /object HTTP/1.1 Host: bucket.obs.region.example.com Date: Tue, 04 Jun 2019 06:54:59 GMT Content-Type: text/plain Content-Length: 5913 Authorization: OBS **AccessKeyID**:**Signature**
	7. Obtain the SK based on the AK in the request.	Obtain the AK from the authorization header and obtain the SK of the user from IAM.
	8. Calculate **StringToSign** based on the signature rule.	StringToSign = HTTP-Verb + "\n" + Content-MD5 + "\n" + Content-Type + "\n" + Date + "\n" + CanonicalizedHeaders + CanonicalizedResource
	9. Calculate **Signature**.	Signature = Base64(HMAC-SHA1(**SecretAccessKeyID**, UTF-8-Encoding-Of(**StringToSign**)))

Procedure		Example
	10. Authenticate the signature.	Verify that the value of **Signature** in the authorization header is the same as the value of **Signature** calculated by the server. If the two values are the same, the signature verification is successful. If the two values are different, the signature verification fails.

3.2.2 Authentication of Signature in a Header

For all API operations, the most common identity authentication is to carry signatures in headers.

In the header, the signature is carried in the authorization header field of the HTTP message. The format of the message header is as follows:

```
Authorization: OBS AccessKeyID:signature
```

The signature calculation process is as follows:

1. Construct the request character string (StringToSign).

2. Perform UTF-8 encoding on the result obtained from the preceding step.

3. Use the SK to perform the HMAC-SHA1 signature calculation on the result obtained from step 2.

4. Perform Base64 encoding on the result of step 3 to obtain the signature.

The StringToSign is constructed according to the following rules. **Table 3-5** describes the parameters.

```
StringToSign =
   HTTP-Verb + "\n" +
   Content-MD5 + "\n" +
   Content-Type + "\n" +
   Date + "\n" +
   CanonicalizedHeaders + CanonicalizedResource
```

Table 3-5 Parameters required for constructing a StringToSign

Parameter	Description
HTTP-Verb	Indicates an HTTP request method supported by the OBS REST API. The value can be an HTTP verb such as **PUT**, **GET**, or **DELETE**.
Content-MD5	Base64-encoded 128-bit MD5 digest of the message according to RFC 1864. This parameter can be empty. For details, see **Table 3-10** and the algorithm examples below the table.

Parameter	Description
Content-Type	Specifies the message type, for example, **text/plain**. If a request does not contain this header field, this parameter is deemed as an empty string. For details, see **Table 3-6**.
Date	Time when a request is initiated. This parameter uses the RFC 1123 time format. If the deviation between the time specified by this parameter and the server time is over 15 minutes, the server returns error 403. This parameter is an empty string when the **x-obs-date** is specified. For details, see **Table 3-10**. If an operation (for example, obtaining an object content) is temporarily authorized, this parameter is not required.
CanonicalizedHeaders	OBS request header field in an HTTP request header, referring to header fields starting with **x-obs-**, such as, **x-obs-date**, **x-obs-acl**, and **x-obs-meta-***. When calling an API, choose a header that is supported by the API as required. 1. All characters of keywords in a request header field must be converted to lowercase letters (content values must be case sensitive, for example, **x-obs-storage-class:STANDARD**). If a request contains multiple header fields, these fields should be organized by keyword in the alphabetical order from a to z. 2. If multiple header fields in a request have the same prefix, combine the header fields into one. For example, **x-obs-meta-name:name1** and **x-obs-meta-name:name2** should be reorganized into **x-obs-meta-name:name1,name2**. Use comma to separate the values. 3. Keywords in the request header field cannot contain non-ASCII or unrecognizable characters, which are also not advisable for values in the request header field. If the two types of characters are necessary, they should be encoded and decoded on the client side. Either URL encoding or Base64 encoding is acceptable, but the server does not perform decoding. 4. Delete meaningless spaces and tabs in a header field. For example, **x-obs-meta-name: name** (with a meaningless space before **name**) must be changed to **x-obs-meta-name:name**. 5. Each header field occupies a separate line. See **Table 3-8**.

Parameter	Description
CanonicalizedResource	Indicates the OBS resource specified by an HTTP request. This parameter is constructed as follows: <Bucket name + Object name> + [Subresource 1] + [Subresource 2] + ... 1. Bucket name and object name, for example, ***/bucket/object***. If no object name is specified, for example, ***/bucket/***, the entire bucket is listed. If no bucket name is specified either, the value of this field is **/**. 2. If a subresource (such as **?acl** and **?logging**) exists, the subresource must be added. OBS supports a variety of sub-resources, including acl, append, attname, cors, customdomain, delete, deletebucket, encryption, length, lifecycle, location, logging, metadata, modify, name, notification, partNumber, policy, position, quota, rename, replication, response-cache-control, response-content-disposition, response-content-encoding, response-content-language, response-content-type, response-expires, restore, storageClass, storagePolicy, storageinfo, tagging, torrent, truncate, uploadId, uploads, versionId, versioning, versions, website, and x-obs-security-token. 3. If there are multiple subresources, sort them in the alphabetical order from a to z, and use **&** to combine the subresources. **NOTE** ● A subresource is unique. Do not add subresources with the same keyword (for example, **key=value1&key=value2**) in the same request URL. In this case, signature is computed only based on the first subresource, and only the value of the first subresource takes effect on the actual service. ● Using the **GetObject** API as an example, assume there is a bucket named **bucket-test** and an object named **object-test** in the bucket, and the object version is **xxx**. When obtaining the object, you need to rewrite Content-Type to **text/plain**. Then, the **CanonicalizedResource** calculated by the signature is **/bucket-test/object-test?response-content-type=text/plain&versionId=xxx**.

The following tables provide some examples of generating StringToSign.

Table 3-6 Obtaining an object

Request Header	StringToSign
GET /object.txt HTTP/1.1 Host: bucket.obs.*region*.example.com Date: Sat, 12 Oct 2015 08:12:38 GMT	GET \n \n \n Sat, 12 Oct 2015 08:12:38 GMT\n /bucket/object.txt

Table 3-7 Using temporary AK/SK and security token to upload objects

Request Header	StringToSign
PUT /object.txt HTTP/1.1 User-Agent: curl/7.15.5 Host: bucket.obs.*region*.example.com x-obs-date:Tue, 15 Oct 2015 07:20:09 GMT x-obs-security-token: YwkaRTbdY8g7q.... content-type: text/plain Content-Length: 5913339	PUT\n \n text/plain\n \n x-obs-date:Tue, 15 Oct 2015 07:20:09 GMT\n x-obs-security-token:YwkaRTbdY8g7q....\n /bucket/object.txt

Table 3-8 An object upload request containing header fields

Request Header	StringToSign
PUT /object.txt HTTP/1.1 User-Agent: curl/7.15.5 Host: bucket.obs.*region*.example.com Date: Mon, 14 Oct 2015 12:08:34 GMT x-obs-acl: public-read content-type: text/plain Content-Length: 5913339	PUT\n \n text/plain\n Mon, 14 Oct 2015 12:08:34 GMT\n x-obs-acl:public-read\n /bucket/object.txt

Table 3-9 Obtaining an object ACL

Request Header	StringToSign
GET /object.txt?acl HTTP/1.1 Host: bucket.obs.*region*.example.com Date: Sat, 12 Oct 2015 08:12:38 GMT	GET \n \n \n Sat, 12 Oct 2015 08:12:38 GMT\n /bucket/object.txt?acl

Table 3-10 An object upload request carrying the Content-MD5 header

Request Header	StringToSign
PUT /object.txt HTTP/1.1 Host: bucket.obs.*region*.example.com x-obs-date:Tue, 15 Oct 2015 07:20:09 GMT Content-MD5: I5pU0r4+sgO9Emgl1KMQUg== Content-Length: 5913339	PUT\n I5pU0r4+sgO9Emgl1KMQUg==\n \n \n x-obs-date:Tue, 15 Oct 2015 07:20:09 GMT\n /bucket/object.txt

Table 3-11 Uploading an object through a user domain name

Request Header	StringToSign
PUT /object.txt HTTP/1.1 Host: obs.ccc.com x-obs-date:Tue, 15 Oct 2015 07:20:09 GMT Content-MD5: I5pU0r4+sgO9Emgl1KMQUg== Content-Length: 5913339	PUT\n I5pU0r4+sgO9Emgl1KMQUg==\n \n \n x-obs-date:Tue, 15 Oct 2015 07:20:09 GMT\n /obs.ccc.com/object.txt

Content-MD5 Algorithm in Java

```
import java.security.MessageDigest;
import sun.misc.BASE64Encoder;
import java.io.UnsupportedEncodingException;
import java.security.NoSuchAlgorithmException;

public class Md5{
    public static void main(String[] args) {
        try {
            String exampleString = "blog";
            MessageDigest messageDigest = MessageDigest.getInstance("MD5");
            BASE64Encoder encoder = new BASE64Encoder();
            String contentMd5 = encoder.encode(messageDigest.digest(exampleString.getBytes("utf-8")));
```



```
            System.out.println("Content-MD5:" + contentMd5);
        } catch (NoSuchAlgorithmException | UnsupportedEncodingException e)
        {
            e.printStackTrace();
        }
    }
}
```

The signature is generated as follows based on the StringToSign and SK. The hash-based message authentication code algorithm (HMAC algorithm) is used to generate the signature.

```
Signature = Base64( HMAC-SHA1( YourSecretAccessKeyID, UTF-8-Encoding-Of( StringToSign ) ) )
```

For example, to create a private bucket named **newbucketname2** in a region, the client request format is as follows:

```
PUT / HTTP/1.1
Host: newbucketname2.obs.region.example.com
Content-Length: length
Date: Fri, 06 Jul 2018 03:45:51 GMT
x-obs-acl:private
x-obs-storage-class:STANDARD
Authorization: OBS UDSIAMSTUBTEST000254:ydH8ffpcbS6YpeOMcEZfn0wE90c=

<CreateBucketConfiguration xmlns="http://obs.region.example.com/doc/2015-06-30/">
    <Location>region</Location>
</CreateBucketConfiguration>
```

Signature Calculation in Java

```
import java.io.UnsupportedEncodingException;
import java.net.URLEncoder;
import java.security.InvalidKeyException;
import java.security.NoSuchAlgorithmException;
import java.util.ArrayList;
import java.util.Arrays;
import java.util.Base64;
import java.util.Collections;
import java.util.HashMap;
import java.util.List;
import java.util.Locale;
import java.util.Map;
import java.util.TreeMap;

import javax.crypto.Mac;
import javax.crypto.spec.SecretKeySpec;

import org.omg.CosNaming.IstringHelper;


public class SignDemo {

    private static final String SIGN_SEP = "\n";

    private static final String OBS_PREFIX = "x-obs-";

 private static final String DEFAULT_ENCODING = "UTF-8";

 private static final List<String> SUB_RESOURCES = Collections.unmodifiableList(Arrays.asList(
   "CDNNotifyConfiguration", "acl", "append", "attname",  "cors", "customdomain", "delete",
   "deletebucket", "encryption", "length", "lifecycle", "location", "logging",
   "metadata", "mirrorBackToSource", "modify", "name", "notification", "obscompresspolicy",
   "partNumber", "policy", "position", "quota","rename", "replication", "response-cache-control",
   "response-content-disposition","response-content-encoding", "response-content-language", "response-
content-type",
   "response-expires","restore", "storageClass", "storagePolicy", "storageinfo", "tagging", "torrent",
"truncate",
```



```
  "uploadId", "uploads", "versionId", "versioning", "versions", "website",
  "x-obs-security-token"));

 private String ak;

 private String sk;

  public String urlEncode(String input) throws UnsupportedEncodingException
   {
  return URLEncoder.encode(input, DEFAULT_ENCODING)
        .replaceAll("%7E", "~") //for browser
        .replaceAll("%2F", "/")
        .replaceAll("%20", "+");
   }

 private String join(List<?> items, String delimiter)
   {
       StringBuilder sb = new StringBuilder();
       for (int i = 0; i < items.size(); i++)
       {
 String item = items.get(i).toString();
           sb.append(item);
           if (i < items.size() - 1)
           {
               sb.append(delimiter);
           }
       }
       return sb.toString();
   }

    private boolean isValid(String input) {
       return input != null && !input.equals("");
   }

    public String hamcSha1(String input) throws NoSuchAlgorithmException, InvalidKeyException,
UnsupportedEncodingException {
       SecretKeySpec signingKey = new SecretKeySpec(this.sk.getBytes(DEFAULT_ENCODING), "HmacSHA1");
       Mac mac = Mac.getInstance("HmacSHA1");
       mac.init(signingKey);
       return Base64.getEncoder().encodeToString(mac.doFinal(input.getBytes(DEFAULT_ENCODING)));
   }

    private String stringToSign(String httpMethod, Map<String, String[]> headers, Map<String, String>
queries,
           String bucketName, String objectName) throws Exception{
       String contentMd5 = "";
       String contentType = "";
       String date = "";

       TreeMap<String, String> canonicalizedHeaders = new TreeMap<String, String>();

       String key;
       List<String> temp = new ArrayList<String>();
       for(Map.Entry<String, String[]> entry : headers.entrySet()) {
           key = entry.getKey();
           if(key == null || entry.getValue() == null || entry.getValue().length == 0) {
               continue;
           }

           key = key.trim().toLowerCase(Locale.ENGLISH);
           if(key.equals("content-md5")) {
               contentMd5 = entry.getValue()[0];
               continue;
           }

           if(key.equals("content-type")) {
               contentType = entry.getValue()[0];
               continue;
           }
```



```
            if(key.equals("date")) {
                date = entry.getValue()[0];
                continue;
            }

            if(key.startsWith(OBS_PREFIX)) {

                for(String value : entry.getValue()) {
                    if(value != null) {
                        temp.add(value.trim());
                    }
                }
                canonicalizedHeaders.put(key, this.join(temp, ","));
                temp.clear();
            }
        }

        if(canonicalizedHeaders.containsKey("x-obs-date")) {
            date = "";
        }


        // handle method/content-md5/content-type/date
        StringBuilder stringToSign = new StringBuilder();
        stringToSign.append(httpMethod).append(SIGN_SEP)
            .append(contentMd5).append(SIGN_SEP)
            .append(contentType).append(SIGN_SEP)
            .append(date).append(SIGN_SEP);

        // handle canonicalizedHeaders
        for(Map.Entry<String, String> entry : canonicalizedHeaders.entrySet()) {
            stringToSign.append(entry.getKey()).append(":").append(entry.getValue()).append(SIGN_SEP);
        }

        // handle CanonicalizedResource
        stringToSign.append("/");
        if(this.isValid(bucketName)) {
            stringToSign.append(bucketName).append("/");
            if(this.isValid(objectName)) {
                stringToSign.append(this.urlEncode(objectName));
            }
        }

        TreeMap<String, String> canonicalizedResource = new TreeMap<String, String>();
        for(Map.Entry<String, String> entry : queries.entrySet()) {
            key = entry.getKey();
            if(key == null) {
                continue;
            }

            if(SUB_RESOURCES.contains(key)) {
                canonicalizedResource.put(key, entry.getValue());
            }
        }

        if(canonicalizedResource.size() > 0) {
            stringToSign.append("?");
            for(Map.Entry<String, String> entry : canonicalizedResource.entrySet()) {
                stringToSign.append(entry.getKey());
                if(this.isValid(entry.getValue())) {
                    stringToSign.append("=").append(entry.getValue());
                }
                            stringToSign.append("&");
            }
                    stringToSign.deleteCharAt(stringToSign.length()-1);
        }

//      System.out.println(String.format("StringToSign:%s%s", SIGN_SEP, stringToSign.toString()));
```



```
        return stringToSign.toString();
    }

    public String headerSignature(String httpMethod, Map<String, String[]> headers, Map<String, String>
queries,
            String bucketName, String objectName) throws Exception {

        //1. stringToSign
        String stringToSign = this.stringToSign(httpMethod, headers, queries, bucketName, objectName);

        //2. signature
        return String.format("OBS %s:%s", this.ak, this.hamcSha1(stringToSign));
    }


    public String querySignature(String httpMethod, Map<String, String[]> headers, Map<String, String>
queries,
            String bucketName, String objectName, long expires) throws Exception {
        if(headers.containsKey("x-obs-date")) {
            headers.put("x-obs-date", new String[] {String.valueOf(expires)});
        }else {
            headers.put("date", new String[] {String.valueOf(expires)});
        }
        //1. stringToSign
        String stringToSign = this.stringToSign(httpMethod, headers, queries, bucketName, objectName);

        //2. signature
        return this.urlEncode(this.hamcSha1(stringToSign));
    }

    public static void main(String[] args) throws Exception {
        SignDemo demo = new SignDemo();

            /* 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 the code in this example, configure environment variables YOUR_AK and YOUR_SK. */
        demo.ak = System.getenv("YOUR_AK");
        demo.sk = System.getenv("YOUR_SK");

        String bucketName = "bucket-test";
        String objectName = "hello.jpg";
        Map<String, String[]> headers = new HashMap<String, String[]>();
        headers.put("date", new String[] {"Sat, 12 Oct 2015 08:12:38 GMT"});
        headers.put("x-obs-acl", new String[] {"public-read"});
        headers.put("x-obs-meta-key1", new String[] {"value1"});
        headers.put("x-obs-meta-key2", new String[] {"value2", "value3"});
        Map<String, String> queries = new HashMap<String, String>();
        queries.put("acl", null);

        System.out.println(demo.headerSignature("PUT", headers, queries, bucketName, objectName));
    }

}
```

The calculation result of the signature is **ydH8ffpcbS6YpeOMcEZfn0wE90c=**, which varies depending on the execution time.

Signature Algorithm in Python

```
import sys
import hashlib
import hmac
import binascii
from datetime import datetime
IS_PYTHON2 = sys.version_info.major == 2 or sys.version < '3'

# 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 the code in this example, configure environment variables YOUR_AK and YOUR_SK.
yourSecretAccessKeyID = os.getenv('YOUR_SK')
httpMethod = "PUT"
contentType = "application/xml"
# "date" is the time when the request was actually generated
date = datetime.utcnow().strftime('%a, %d %b %Y %H:%M:%S GMT')
canonicalizedHeaders = "x-obs-acl:private\n"
CanonicalizedResource = "/newbucketname2"
canonical_string = httpMethod + "\n" + "\n" + contentType + "\n" + date + "\n" + canonicalizedHeaders +
CanonicalizedResource
if IS_PYTHON2:
    hashed = hmac.new(yourSecretAccessKeyID, canonical_string, hashlib.sha1)
    encode_canonical = binascii.b2a_base64(hashed.digest())[:-1]
else:
    hashed = hmac.new(yourSecretAccessKeyID.encode('UTF-8'),
canonical_string.encode('UTF-8'),hashlib.sha1)
    encode_canonical = binascii.b2a_base64(hashed.digest())[:-1].decode('UTF-8')
print(encode_canonical)
```

The calculation result of the signature is **ydH8ffpcbS6YpeOMcEZfn0wE90c=**, which varies depending on the execution time.

3.2.3 Authentication of Signature in a URL

OBS allows users to construct a URL for a specific operation. The URL contains information such as the user's AK, signature, validity period, and resources. Any user who obtains the URL can perform the operation. After receiving the request, the OBS deems that the operation is performed by the user who issues the URL. For example, if the URL of an object download request carries signature information is constructed, the user who obtains the URL can download the object, but the URL is valid only within the expiration time specified by the parameter of **Expires**. The URL that carries the signature is used to allow others to use the pre-issued URL for identity authentication when the SK is not provided, and perform the predefined operation.

The format of the message where a signature is contained in the URL:

```
GET /ObjectKey?AccessKeyId=AccessKeyID&Expires=ExpiresValue&Signature=signature HTTP/1.1
Host: bucketname.obs.region.example.com
```

The format of the message where a temporary AK/SK pair and a security token are used in the URL for downloading objects:

```
GET /ObjectKey?AccessKeyId=AccessKeyID&Expires=ExpiresValue&Signature=signature&x-obs-security-
token=securitytoken HTTP/1.1
Host: bucketname.obs.region.example.com
```

Table 3-12 describes the parameters.

Table 3-12 Request parameters

Parameter	Description	Mandatory
AccessKeyId	AK information of the issuer. OBS determines the identity of the issuer based on the AK and considers that the URL is accessed by the issuer. Type: string	Yes

Parameter	Description	Mandatory
Expires	Indicates when the temporarily authorized URL expires, in seconds. The time must be in Coordinated Universal Time (UTC) format and later than 00:00:00 on January 1, 1970. Type: string	Yes
Signature	The signature generated using the SK and the expiration time. Type: string	Yes
x-obs-security-token	During temporary authentication, the temporary AK/SK and security token must be used at the same time and the **x-obs-security-token** field must be added to the request header.	No

The process of calculating a signature is as follows:

1. Construct the StringToSign.
2. Encode the result of **1** in UTF-8.
3. Use the SK to calculate the HMAC-SHA1 signature on the result of **2**.
4. Encode the result of **3** in Base64.
5. Encode the result of **4** in URL to obtain the signature.

The StringToSign is constructed according to the following rules. **Table 3-13** describes the parameters.

```
StringToSign =
    HTTP-Verb + "\n" +
    Content-MD5 + "\n" +
    Content-Type + "\n" +
    Expires + "\n" +
    CanonicalizedHeaders +   CanonicalizedResource;
```

Table 3-13 Parameters required for constructing a StringToSign

Parameter	Description
HTTP-Verb	Indicates an HTTP request method supported by the OBS REST API. The value can be an HTTP verb such as **PUT**, **GET**, or **DELETE**.
Content-MD5	Base64-encoded 128-bit MD5 digest of the message according to RFC 1864. This parameter can be empty.
Content-Type	Specifies the message type, for example, **text/plain**. If a request does not contain this header field, this parameter is deemed as an empty string.

Parameter	Description
Expires	Expiration time of the temporary authorization, that is, the value of parameter **Expires** in the request message: **ExpiresValue**.
CanonicalizedHeaders	OBS request header field in an HTTP request header, referring to header fields starting with **x-obs-**, such as, **x-obs-date**, **x-obs-acl**, and **x-obs-meta-***. 1. All characters of keywords in the header field must be converted to lower-case letters. If a request contains multiple header fields, these fields should be organized by keywords in the alphabetical order from a to z. 2. If multiple header fields in a request have the same prefix, combine the header fields into one. For example, **x-obs-meta-name:name1** and **x-obs-meta-name:name2** should be reorganized into **x-obs-meta-name:name1,name2**. Use comma to separate the values. 3. Keywords in the request header field cannot contain non-ASCII or unrecognizable characters, which are also not advisable for values in the request header field. If the two types of characters are necessary, they should be encoded and decoded on the client side. Either URL encoding or Base64 encoding is acceptable, but the server does not perform decoding. 4. Delete meaningless spaces and tabs in a header field. For example, **x-obs-meta-name: name** (with a meaningless space before **name**) must be changed to **x-obs-meta-name:name**. 5. Each header field occupies a separate line.

Parameter	Description
CanonicalizedResource	Indicates the OBS resource specified by an HTTP request. This parameter is constructed as follows: <Bucket name + Object name> + [Subresource 1] + [Subresource 2] + ... 1. Bucket name and object name, for example, **/*bucket/object***. If no object name is specified, for example, **/*bucket/***, the entire bucket is listed. If no bucket name is specified either, the value of this field is **/**. 2. If a subresource (such as **?acl** and **?logging**) exists, the subresource must be added. OBS supports a variety of sub-resources, including acl, append, attname, cors, customdomain, delete, deletebucket, encryption, length, lifecycle, location, logging, metadata, modify, name, notification, partNumber, policy, position, quota, rename, replication, response-cache-control, response-content-disposition, response-content-encoding, response-content-language, response-content-type, response-expires, restore, storageClass, storagePolicy, storageinfo, tagging, torrent, truncate, uploadId, uploads, versionId, versioning, versions, website, and x-obs-security-token. 3. If there are multiple subresources, sort them in the alphabetical order from a to z, and use **&** to combine the subresources. **NOTE** • A subresource is unique. Do not add subresources with the same keyword (for example, **key=value1&key=value2**) in the same request URL. In this case, signature is computed only based on the first subresource, and only the value of the first subresource takes effect on the actual service. • Using the **GetObject** API as an example, assume there is a bucket named **bucket-test** and an object named **object-test** in the bucket, and the object version is **xxx**. When obtaining the object, you need to rewrite Content-Type to **text/plain**. Then, the **CanonicalizedResource** calculated by the signature is **/bucket-test/object-test?response-content-type=text/plain&versionId=xxx**.

The signature is generated as follows based on the StringToSign and SK. The hash-based message authentication code algorithm (HMAC algorithm) is used to generate the signature.

```
Signature = URL-Encode( Base64( HMAC-SHA1( YourSecretAccessKeyID, UTF-8-Encoding-
Of( StringToSign ) ) ) )
```

The method for calculating the signature carried in the URL is different from that for calculating the authorization signature carried in a header.

- The signature in the URL must be encoded using the URL after Base64 encoding.
- **Expires** in **StringToSign** corresponds to **Date** in authorization information.

Generate a predefined URL instance for the browser by carrying the signature in the URL.

Table 3-14 Request that has the signature carried in the URL and the StringToSign

Request Header	StringToSign
GET /objectkey?AccessKeyId=MFyfvK41ba2giqM7Uio6PznpdUKGpownRZlmVmHc&Expires=1532779451&Signature=0Akylf43Bm3mD1bh2rM3dmVp1Bo%3D HTTP/1.1 Host: examplebucket.obs.*region*.example.com	GET \n \n \n 1532779451\n /examplebucket/objectkey

Table 3-15 Object download request that has the temporary AK/SK and security token carried in the URL and the StringToSign

Request Header	StringToSign
GET /objectkey?AccessKeyId=MFyfvK41ba2giqM7Uio6PznpdUKGpownRZlmVmHc&Expires=1532779451&Signature=0Akylf43Bm3mD1bh2rM3dmVp1Bo%3D&x-obs-security-token=YwkaRTbdY8g7q.... HTTP/1.1 Host: examplebucket.obs.*region*.example.com	GET \n \n \n 1532779451\n /examplebucket/objectkey?x-obs-security-token=YwkaRTbdY8g7q....

Calculation rule of the signature

```
Signature = URL-Encode( Base64( HMAC-SHA1( YourSecretAccessKeyID, UTF-8-Encoding-Of( StringToSign ) ) ) )
```

Calculate the signature and use the host as the prefix of the URL to generate a predefined URL:

http(s)://examplebucket.obs.*region*.example.com/objectkey?AccessKeyId=AccessKeyID&Expires=1532779451&Signature=0Akylf43Bm3mD1bh2rM3dmVp1Bo%3D

If you enter the address in the browser, then the object **objectkey** in the **examplebucket** bucket can be downloaded. The validity period of this link is **1532779451** (indicating Sat Jul 28 20:04:11 CST 2018).

In the Linux operating system, when running the **curl** command, you need to add a forward slash (\) to escape the character (&). The following command can download the **objectkey** object to the **output** file:

curl http(s)://examplebucket.obs.*region*.example.com/objectkey?AccessKeyId=AccessKeyID\&Expires=1532779451\&Signature=0Akylf43Bm3mD1bh2rM3dmVp1Bo%3D -X GET -o output

NOTE

If you want to use the pre-defined URL generated by the signature carried in the URL in the browser, do not use Content-MD5, Content-Type, or CanonicalizedHeaders that can only be carried in the header to calculate the signature. Otherwise, the browser cannot carry these parameters. After the request is sent to the server, a message is displayed indicating that the signature is incorrect.

Signature Calculation in Java

```
import java.io.UnsupportedEncodingException;
import java.net.URLEncoder;
import java.security.InvalidKeyException;
import java.security.NoSuchAlgorithmException;
import java.util.ArrayList;
import java.util.Arrays;
import java.util.Base64;
import java.util.Collections;
import java.util.HashMap;
import java.util.List;
import java.util.Locale;
import java.util.Map;
import java.util.TreeMap;
import java.util.regex.Pattern;

import javax.crypto.Mac;
import javax.crypto.spec.SecretKeySpec;

public class SignDemo {

    private static final String SIGN_SEP = "\n";

    private static final String OBS_PREFIX = "x-obs-";

    private static final String DEFAULT_ENCODING = "UTF-8";

    private static final List<String> SUB_RESOURCES = Collections.unmodifiableList(Arrays.asList(
            "CDNNotifyConfiguration", "acl", "append", "attname",  "cors", "customdomain", "delete",
            "deletebucket", "encryption", "length", "lifecycle", "location", "logging",
            "metadata", "mirrorBackToSource", "modify", "name", "notification", "obscompresspolicy",
            "partNumber", "policy", "position", "quota","rename", "replication", "response-cache-control",
            "response-content-disposition","response-content-encoding", "response-content-language",
"response-content-type",
            "response-expires","restore", "storageClass", "storagePolicy", "storageinfo", "tagging", "torrent",
"truncate",
            "uploadId", "uploads", "versionId", "versioning", "versions", "website",
            "x-obs-security-token"));

    private String ak;

    private String sk;

    private boolean isBucketNameValid(String bucketName) {
        if (bucketName == null || bucketName.length() > 63 || bucketName.length() < 3) {
            return false;
        }
```

```
        if (!Pattern.matches("^[a-z0-9][a-z0-9.-]+$", bucketName)) {
            return false;
        }

        if (Pattern.matches("(\\d{1,3}\\.){3}\\d{1,3}", bucketName)) {
            return false;
        }

        String[] fragments = bucketName.split("\\.");
        for (int i = 0; i < fragments.length; i++) {
            if (Pattern.matches("^-.*", fragments[i]) || Pattern.matches(".*-$", fragments[i])
                    || Pattern.matches("^$", fragments[i])) {
                return false;
            }
        }

        return true;
    }

    public String encodeUrlString(String path) throws UnsupportedEncodingException {
        return URLEncoder.encode(path, DEFAULT_ENCODING)
                .replaceAll("\\+", "%20")
                .replaceAll("\\*", "%2A")
                .replaceAll("%7E", "~");
    }

    public String encodeObjectName(String objectName) throws UnsupportedEncodingException {
        StringBuilder result = new StringBuilder();
        String[] tokens = objectName.split("/");
        for (int i = 0; i < tokens.length; i++) {
            result.append(this.encodeUrlString(tokens[i]));
            if (i < tokens.length - 1) {
                result.append("/");
            }
        }
        return result.toString();
    }

    private String join(List<?> items, String delimiter) {
        StringBuilder sb = new StringBuilder();
        for (int i = 0; i < items.size(); i++) {
            String item = items.get(i).toString();
            sb.append(item);
            if (i < items.size() - 1) {
                sb.append(delimiter);
            }
        }
        return sb.toString();
    }

    private boolean isValid(String input) {
        return input != null && !input.equals("");
    }

    public String hmacSha1(String input) throws NoSuchAlgorithmException, InvalidKeyException,
UnsupportedEncodingException {
        SecretKeySpec signingKey = new SecretKeySpec(this.sk.getBytes(DEFAULT_ENCODING), "HmacSHA1");
        Mac mac = Mac.getInstance("HmacSHA1");
        mac.init(signingKey);
        return Base64.getEncoder().encodeToString(mac.doFinal(input.getBytes(DEFAULT_ENCODING)));
    }

    private String stringToSign(String httpMethod, Map<String, String[]> headers, Map<String, String>
queries,
                                String bucketName, String objectName, long expires) throws Exception {
        String contentMd5 = "";
        String contentType = "";
        TreeMap<String, String> canonicalizedHeaders = new TreeMap<String, String>();
        String key;
```

```
List<String> temp = new ArrayList<String>();
for (Map.Entry<String, String[]> entry : headers.entrySet()) {
    key = entry.getKey();
    if (key == null || entry.getValue() == null || entry.getValue().length == 0) {
        continue;
    }
    key = key.trim().toLowerCase(Locale.ENGLISH);
    if (key.equals("content-md5")) {
        contentMd5 = entry.getValue()[0];
        continue;
    }
    if (key.equals("content-type")) {
        contentType = entry.getValue()[0];
        continue;
    }
    if (key.startsWith(OBS_PREFIX)) {
        for (String value : entry.getValue()) {
            if (value != null) {
                temp.add(value.trim());
            }
        }
        canonicalizedHeaders.put(key, this.join(temp, ","));
        temp.clear();
    }
}
// handle method/content-md5/content-type
StringBuilder stringToSign = new StringBuilder();
stringToSign.append(httpMethod).append(SIGN_SEP)
        .append(contentMd5).append(SIGN_SEP)
        .append(contentType).append(SIGN_SEP)
        .append(expires).append(SIGN_SEP);


// handle canonicalizedHeaders
for (Map.Entry<String, String> entry : canonicalizedHeaders.entrySet()) {
    stringToSign.append(entry.getKey()).append(":").append(entry.getValue()).append(SIGN_SEP);
}


// handle CanonicalizedResource
stringToSign.append("/");
if (this.isValid(bucketName)) {
    stringToSign.append(bucketName).append("/");
    if (this.isValid(objectName)) {
        stringToSign.append(this.encodeObjectName(objectName));
    }
}

TreeMap<String, String> canonicalizedResource = new TreeMap<String, String>();
for (Map.Entry<String, String> entry : queries.entrySet()) {
    key = entry.getKey();
    if (key == null) {
        continue;
    }

    if (SUB_RESOURCES.contains(key)) {
        canonicalizedResource.put(key, entry.getValue());
    }
}

if (canonicalizedResource.size() > 0) {
    stringToSign.append("?");
    for (Map.Entry<String, String> entry : canonicalizedResource.entrySet()) {
        stringToSign.append(entry.getKey());
        if (this.isValid(entry.getValue())) {
            stringToSign.append("=").append(entry.getValue());
        }
        stringToSign.append("&");
    }
```



```
            stringToSign.deleteCharAt(stringToSign.length() - 1);
        }
        //        System.out.println(String.format("StringToSign:%s%s", SIGN_SEP, stringToSign.toString()));

        return stringToSign.toString();
    }

    public String querySignature(String httpMethod, Map<String, String[]> headers, Map<String, String>
queries,
                                 String bucketName, String objectName, long expires) throws Exception {
        if (!isBucketNameValid(bucketName)) {
            throw new IllegalArgumentException("the bucketName is illegal");
        }
        //1. stringToSign
        String stringToSign = this.stringToSign(httpMethod, headers, queries, bucketName, objectName,
expires);

        //2. signature
        return this.encodeUrlString(this.hmacSha1(stringToSign));
    }

    public String getURL(String endpoint, Map<String, String> queries,
                         String bucketName, String objectName, String signature, long expires) throws
UnsupportedEncodingException {
        StringBuilder URL = new StringBuilder();
        URL.append("https://").append(bucketName).append(".").append(endpoint).append("/").
                append(this.encodeObjectName(objectName)).append("?");
        String key;
        for (Map.Entry<String, String> entry : queries.entrySet()) {
            key = entry.getKey();
            if (key == null) {
                continue;
            }
            if (SUB_RESOURCES.contains(key)) {
                String value = entry.getValue();
                URL.append(key);
                if (value != null) {
                    URL.append("=").append(value).append("&");
                } else {
                    URL.append("&");
                }
            }
        }
        URL.append("AccessKeyId=").append(this.ak).append("&Expires=").append(expires).
                append("&Signature=").append(signature);
        return URL.toString();
    }

    public static void main(String[] args) throws Exception {
        SignDemo demo = new SignDemo();

        /* 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 the code in this example, configure environment variables YOUR_AK and YOUR_SK. */
    demo.ak = System.getenv("YOUR_AK");
    demo.sk = System.getenv("YOUR_SK");
        String endpoint = "<your-endpoint>";

        String bucketName = "bucket-test";
        String objectName = "hello.jpg";

                // A header cannot be carried if you want to use a URL to access OBS with a browser. If a header
is added to headers, the signature does not match. To use headers, it must be processed by the client.
        Map<String, String[]> headers = new HashMap<String, String[]>();
        Map<String, String> queries = new HashMap<String, String>();

                // Expiration time. Set it to expire in 24 hours.
        long expires = (System.currentTimeMillis() + 86400000L) / 1000;
```



```
        String signature = demo.querySignature("GET", headers, queries, bucketName, objectName, expires);
        System.out.println(signature);
        String URL = demo.getURL(endpoint, queries, bucketName, objectName, signature, expires);
        System.out.println(URL);
    }
}
```

3.2.4 Authentication of Signature Carried in the Table Uploaded Through a Browser

OBS supports browser-based object upload using the POST method. Signatures of such requests are uploaded in tables. First, create a security policy and specify the requirements in the request, for example, bucket name and object name prefix. Then, create a signature based on this policy. The request form to be signed must contain valid signature and policy. Finally, create a table to upload the object to the bucket.

The process of calculating a signature is as follows:

1. Encode the policy content in UTF-8.
2. Encode the result of **1** in Base64.
3. Use the SK to calculate the HMAC-SHA1 signature on the result of **2**.
4. Encode the result of **3** in Base64 to obtain the signature.

```
StringToSign = Base64( UTF-8-Encoding-Of( policy ) )
Signature = Base64( HMAC-SHA1( YourSecretAccessKeyID, StringToSign ) )
```

The content of the policy is as follows:

```
{ "expiration": "2017-12-31T12:00:00.000Z",
  "conditions": [
    {"x-obs-acl": "public-read" },
    {"x-obs-security-token": "YwkaRTbdY8g7q...." },
    {"bucket": "book" },
    ["starts-with", "$key", "user/"]
  ]
}
```

The policy contains the validity period (see **Expiration**) and conditions (see **Conditions**).

Expiration

The **expiration** field describes when the signature will expire, which is expressed in the format according to ISO 8601 UTC. For example, **expiration: 2017-12-31T12:00:00.000Z** in the example means that the request becomes invalid after 12:00:00 on December 31, 2017. This field must be specified in a policy. It can only be in the **yyyy-MM-dd'T'HH:mm:ss'Z'** or **yyyy-MM-dd'T'HH:mm:ss.SSS'Z'** format.

Conditions

A mechanism used to verify the validity of a request. Conditions are used to define the content that must be contained in a request. In the example, the requested bucket name is **book**, the object name is prefixed with **user/**, and the ACL of the object is public read. All items in the form, excluding **AccessKeyId**, **signature**, **file**, **policy**, **token**, **field names**, and the prefix **x-ignore-**, must be included in the policy. The following table lists the items that should be contained in **Conditions**.

Table 3-16 Conditions contained in a policy

Element	Description
x-obs-acl	ACL in the request. Supports exact match and conditional match such as **starts-with**.
content-length-range	Maximum and minimum length of an object to be uploaded. The value can be a range.
Cache-Control, Content-Type, Content-Disposition, Content-Encoding, Expires	Headers specially for REST requests Supports exact match and conditional match such as **starts-with**.
key	Name of an object to be uploaded. Supports exact match and conditional match such as **starts-with**.
bucket	Name of the requested bucket. Supports exact match.
success_action_redirect	Redirection address after the upload is successful. For details, see **Uploading an Object - POST**. Supports exact match and conditional match such as **starts-with**.
success_action_status	If **success_action_redirect** is not specified, the status code is returned to the client when the upload is successful. For details, see **Uploading an Object - POST**. Supports exact match.
x-obs-meta-*	User-defined metadata. Keywords in an element cannot contain non-ASCII or unrecognizable characters. If non-ASCII or unrecognizable characters are necessary, they should be encoded and decoded on the client side. Either URL encoding or Base64 encoding is acceptable, but the server does not perform decoding. Supports exact match and conditional match such as **starts-with**.
x-obs-*	Other header fields with prefix **x-obs-**. Supports exact match and conditional match such as **starts-with**.

Element	Description
x-obs-security-token	Field name in the request header. Mandatory field for the temporary AK/SK and security token authentication.

The table below describes how policy conditions can be matched.

Table 3-17 Policy condition matching methods

Matching Method	Description
Exact Matches	Exact match by default. The value in the POST table must be the same as that in the policy. For example, if object ACL is set to **public-read** when the object is uploaded, the value of the **x-obs-acl** element in the table is **public-read**. Therefore, the conditions in the policy can be set to {"x-obs-acl": "public-read"} or ["eq", "$x-obs-acl", "public-read"], which are equivalent.
Starts With	If this condition is used, the value set in the POST table must start with a fixed character string. For example, if the name of uploaded objects must be prefixed with **user/**, the value of the **key** element in the table can be **user/test1**, **user/test2**, and so on. Therefore, conditions in the policy can be set to: **["starts-with", "$key", "user/"]**
Matching Any Content	The corresponding element in the POST table can be any value. For example, if the redirection address upon request success can be any address, the value of the **success_action_redirect** element in the table can be any value. Therefore, conditions in the policy can be set to: **["starts-with", "$success_action_redirect", ""]**

Matching Method	Description
Specifying Ranges	The content length of the **file** element in the POST table can be a specified range and is used only to limit the object size. For example, if the size of the uploaded object is between 1 MB to 10 MB, the content length of the **file** element in the table can be from **1048576** to **10485760**. Therefore, conditions in the policy can be set to (the value does not contain quotation marks) **["content-length-range", 1048576, 10485760]**

NOTE

A policy is in the JSON format. Conditions can be put in curly brackets {} and square brackets []. The key and value elements of the table are written in the curly brackets {}, which are separated by colons (:). The square brackets [] contain the condition type, key, and value. These three items are separated by commas (,). The dollar sign ($) in front of the key indicates that the key is a variable.

The table below lists the characters that must be escaped in a policy.

Table 3-18 Characters that must be escaped in a policy

Character After Escape	Real Character
\\	Backslash (\)
\$	Dollar symbol ($)
\b	Backspace
\f	Page up and down
\n	Newline characters
\r	Enter
\t	Horizontal table
\v	Vertical table
\u***xxxx***	All Unicode characters

Request and Policy Examples

The following tables provide examples of requests and policies.

Example 1: Upload the **testfile.txt** object to bucket **examplebucket** and set the object ACL to **public-read**.

Request	Policy

POST / HTTP/1.1
Host: examplebucket.obs.*region*.example.com
Content-Type: multipart/form-data; boundary=7e32233530b26
Content-Length: 1250
--7e32233530b26
Content-Disposition: form-data; name="key"
testfile.txt
--7e32233530b26
Content-Disposition: form-data; name="x-obs-acl"
public-read
--7e32233530b26
Content-Disposition: form-data; name="content-type"
text/plain
--7e32233530b26
Content-Disposition: form-data; name="AccessKeyId"
UDSIAMSTUBTEST000002
--7e32233530b26
Content-Disposition: form-data; name="policy"
ewogICJleHBpcmF0aW9uIjogIjIwMTktMDctMDFUMTI6MDA6MDAuMDAwWiIsCiAgImNvbmRpdGlvbnMiOiBbCiAgICB7ImJ1Y2tldCI6ICJleGFtcGxlYnVja2V0IiB9LAogICAgWyJlcSIsICIka2V5IiwgInRlc3RmaWxlLnR4dCJdLAogICAgeyJ4LW9icy1hY2wiOiAicHVibGljLXJlYWQiIH0sCiAgICBbImVxIiwgIiRDb250ZW50LVR5cGUiLCAidGV4dC9wbGFpbiJdLAogICAgWyJjb250ZW50LWxlbmd0aC1yYW5nZSIsIDYsIDEwXQogIF0KfQo=
--7e32233530b26
Content-Disposition: form-data; name="signature"
xxl7bZs/5FgtBUggOdQ88DPZUo0=
	{
	"expiration": "2019-07-01T12:00:00.000Z",
	"conditions": [
	{"bucket": "examplebucket" },
	["eq", "$key", "testfile.txt"],
	{"x-obs-acl": "public-read" },
	["eq", "$Content-Type", "text/plain"]
	]
	}

Request	Policy
--7e32233530b26 Content-Disposition: form-data; name="file"; filename="E:\TEST_FILE\TEST.txt" Content-Type: text/plain 123456 --7e32233530b26 Content-Disposition: form-data; name="submit" Upload --7e32233530b26--	

Example 2: Upload the **file/obj1** object to bucket **examplebucket** and configure the four custom metadata items of the object.

Request	Policy

POST / HTTP/1.1
Host: examplebucket.obs.*region*.example.com
Content-Type: multipart/form-data; boundary=7e329d630b26
Content-Length: 1597
--7e3542930b26
Content-Disposition: form-data; name="key"
file/obj1
--7e3542930b26
Content-Disposition: form-data; name="AccessKeyId"
UDSIAMSTUBTEST000002
--7e3542930b26
Content-Disposition: form-data; name="policy"
ewogICJleHBpcmF0aW9uIjogIjIwMTktMDctMDFUMTI6MDA6MDAuMDAwWiIsCiAgImNvbmRpdGlvbnMiOiBbCiAgICB7ImJ1Y2tldCI6ICJleGFtcGxlYnVja2V0IiB9LAogICAgWyJzdGFydHMtd2l0aCIsICIka2V5IiwgImZpbGUvIl0sCiAgICB7Ingtb2JzLW1ldGEtdGVzdDEiOiJ2YWx1ZTEifSwKICAgIFsiZXEiLCAiJHgtb2JzLW1ldGEtdGVzdDIiLCAidmFsdWUyIl0sCiAgICBbInN0YXJ0cy13aXRoIiwgIiR4LW9icy1tZXRhLXRlc3QzIiwgImRvYyJdLAogICAgWyJzdGFydHMtd2l0aCIsICIkeC1vYnMtbWV0YS10ZXN0NCIsICIiXQogIF0KfQo=
--7e3542930b26
Content-Disposition: form-data; name="signature"
HTId8hcaisn6FfdWKqSJP9RN4Oo=
--7e3542930b26
Content-Disposition: form-data; name="x-obs-meta-test1"
value1
--7e3542930b26
	{
	"expiration": "2019-07-01T12:00:00.000Z",
	"conditions": [
	{"bucket": "examplebucket" },
	["starts-with", "$key", "file/"],
	{"x-obs-meta-test1":"value1"},
	["eq", "$x-obs-meta-test2", "value2"],
	["starts-with", "$x-obs-meta-test3", "doc"],
	["starts-with", "$x-obs-meta-test4", ""]
	]
	}

Request	Policy
Content-Disposition: form-data; name="x-obs-meta-test2" value2 --7e3542930b26 Content-Disposition: form-data; name="x-obs-meta-test3" doc123 --7e3542930b26 Content-Disposition: form-data; name="x-obs-meta-test4" my --7e3542930b26 Content-Disposition: form-data; name="file"; filename="E:\TEST_FILE\TEST.txt" Content-Type: text/plain 123456 --7e3542930b26 Content-Disposition: form-data; name="submit" Upload --7e3542930b26--	

3.3 Returned Values

After sending a request, you will receive a response, including the status code, response header, and response body.

Status Codes

A status code is a group of digits ranging from 2*xx* (indicating successes) to 4*xx* or 5*xx* (indicating errors). It indicates the status of a response. For more information, see **Status Codes**.

Response Headers

A response header corresponds to a request header, for example, Content-Type.

For details about common response headers, see **Table 3-19**.

Table 3-19 Common response headers

Header	Description
Content-Length	The length (in bytes) of the response body. Type: string Default value: none
Connection	Indicates whether the connection to the server is a long connection or a short connection. Type: string Value options: **keep-alive**, **close** Default value: none
Date	The date and time at which OBS responds to the request. Type: string Default value: none
ETag	128-bit MD5 digest of the Base64 code of an object. ETag is the unique identifier of the object content. It can be used to identify whether the object content is changed. For example, if ETag value is **A** when an object is uploaded and the ETag value has changed to **B** when the object is downloaded, it indicates that the object content is changed. The actual ETag is the hash value of the object, which only reflects the changed content rather than the metadata. An uploaded object or copied object has a unique ETag after being encrypted using MD5. If an object is uploaded in the multipart mode, the MD5 splits ETag regardless of the encryption method. In this case, the ETag is not an MD5 digest. Type: string
x-obs-id-2	A special symbol that helps troubleshoot faults. Type: string Default value: none
x-reserved-indicator	A special symbol that helps troubleshoot faults. Type: string Default value: none
x-obs-request-id	The value created by OBS to uniquely identify the request. OBS uses this value to troubleshoot faults. Type: string Default value: none

(Optional) Response Body

A response body is generally returned in a structured format (for example, JSON or XML), corresponding to **Content-Type** in the response header, and is used to transfer content other than the response header.

4 Getting Started

4.1 Creating a Bucket

Scenarios

A bucket is a container that stores objects in OBS. You need to create a bucket before storing data in OBS.

The following describes how to call the API for **creating a bucket** in a specified region. For details about how to call an API, see **Calling APIs**.

Prerequisites

- You have obtained the AK and SK. For details about how to obtain the AK and SK, see **Obtaining Access Keys (AK/SK)**.
- You have planned the region where you want to create a bucket and obtained the endpoint required for API calls. For details, see **Endpoints**.

Once a region is determined, it cannot be modified after the bucket is created.

Creating a Bucket Named bucket001 in the a1 Region

In this example, an Apache HttpClient is used.

```
package com.obsclient;

import java.io.*;

import org.apache.http.Header;
import org.apache.http.client.methods.CloseableHttpResponse;
import org.apache.http.client.methods.HttpPut;
import org.apache.http.entity.StringEntity;
import org.apache.http.impl.client.CloseableHttpClient;
import org.apache.http.impl.client.HttpClients;

public class TestMain {
    /* 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 the code in this example, configure environment variables YOUR_AK and YOUR_SK. */
    public static String accessKey = System.getenv("YOUR_AK"); //The value is the AK obtained.
    public static String securityKey = System.getenv("YOUR_SK");  //The value is the SK obtained.
```



```
    public static String region = "a1"; // The value is the region where the planned bucket resides.
    public static String createBucketTemplate =
            "<CreateBucketConfiguration " +
            "xmlns=\"http://obs.a1.example.com/doc/2015-06-30/\">\n" +
            "<Location>" + region + "</Location>\n" +
            "</CreateBucketConfiguration>";

    public static void main(String[] str) {

         createBucket();

    }

    private static void createBucket() {
        CloseableHttpClient httpClient = HttpClients.createDefault();
        String requesttime = DateUtils.formatDate(System.currentTimeMillis());
        String contentType = "application/xml";
        HttpPut httpPut = new HttpPut("http://bucket001.obs.a1.example.com");
        httpPut.addHeader("Date", requesttime);
        httpPut.addHeader("Content-Type", contentType);

        /**Calculate the signature based on the request.**/
        String contentMD5 = "";
        String canonicalizedHeaders = "";
        String canonicalizedResource = "/bucket001/";
        // Content-MD5 and Content-Type fields do not contain line breaks. The data format is RFC 1123,
which is the same as the time in the request.
        String canonicalString = "PUT" + "\n" + contentMD5 + "\n" + contentType + "\n" + requesttime + "\n"
+ canonicalizedHeaders + canonicalizedResource;
        System.out.println("StringToSign:[" + canonicalString + "]");
        String signature = null;
        CloseableHttpResponse httpResponse = null;
        try {
            signature = Signature.signWithHmacSha1(securityKey, canonicalString);

             // Added the Authorization: OBS AccessKeyID:signature field to the header.
            httpPut.addHeader("Authorization", "OBS " + accessKey + ":" + signature);

            // Add a body.
            httpPut.setEntity(new StringEntity(createBucketTemplate));

            httpResponse = httpClient.execute(httpPut);

            // Prints the sending request information and the received response message.
            System.out.println("Request Message:");
            System.out.println(httpPut.getRequestLine());
            for (Header header : httpPut.getAllHeaders()) {
                System.out.println(header.getName() + ":" + header.getValue());
            }

            System.out.println("Response Message:");
            System.out.println(httpResponse.getStatusLine());
            for (Header header : httpResponse.getAllHeaders()) {
                System.out.println(header.getName() + ":" + header.getValue());
            }
            BufferedReader reader = new BufferedReader(new InputStreamReader(
                    httpResponse.getEntity().getContent()));

            String inputLine;
            StringBuffer response = new StringBuffer();

            while ((inputLine = reader.readLine()) != null) {
                response.append(inputLine);
            }
            reader.close();

            // print result
            System.out.println(response.toString());
        } catch (UnsupportedEncodingException e) {
```



```
            e.printStackTrace();
        } catch (IOException e) {
            e.printStackTrace();
        } finally {
            try {
                httpClient.close();
            } catch (IOException e) {
                e.printStackTrace();
            }
        }

    }

}
```

The format of the **Date** header field **DateUtils** is as follows:

```
package com.obsclient;

import java.text.DateFormat;
import java.text.SimpleDateFormat;
import java.util.Locale;
import java.util.TimeZone;

public class DateUtils {

    public static String formatDate(long time)
    {
        DateFormat serverDateFormat = new SimpleDateFormat("EEE, dd MMM yyyy HH:mm:ss z",
Locale.ENGLISH);
        serverDateFormat.setTimeZone(TimeZone.getTimeZone("GMT"));
        return serverDateFormat.format(time);
    }
}
```

The method of calculating the signature character string is as follows:

```
package com.obsclient;

import javax.crypto.Mac;
import javax.crypto.spec.SecretKeySpec;
import java.io.UnsupportedEncodingException;
import java.security.NoSuchAlgorithmException;
import java.security.InvalidKeyException;
import java.util.Base64;

public class Signature {
    public static String signWithHmacSha1(String sk, String canonicalString) throws
UnsupportedEncodingException {

        try {
            SecretKeySpec signingKey = new SecretKeySpec(sk.getBytes("UTF-8"), "HmacSHA1");
            Mac mac = Mac.getInstance("HmacSHA1");
            mac.init(signingKey);
            return Base64.getEncoder().encodeToString(mac.doFinal(canonicalString.getBytes("UTF-8")));
        } catch (NoSuchAlgorithmException | InvalidKeyException | UnsupportedEncodingException e) {
            e.printStackTrace();
        }
        return null;
    }
}
```


4.2 Listing Buckets

Scenarios

If you want to view information about all buckets created by yourself, you can call the API for listing buckets.

The following describes how to call the API for **listing buckets**. For details about how to call an API, see **Calling APIs**.

Prerequisites

- You have obtained the AK and SK. For details about how to obtain the AK and SK, see **Obtaining Access Keys (AK/SK)**.
- You have specified the region where you want to list buckets and obtained the endpoint required for API calls. For details, see **Endpoints**.

Obtaining the Bucket List in the a1 Region

In this example, an Apache HttpClient is used.

```
package com.obsclient;

import java.io.*;
import java.util.ArrayList;
import java.util.List;

import org.apache.http.Header;
import org.apache.http.HttpEntity;
import org.apache.http.NameValuePair;
import org.apache.http.client.entity.UrlEncodedFormEntity;
import org.apache.http.client.methods.CloseableHttpResponse;
import org.apache.http.client.methods.HttpGet;
import org.apache.http.client.methods.HttpPost;
import org.apache.http.client.methods.HttpPut;
import org.apache.http.entity.InputStreamEntity;
import org.apache.http.entity.StringEntity;
import org.apache.http.impl.client.CloseableHttpClient;
import org.apache.http.impl.client.HttpClients;
import org.apache.http.message.BasicNameValuePair;


public class TestMain {

    /* 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 the code in this example, configure environment variables YOUR_AK and YOUR_SK. */
    public static String accessKey = System.getenv("YOUR_AK"); //The value is the AK obtained.
    public static String securityKey = System.getenv("YOUR_SK");  //The value is the SK obtained.

    public static void main(String[] str) {

        listAllMyBuckets();

    }


    private static void listAllMyBuckets() {
        CloseableHttpClient httpClient = HttpClients.createDefault();
        String requesttime = DateUtils.formatDate(System.currentTimeMillis());
```



```
        HttpGet httpGet = new HttpGet("http://obs.a1.example.com");
        httpGet.addHeader("Date", requesttime);

        /**Calculate the signature based on the request.**/
        String contentMD5 = "";
        String contentType = "";
        String canonicalizedHeaders = "";
        String canonicalizedResource = "/";
        // Content-MD5 and Content-Type fields do not contain line breaks. The data format is RFC 1123,
which is the same as the time in the request.
        String canonicalString = "GET" + "\n" + contentMD5 + "\n" + contentType + "\n" + requesttime + "\n"
+ canonicalizedHeaders + canonicalizedResource;
        System.out.println("StringToSign:[" + canonicalString + "]");
        String signature = null;
        try {
            signature = Signature.signWithHmacSha1(securityKey, canonicalString);

             // Added the Authorization: OBS AccessKeyID:signature field to the header.
            httpGet.addHeader("Authorization", "OBS " + accessKey + ":" + signature);
            CloseableHttpResponse httpResponse = httpClient.execute(httpGet);

            // Prints the sending request information and the received response message.
            System.out.println("Request Message:");
            System.out.println(httpGet.getRequestLine());
            for (Header header : httpGet.getAllHeaders()) {
                System.out.println(header.getName() + ":" + header.getValue());
            }

            System.out.println("Response Message:");
            System.out.println(httpResponse.getStatusLine());
            for (Header header : httpResponse.getAllHeaders()) {
                System.out.println(header.getName() + ":" + header.getValue());
            }
            BufferedReader reader = new BufferedReader(new InputStreamReader(
                    httpResponse.getEntity().getContent()));

            String inputLine;
            StringBuffer response = new StringBuffer();

            while ((inputLine = reader.readLine()) != null) {
                response.append(inputLine);
            }
            reader.close();
            // print result
            System.out.println(response.toString());
        } catch (UnsupportedEncodingException e) {
            e.printStackTrace();

        } catch (IOException e) {
            e.printStackTrace();
        } finally {
            try {
                httpClient.close();
            } catch (IOException e) {
                e.printStackTrace();
            }
        }

    }

}
```

The format of the **Date** header field **DateUtils** is as follows:

```
package com.obsclient;

import java.text.DateFormat;
import java.text.SimpleDateFormat;
import java.util.Locale;
```



```
import java.util.TimeZone;

public class DateUtils {

    public static String formatDate(long time)
    {
        DateFormat serverDateFormat = new SimpleDateFormat("EEE, dd MMM yyyy HH:mm:ss z",
Locale.ENGLISH);
        serverDateFormat.setTimeZone(TimeZone.getTimeZone("GMT"));
        return serverDateFormat.format(time);
    }
}
```

The method of calculating the signature character string is as follows:

```
package com.obsclient;

import javax.crypto.Mac;
import javax.crypto.spec.SecretKeySpec;
import java.io.UnsupportedEncodingException;
import java.security.NoSuchAlgorithmException;
import java.security.InvalidKeyException;
import java.util.Base64;

public class Signature {
    public static String signWithHmacSha1(String sk, String canonicalString) throws
UnsupportedEncodingException {

        try {
            SecretKeySpec signingKey = new SecretKeySpec(sk.getBytes("UTF-8"), "HmacSHA1");
            Mac mac = Mac.getInstance("HmacSHA1");
            mac.init(signingKey);
            return Base64.getEncoder().encodeToString(mac.doFinal(canonicalString.getBytes("UTF-8")));
        } catch (NoSuchAlgorithmException | InvalidKeyException | UnsupportedEncodingException e) {
            e.printStackTrace();
        }
        return null;
    }
}
```

4.3 Uploading an Object

Scenarios

You can upload files of any type to OBS buckets for storage.

The following describes how to call the API for **uploading objects using the PUT method** to a specified bucket. For details about how to call an API, see **Calling APIs**.

Prerequisites

- You have obtained the AK and SK. For details, see **Obtaining Access Keys (AK/SK)**.
- At least one bucket is available.
- The file to be uploaded has been prepared and you know the complete local path of the file.
- You have obtained the region of the bucket which you want to upload files to and determined the endpoint required for API calls. For details, see **Endpoints**.

Uploading the Object objecttest1 to Bucket bucket001 in the a1 Region

In this example, an Apache HttpClient is used.

```
package com.obsclient;

import java.io.*;
import java.util.ArrayList;
import java.util.List;

import org.apache.http.Header;
import org.apache.http.HttpEntity;
import org.apache.http.NameValuePair;
import org.apache.http.client.entity.UrlEncodedFormEntity;
import org.apache.http.client.methods.CloseableHttpResponse;
import org.apache.http.client.methods.HttpGet;
import org.apache.http.client.methods.HttpPost;
import org.apache.http.client.methods.HttpPut;
import org.apache.http.entity.InputStreamEntity;
import org.apache.http.entity.StringEntity;
import org.apache.http.impl.client.CloseableHttpClient;
import org.apache.http.impl.client.HttpClients;
import org.apache.http.message.BasicNameValuePair;


public class TestMain {

    /* 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 the code in this example, configure environment variables YOUR_AK and YOUR_SK. */
    public static String accessKey = System.getenv("YOUR_AK"); //The value is the AK obtained.
    public static String securityKey = System.getenv("YOUR_SK");  //The value is the SK obtained.

    public static void main(String[] str) {

        putObjectToBucket();

    }


    private static void putObjectToBucket() {

        InputStream inputStream = null;
        CloseableHttpClient httpClient = HttpClients.createDefault();
        CloseableHttpResponse httpResponse = null;
        String requestTime = DateUtils.formatDate(System.currentTimeMillis());
        HttpPut httpPut = new HttpPut("http://bucket001.obs.a1.example.com/objecttest1");
        httpPut.addHeader("Date", requestTime);

         /**Calculate the signature based on the request.**/
        String contentMD5 = "";
        String contentType = "";
        String canonicalizedHeaders = "";
        String canonicalizedResource = "/bucket001/objecttest1";
        // Content-MD5 and Content-Type fields do not contain line breaks. The data format is RFC 1123, which is the same as the time in the request.
        String canonicalString = "PUT" + "\n" + contentMD5 + "\n" + contentType + "\n" + requestTime + "\n" + canonicalizedHeaders + canonicalizedResource;
        System.out.println("StringToSign:[" + canonicalString + "]");
        String signature = null;
        try {
            signature = Signature.signWithHmacSha1(securityKey, canonicalString);
            // Directory for storing uploaded files
            inputStream = new FileInputStream("D:\\OBSobject\\text01.txt");
            InputStreamEntity entity = new InputStreamEntity(inputStream);
            httpPut.setEntity(entity);

           // Added the Authorization: OBS AccessKeyID:signature field to the header.
```



```
            httpPut.addHeader("Authorization", "OBS " + accessKey + ":" + signature);
            httpResponse = httpClient.execute(httpPut);

           // Prints the sending request information and the received response message.
            System.out.println("Request Message:");
            System.out.println(httpPut.getRequestLine());
            for (Header header : httpPut.getAllHeaders()) {
                System.out.println(header.getName() + ":" + header.getValue());
            }

            System.out.println("Response Message:");
            System.out.println(httpResponse.getStatusLine());
            for (Header header : httpResponse.getAllHeaders()) {
                System.out.println(header.getName() + ":" + header.getValue());
            }
            BufferedReader reader = new BufferedReader(new InputStreamReader(
                    httpResponse.getEntity().getContent()));

            String inputLine;
            StringBuffer response = new StringBuffer();

            while ((inputLine = reader.readLine()) != null) {
                response.append(inputLine);
            }
            reader.close();

            // print result
            System.out.println(response.toString());


        } catch (UnsupportedEncodingException e) {
            e.printStackTrace();

        } catch (IOException e) {
            e.printStackTrace();
        } finally {
            try {
                httpClient.close();
            } catch (IOException e) {
                e.printStackTrace();
            }
        }
    }

}
```

The format of the Date header field DateUtils is as follows:

```
package com.obsclient;

import java.text.DateFormat;
import java.text.SimpleDateFormat;
import java.util.Locale;
import java.util.TimeZone;

public class DateUtils {

    public static String formatDate(long time)
    {
        DateFormat serverDateFormat = new SimpleDateFormat("EEE, dd MMM yyyy HH:mm:ss z",
Locale.ENGLISH);
        serverDateFormat.setTimeZone(TimeZone.getTimeZone("GMT"));
        return serverDateFormat.format(time);
    }
}
```

The method of calculating the signature character string is as follows:


```
package com.obsclient;

import javax.crypto.Mac;
import javax.crypto.spec.SecretKeySpec;
import java.io.UnsupportedEncodingException;
import java.security.NoSuchAlgorithmException;
import java.security.InvalidKeyException;
import java.util.Base64;

public class Signature {
    public static String signWithHmacSha1(String sk, String canonicalString) throws
UnsupportedEncodingException {

        try {
            SecretKeySpec signingKey = new SecretKeySpec(sk.getBytes("UTF-8"), "HmacSHA1");
            Mac mac = Mac.getInstance("HmacSHA1");
            mac.init(signingKey);
            return Base64.getEncoder().encodeToString(mac.doFinal(canonicalString.getBytes("UTF-8")));
        } catch (NoSuchAlgorithmException | InvalidKeyException | UnsupportedEncodingException e) {
            e.printStackTrace();
        }
        return null;
    }
}
```


5 APIs

5.1 Operations on Buckets

5.1.1 Listing Buckets

Functions

You can perform this operation to list all buckets that you have created.

Request Syntax

```
GET / HTTP/1.1
Host: obs.region.example.com
Date: date
Authorization: authorization
```

Request Parameters

This request contains no parameters.

Request Headers

The operation message header is the same as that of a common request. For details, see **Table 3-3**. However, this request can contain additional headers. The following table describes the additional headers for this request.

Table 5-1 Additional request headers

Header	Description	Mandatory
x-obs-bucket-type	This header field is used to specify the content to be obtained. Value: • **OBJECT**: Obtain the list of all buckets. • **POSIX**: Obtain the list of all parallel file systems. If this header is not carried, the list of all buckets and parallel file systems is obtained. Type: string Example: **x-obs-bucket-type: POSIX**	No

Request Elements

The request does not use request elements.

Response Syntax

```
GET HTTP/1.1 status_code
Content-Type: type
Date: date
Content-Length: length

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ListAllMyBucketsResult xmlns="http://obs.region.example.com/doc/2015-06-30/">
   <Owner>
      <ID>id</ID>
   </Owner>
   <Buckets>
      <Bucket>
         <Name>bucketName</Name>
         <CreationDate>date</CreationDate>
         <Location>region</Location>
      </Bucket>
      ...
   </Buckets>
</ListAllMyBucketsResult>
```

Response Headers

The response to the request uses common headers. For details, see **Table 3-19**.

Response Elements

This response contains the XML list of buckets owned by the user. **Table 5-2** describes the elements.

Table 5-2 Response elements

Element	Description
ListAllMyBucketsResult	List of buckets created by the user Type: XML
Owner	Bucket owner information, including the tenant ID. Type: XML
ID	Domain ID (account ID) of a user. Type: string
Buckets	Buckets owned by the user Type: XML
Bucket	Details about a bucket Type: XML
Name	Bucket name Type: string
CreationDate	Creation time of the bucket Type: string
Location	Location of the bucket Type: string

Error Responses

No special error responses are returned. For details about error responses, see **Table 6-2**.

Sample Request

```
GET / HTTP/1.1
User-Agent: curl/7.29.0
Host: obs.region.example.com
Accept: */*
Date: Mon, 25 Jun 2018 05:37:12 +0000
Authorization: OBS GKDF4C7Q6SI0IPGTXTJN:9HXkVQIiQKw33UEmyBI4rWrzmic=
```

Sample Response

```
HTTP/1.1 200 OK
Server: OBS
x-obs-request-id: BF260000016435722C11379647A8A00A
x-obs-id-2: 32AAAQAAEAABAAAQAAEAABAAAQAAEAABCSGGDRUM62QZi3hGP8Fz3gOloYCfZ39U
Content-Type: application/xml
Date: Mon, 25 Jun 2018 05:37:12 GMT
Content-Length: 460

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ListAllMyBucketsResult xmlns="http://obs.example.com/doc/2015-06-30/">
  <Owner>
```



```
  <ID>783fc6652cf246c096ea836694f71855</ID>
 </Owner>
 <Buckets>
  <Bucket>
   <Name>examplebucket01</Name>
   <CreationDate>2018-06-21T09:15:01.032Z</CreationDate>
   <Location>region</Location>
  </Bucket>
  <Bucket>
   <Name>examplebucket02</Name>
   <CreationDate>2018-06-22T03:56:33.700Z</CreationDate>
   <Location>region</Location>
  </Bucket>
 </Buckets>
</ListAllMyBucketsResult>
```

5.1.2 Creating a Bucket

Functions

This operation is used to create a bucket with a specified name.

NOTE

- By default, a user can have a maximum of 100 buckets.
- The name of a deleted bucket can be reused for a bucket or a parallel file system at least 30 minutes after the deletion.

A bucket name must be unique in OBS. If a user creates a bucket with the same name as that of an existing bucket under the same account and in the same region, a 200 code (indicating success) is returned. In scenarios other than the preceding one, the request for creating a bucket with the same name as that of an existing one will receive the 409 code (indicating that a namesake bucket already exists). To set an access control policy for the bucket to be created, you can add the **x-obs-acl** parameter to request headers.

Storage Class

You can create buckets with different storage classes. The **x-obs-storage-class** header in a bucket creation request specifies the bucket's storage class. If you do not specify a storage class when you upload an object to the bucket, the object inherits the storage class of the bucket. The storage class options are as follows: **STANDARD** (Standard), **WARM** (Warm), **COLD** (Cold). If the **x-obs-storage-class** header is not in the request, a Standard bucket will be created.

If the storage class of an object is not specified when it is uploaded to a bucket (see **Uploading an Object - PUT**), the object will be stored in the default storage class of the bucket.

- OBS Standard features low access latency and high throughput. It is most suitable for storing frequently accessed (multiple times per month) hot files. Potential application scenarios include big data, mobile applications, trending videos, and social media images.
- OBS Warm storage class is suitable for storing data that is infrequently accessed (less than 12 times a year) yet has quick response requirements. Potential application scenarios include file synchronization or sharing and enterprise backup. It provides the same durability, access latency, and

throughput as the Standard storage class but at a lower price. However, the Warm storage class has lower availability than the Standard one.

- OBS Cold storage class is applicable to archiving rarely-accessed (averagely once a year) data. The application scenarios include data archiving and long-term data retention for backup. The Cold storage class is secure, durable, and inexpensive, which can replace tape libraries. To keep cost low, it may take hours to restore data from the Cold storage class.

Request Syntax

```
PUT / HTTP/1.1
Host: bucketname.obs.region.example.com
Content-Length: length
Date: date
Authorization: authorization

<CreateBucketConfiguration xmlns="http://obs.region.example.com/doc/2015-06-30/">
   <Location>location</Location>
</CreateBucketConfiguration>
```

Request Parameters

This request contains no parameters.

Request Headers

The operation message header is the same as that of a common request. For details, see **Table 3-3**. However, this request can contain additional headers. The following table describes the additional headers for this request.

Table 5-3 Additional request headers

Header	Description	Mandatory
x-obs-acl	When creating a bucket, you can add this header to set the permission control policy for the bucket. The predefined common policies are as follows: **private**, **public-read**, **public-read-write**, **public-read-delivered**, and **public-read-write-delivered**. Type: string	No
x-obs-storage-class	When creating a bucket, you can add this header to specify the default storage class for the bucket. The storage class options are as follows: **STANDARD** (Standard), **WARM** (Warm), and **COLD** (Cold). If this header is not in the request, a Standard bucket will be created. Type: string	No

Header	Description	Mandatory
x-obs-grant-read	This header grants the read permission to all users under an account. It allows you to list objects in a bucket, list multipart tasks in a bucket, list multi-version objects in a bucket, and obtain bucket metadata. Type: string Example: **x-obs-grant-read:id=***Tenant ID*	No
x-obs-grant-write	This header grants the write permission to all users under an account. Therefore, the users can create, delete, and overwrite all objects in a bucket, and can initialize parts, upload parts, copy parts, merge parts, and cancel multipart upload tasks. Type: string Example: **x-obs-grant-write:id=***Tenant ID*	No
x-obs-grant-read-acp	This header grants the ACL read permission to all users under an account. Therefore, the users can read the bucket ACL information. Type: string Example: **x-obs-grant-read-acp:id=***Account ID*	No
x-obs-grant-write-acp	This header grants the ACL write permission to all users under an account. Therefore, the users can modify the ACL of the bucket. Type: string Example: **x-obs-grant-write-acp:id=***Account ID*	No
x-obs-grant-full-control	This header grants the full control permission to all users under an account. Type: string Example: **x-obs-grant-full-control:id=***Account ID*	No
x-obs-grant-read-delivered	This header grants the read permission to all users under an account. By default, the read permission is applied to all objects in the bucket. Type: string Example: **x-obs-grant-read-delivered:id=***Account ID*	No

Header	Description	Mandatory
x-obs-grant-full-control-delivered	This header grants the full control permission to all users under an account. By default, the FULL_CONTROL permission is applied to all objects in the bucket. Type: string Example: **x-obs-grant-full-control-delivered:id=***Account ID*	No
x-obs-fs-file-interface	This header can be carried when you create a bucket as a parallel file system. Type: string Example: **x-obs-fs-file-interface:Enabled**	No
x-obs-epid	Enterprise project ID, which can be obtained from the enterprise project service. The value is a universally unique identifier (UUID). The value of a default enterprise project is **0** or does not contain this header. Users who have not enabled the enterprise project service do not need to carry this header either. Type: string Example: **x-obs-epid:9892d768-2d13-450f-aac7-ed0e44c2585f**	No

Request Elements

This request can use additional elements. For details about additional elements, see **Table 5-4**.

Table 5-4 Additional request elements

Element	Description	Mandatory
Location	Specifies the region where a bucket will be created. • When creating a bucket using the endpoint of the default region, note the following: – If **Location** is not specified, the bucket is created in the default region. – If Location is specified to other region, the bucket is created in the specified region. • When creating a bucket using the endpoint of a non-default region, **Location** must be specified to the region corresponding to the endpoint. For details about OBS regions and endpoints, see **Endpoints**. Type: string	No

Response Syntax

```
HTTP/1.1 status_code
Location: location
Date: date
Content-Length: length
```

Response Headers

The response to the request uses common headers. For details, see **Table 3-19**.

Response Elements

This response contains no elements.

Error Responses

No special error responses are returned. For details about error responses, see **Table 6-2**.

Sample Request: Creating a Bucket

```
PUT / HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
Date: WED, 01 Jul 2015 02:25:05 GMT
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:75/Y4Ng1izvzc1nTGxpMXTE6ynw=
Content-Length: 157

<CreateBucketConfiguration xmlns="http://obs.region.example.com/doc/2015-06-30/">
    <Location>region</Location>
</CreateBucketConfiguration>
```

Sample Response: Creating a Bucket

```
HTTP/1.1 200 OK
Server: OBS
x-obs-request-id: BF260000016435CE298386946AE4C482
Location: /examplebucket
x-obs-id-2: 32AAAQAAEAABSAAgAAEAABAAAQAAEAABCT9W2tcvLmMJ+plfdopaD62S0npbaRUz
Date: WED, 01 Jul 2015 02:25:06 GMT
Content-Length: 0
```

Sample Request: Creating a Bucket (with the ACL and Storage Class Specified)

```
PUT / HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
Date: WED, 01 Jul 2015 02:25:05 GMT
x-obs-acl:public-read
x-obs-storage-class:STANDARD
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:75/Y4Ng1izvzc1nTGxpMXTE6ynw=
Content-Length: 157

<CreateBucketConfiguration xmlns="http://obs.region.example.com/doc/2015-06-30/">
    <Location>region</Location>
</CreateBucketConfiguration>
```

Sample Response: Creating a Bucket (with the ACL and Storage Class Specified)

```
HTTP/1.1 200 OK
Server: OBS
x-obs-request-id: BF260000016435CE298386946AE4C482
Location: /examplebucket
x-obs-id-2: 32AAAQAAEAABSAAgAAEAABAAAQAAEAABCT9W2tcvLmMJ+plfdopaD62S0npbaRUz
Date: WED, 01 Jul 2015 02:25:06 GMT
Content-Length: 0
```

Sample Request: Creating a Parallel File System

```
PUT / HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
Date: WED, 01 Jul 2015 02:25:05 GMT
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:75/Y4Ng1izvzc1nTGxpMXTE6ynw=
Content-Length: 157
x-obs-fs-file-interface: Enabled

<CreateBucketConfiguration xmlns="http://obs.region.example.com/doc/2015-06-30/">
<Location>region</Location>
</CreateBucketConfiguration>
```


Sample Response: Creating a Parallel File System

```
HTTP/1.1 200 OK
Server: OBS
x-obs-request-id: BF260000016435CE298386946AE4C482
Location: /examplebucket
x-obs-id-2: 32AAAQAAEAABSAAgAAEAABAAAQAAEAABCT9W2tcvLmMJ+plfdopaD62S0npbaRUz
Date: WED, 01 Jul 2015 02:25:06 GMT
Content-Length: 0
```

5.1.3 Listing Objects in a Bucket

Functions

This operation lists objects in a bucket. To use this operation, you must have the permission to read the bucket.

If you specify only the bucket name in the request, OBS returns descriptions for some or all of the objects (a maximum of 1,000 objects) in the bucket. If you also specify one or more parameters among **prefix**, **marker**, **max-keys**, and **delimiter** in the request, OBS returns a list of objects based on the semantics specified in **Table 5-5**.

You can also add the **versions** parameter to the request to list multiple versions of an object in a bucket.

Request Syntax

```
GET / HTTP/1.1

Host: bucketname.obs.region.example.com
Date: date
Authorization: authorization
```

Request Syntax (for multi-version objects)

```
GET /?versions HTTP/1.1
Host: bucketname.obs.region.example.com
Date: date
Authorization: authorization
```

Request Parameters

This request uses parameters to list some objects in a bucket. **Table 5-5** describes the parameters.

Table 5-5 Request parameters

Parameter	Description	Mandatory
prefix	Lists objects that begin with the specified prefix. Type: string	No

Parameter	Description	Mandatory
marker	Specifies a marker when listing objects in a bucket. With a marker configured, objects after this marker will be returned in alphabetical order. This field is used only for listing objects. Type: string	No
max-keys	Specifies the maximum number (from **1** to **1000**) of objects returned (in alphabetical order) in the response. If the value is beyond this range, only 1,000 objects are returned by default. Type: integer	No
delimiter	Separator used to group object names. If a prefix is specified, objects with the same string from the prefix to the first delimiter are grouped into one **CommonPrefixes**. If no prefix is specified, objects with the same string from the first character to the first delimiter are grouped into one **CommonPrefixes**. For example, there are three objects (**abcd**, **abcde**, and **bbcde**) in a bucket. If **delimiter** is set to **d** and **prefix** is set to **a**, objects **abcd** and **abcde** are grouped into a **CommonPrefixes** with **abcd** as the prefix. If only **delimiter** is set to **d**, objects **abcd** and **abcde** are grouped into a **CommonPrefixes** with **abcd** as the prefix, and **bbcde** is grouped separately into another **CommonPrefixes** with **bbcd** as the prefix. For a parallel file system, if this parameter is not specified, all the content in the directory is recursively listed by default, and subdirectories are also listed. In big data scenarios, parallel file systems usually have deep directory levels and each directory has a large number of files. In such case, you are advised to configure **[delimiter=/]** to list the content in the current directory, but not list subdirectories, thereby improving the listing efficiency. Type: string	No
key-marker	Position to start with when objects are listed. This field is used only for listing versioned objects. Type: string Valid value: value of **NextKeyMarker** in the response body of the last request	No

Parameter	Description	Mandatory
version-id-marker	This parameter applies only when versioning is enabled. Specifies the version ID to start with when objects in a bucket are listed. Objects are listed in alphabetical order (a maximum of 1,000 objects are displayed at a time). This parameter is used together with the **key-marker** in the request. If the value of **version-id-marker** is not a version ID specified by **key-marker**, **version-id-marker** is invalid. Type: string Valid value: object version ID, that is, the value of **NextVersionIdMarker** in the response body of the last request	No

Request Headers

This request uses common request headers. For details, see **Table 3-3**.

Request Elements

This request contains no elements.

Response Syntax

```
HTTP/1.1 status_code
Date: date
x-obs-bucket-location: region
Content-Type: application/xml
Content-Length: length
<Response Body>
```

Response Headers

The response to the request uses common headers. For details, see **Table 3-19**.

Response Elements

This response lists objects in XML format. Specific elements are described in **Table 5-6**.

Table 5-6 Response elements

Element	Description
ListBucketResult	A list of objects in a bucket Type: XML

Element	Description
Contents	Object metadata Type: XML Parent: ListBucketResult
CommonPrefixes	Group information. If you specify a delimiter in the request, the response contains group information in **CommonPrefixes**. Type: XML Parent: ListBucketResult
Delimiter	The delimiter parameter specified in a request Type: string Parent: ListBucketResult
ETag	Base64-encoded 128-bit MD5 digest of an object. ETag is the unique identifier of the object content. It can be used to determine whether the object content is changed. For example, if the ETag value is **A** when an object is uploaded, but this value has changed to **B** when the object is downloaded, it indicates that the object content has been changed. The ETag value is a hash of the object. The ETag reflects changes to the object content, rather than the object metadata. An uploaded object or copied object has a unique ETag after being encrypted using MD5. (If the object is encrypted on the server side, the ETag value is not the MD5 digest of the object, but the unique identifier calculated through server-side encryption.) Type: string Parent: ListBucketResult.Contents
Type	Object type. This parameter is returned when the object type is not **Normal**. Type: string Parent: ListBucketResult.Contents
ID	Domain ID of the object owner Type: string Parent: ListBucketResult.Contents.Owner

Element	Description
IsTruncated	Determines whether the returned list of objects is truncated. The value **true** indicates that the list was truncated and **false** indicates that the list was not truncated. Type: boolean Parent: ListBucketResult
Key	Object name Type: string Parent: ListBucketResult.Contents
LastModified	Time (UTC) when an object was last modified Type: date Parent: ListBucketResult.Contents
Marker	Marker for the position from which objects in a bucket will be listed Type: string Parent: ListBucketResult
NextMarker	A marker for the last returned object in the list. **NextMarker** is returned when not all the objects are listed. You can set the **Marker** value to list the remaining objects in follow-up requests. Type: string Parent: ListBucketResult
MaxKeys	Maximum number of objects returned Type: string Parent: ListBucketResult
Name	Name of the requested bucket Type: string Parent: ListBucketResult
Owner	User information, including the domain ID and name of the object owner Type: XML Parent: ListBucketResult.Contents

Element	Description
DisplayName	Name of the object owner Type: string Parent: ListBucketResult.Contents.Owner
Prefix	Prefix of an object name. Only objects whose names have this prefix are listed. Type: string Parent: ListBucketResult
Size	Object size in bytes Type: string Parent: ListBucketResult.Contents
StorageClass	Storage class of an object Type: string Value options: **STANDARD**, **WARM**, **COLD** Parent: ListBucketResult.Contents

Table 5-7 Elements in the response message for listing multi-version objects.

Element	Description
ListVersionsResult	Container for the list of objects (including objects with multiple version IDs) Type: container
Name	Bucket name Type: string Parent: ListVersionsResult
Prefix	Prefix of an object name. Only objects whose names have this prefix are listed. Type: string Parent: ListVersionsResult
KeyMarker	Marker for the object key from which objects will be listed Type: string Parent: ListVersionsResult

Element	Description
VersionIdMarker	Object version ID to start with when objects are listed Type: string Parent: ListVersionsResult
NextKeyMarker	Key marker for the last returned object in the list. **NextKeyMarker** is returned when not all the objects are listed. You can set the **KeyMarker** value to list the remaining objects in follow-up requests. Type: string Parent: ListVersionsResult
NextVersionIdMarker	Version ID marker for the last returned object in the list. **NextVersionIdMarker** is returned when not all the objects are listed. You can set the **VersionIdMarker** value to list the remaining objects in follow-up requests. Type: string Parent: ListVersionsResult
MaxKeys	Maximum number of objects returned Type: string Parent: ListVersionsResult
IsTruncated	Indicates whether the returned list of objects is truncated. The value **true** indicates that the list was truncated and **false** indicates that the list was not truncated. Type: boolean Parent: ListVersionsResult
Version	Container of version information Type: container Parent: ListVersionsResult
DeleteMarker	Container for objects with delete markers Type: container Parent: ListVersionsResult

Element	Description
Key	Object name Type: string Parent: ListVersionsResult.Version | ListVersionsResult.DeleteMarker
VersionId	Object version ID Type: string Parent: ListVersionsResult.Version | ListVersionsResult.DeleteMarker
IsLatest	Whether the object is the latest version. If the parameter value is **true**, the object is the latest version. Type: boolean Parent: ListVersionsResult.Version | ListVersionsResult.DeleteMarker
LastModified	Time (UTC) when an object was last modified Type: date Parent: ListVersionsResult.Version | ListVersionsResult.DeleteMarker
ETag	Base64-encoded 128-bit MD5 digest of an object. ETag is the unique identifier of the object content. It can be used to determine whether the object content is changed. The actual ETag is the hash value of the object. For example, if the ETag value is **A** when an object is uploaded, but this value has changed to **B** when the object is downloaded, it indicates that the object content has been changed. The ETag reflects changes to the object content, rather than the object metadata. An uploaded object or copied object has a unique ETag after being encrypted using MD5. Type: string Parent: ListVersionsResult.Version
Type	Object type. This parameter is returned when the object type is not **Normal**. Type: string Parent: ListVersionsResult.Version

Element	Description
Size	Object size in bytes Type: string Parent: ListVersionsResult.Version
Owner	User information, including the domain ID and name of the object owner Type: container Parent: ListVersionsResult.Version | ListVersionsResult.DeleteMarker
ID	Domain ID of the object owner Type: string Parent: ListVersionsResult.Version.Owner | ListVersionsResult.DeleteMarker.Owner
DisplayName	Name of the object owner Type: string Parent: ListVersionsResult.Version.Owner | ListVersionsResult.DeleteMarker.Owner
StorageClass	Storage class of an object Type: string Value options: **STANDARD**, **WARM**, **COLD** Parent: ListVersionsResult.Version
CommonPrefixes	Group information. If you specify a delimiter in the request, the response contains group information in **CommonPrefixes**. Type: container Parent: ListVersionsResult
Prefix	Indicates a different prefix in the group information in **CommonPrefixes**. Type: string Parent: ListVersionsResult.CommonPrefixes

Error Responses

No special error responses are returned. For details about error responses, see **Table 6-2**.

Sample Request: Listing All Objects

```
GET / HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
Date: WED, 01 Jul 2015 02:28:25 GMT
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:KiyoYze4pmRNPYfmlXBfRTVxt8c=
```

Sample Response: Listing All Objects

```
HTTP/1.1 200 OK
Server: OBS
x-obs-request-id: BF260000016435D34E379ABD93320CB9
x-obs-id-2: 32AAAQAAEAABAAAQAAEAABAAAQAAEAABCSXiN7GPL/yXM6OSBaYCUV1zcY5OelWp
Content-Type: application/xml
Date: WED, 01 Jul 2015 02:23:30 GMT
Content-Length: 586

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ListBucketResult xmlns="http://obs.example.com/doc/2015-06-30/">
  <Name>examplebucket</Name>
  <Prefix/>
  <Marker/>
  <MaxKeys>1000</MaxKeys>
  <IsTruncated>false</IsTruncated>
  <Contents>
    <Key>object001</Key>
    <LastModified>2015-07-01T00:32:16.482Z</LastModified>
    <ETag>"2fa3bcaaec668adc5da177e67a122d7c"</ETag>
    <Size>12041</Size>
    <Owner>
      <ID>b4bf1b36d9ca43d984fbcb9491b6fce9</ID>
      <DisplayName>ObjectOwnerName</DisplayName>
    </Owner>
    <StorageClass>STANDARD</StorageClass>
  </Contents>
</ListBucketResult>
```

Sample Request: Listing Some Objects

Assume that you have a bucket **examplebucket** that contains objects **newfile**, **obj001**, **obj002**, and **obs001**. If you want to list only object **obj002**, the request message is as follows:

```
GET /?marker=obj001&prefix=obj HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
Date: WED, 01 Jul 2015 02:28:25 GMT
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:KiyoYze4pmRNPYfmlXBfRTVxt8c=
```

Sample Response: Listing Some Objects

```
HTTP/1.1 200 OK
Server: OBS
x-obs-request-id: BF260000016435D758FBA857E0801874
x-obs-id-2: 32AAAQAAEAABAAAQAAEAABAAAQAAEAABCShn/xAyk/xHBX6qgGSB36WXrbco0X80
Content-Type: application/xml
Date: WED, 01 Jul 2015 02:29:48 GMT
Content-Length: 707

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ListBucketResult xmlns="http://obs.example.com/doc/2015-06-30/">
<Name>examplebucket</Name>
<Prefix>obj</Prefix>
<Marker>obj001</Marker>
```



```
<MaxKeys>1000</MaxKeys>
<IsTruncated>false</IsTruncated>
  <Contents>
    <Key>obj002</Key>
    <LastModified>2015-07-01T02:11:19.775Z</LastModified>
    <ETag>"a72e382246ac83e86bd203389849e71d"</ETag>
    <Size>9</Size>
    <Owner>
      <ID>b4bf1b36d9ca43d984fbcb9491b6fce9</ID>
      <DisplayName>ObjectOwnerName</DisplayName>
    </Owner>
    <StorageClass>STANDARD</StorageClass>
  </Contents>
</ListBucketResult>
```

Sample Request: Listing Object Versions

```
GET /?versions HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
Date: WED, 01 Jul 2015 02:29:45 GMT
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:iZeDESIMxBK2YODk7vIeVpyO8Dl=
```

Sample Response: Listing Object Versions

```
HTTP/1.1 200 OK
Server: OBS
x-obs-request-id: BF260000016435D758FBA857E0801874
x-obs-id-2: 32AAAQAAEAABAAAQAAEAABAAAQAAEAABCShn/xAyk/xHBX6qgGSB36WXrbco0X80
Content-Type: application/xml
Date: WED, 01 Jul 2015 02:29:48 GMT
Content-Length: 707

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ListVersionsResult xmlns="http://obs.example.com/doc/2015-06-30/">
 <Name>bucket02</Name>
  <Prefix/>
  <KeyMarker/>
  <VersionIdMarker/>
  <MaxKeys>1000</MaxKeys>
  <IsTruncated>false</IsTruncated>
  <Version>
    <Key>object001</Key>
    <VersionId>00011000000000013F16000001643A22E476FFFF9046024ECA3655445346485a</VersionId>
    <IsLatest>true</IsLatest>
    <LastModified>2015-07-01T00:32:16.482Z</LastModified>
    <ETag>"2fa3bcaaec668adc5da177e67a122d7c"</ETag>
    <Size>12041</Size>
    <Owner>
      <ID>b4bf1b36d9ca43d984fbcb9491b6fce9</ID>
      <DisplayName>ObjectOwnerName</DisplayName>
    </Owner>
    <StorageClass>STANDARD</StorageClass>
  </Version>
</ListVersionsResult>
```

5.1.4 Obtaining Bucket Metadata

Functions

This operation queries the metadata of a bucket. To use this operation, you must have the permission to read the bucket.

Request Syntax

```
HEAD / HTTP/1.1
Host: bucketname.obs.region.example.com
Date: date
Authorization: authorization
```

Request Parameters

This request contains no parameters.

Request Headers

This request uses common headers. For details, see **Table 3-3**.

Table 5-8 lists the header fields required when obtaining CORS configuration information.

Table 5-8 Request headers for obtaining CORS configuration

Header	Description	Mandatory
Origin	Origin of the cross-domain request specified by the pre-request. Generally, it is a domain name. Type: string	Yes
Access-Control-Request-Headers	HTTP headers of a request. The request can use multiple HTTP headers. Type: string	No

Request Elements

This request contains no elements.

Response Syntax

```
HTTP/1.1 status_code
x-obs-bucket-location: region
Date: date
```

Response Headers

The response to the request uses common headers. For details, see **Table 3-19**.

In addition to the common response headers, the headers listed in **Table 5-9** may be used.

Table 5-9 Additional response headers

Header	Description
x-obs-bucket-location	The region where the bucket resides. Type: string
x-obs-storage-class	Default storage class of the bucket. The options are as follows: **STANDARD** (Standard), **WARM** (Warm), **COLD** (Cold). Type: string
x-obs-version	OBS version of the bucket. Type: string
x-obs-fs-file-interface	Indicates whether the bucket is a parallel file system. The value can be **Enabled** (parallel file system). If this header field is not carried, the bucket is not a parallel file system. Type: string
x-obs-epid	Enterprise project ID of the current bucket. Type: string
Access-Control-Allow-Origin	Indicates that the origin is included in the response if the origin in the request meets the CORS configuration requirements when CORS is configured for buckets. Type: string
Access-Control-Allow-Headers	Indicates that the headers are included in the response if headers in the request meet the CORS configuration requirements when CORS is configured for buckets. Type: string
Access-Control-Max-Age	Value of **MaxAgeSeconds** in the CORS configuration of the server when CORS is configured for buckets. Type: integer

Header	Description
Access-Control-Allow-Methods	Indicates that methods in the rule are included in the response if **Access-Control-Request-Method** in the request meets the CORS configuration requirements when CORS is configured for buckets. Type: string Value options: **GET**, **PUT**, **HEAD**, **POST**, **DELETE**
Access-Control-Expose-Headers	Value of **ExposeHeader** in the CORS configuration of a server when CORS is configured for buckets. Type: string

Response Elements

This response contains no elements.

Error Responses

No special error responses are returned. For details about error responses, see **Table 6-2**.

Sample Request: Getting CORS Configuration (with No Headers Specified)

```
HEAD / HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
Date: WED, 01 Jul 2015 02:30:25 GMT
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:niCQCuGIZpETKIyx1datxHZyYlk=
```

Sample Response: Getting CORS Configuration (with No Headers Specified)

```
HTTP/1.1 200 OK
Server: OBS
x-obs-request-id: BF260000016439C734E0788404623FA8
Content-Type: application/xml
x-obs-storage-class: STANDARD
x-obs-id-2: 32AAAQAAEAABAAAQAAEAABAAAQAAEAABCSxwLpq9Hzf3OnaXr+pI/OPLKdrtiQAF
Date: WED, 01 Jul 2015 02:30:25 GMT
x-obs-bucket-location: region
x-obs-version: 3.0
Content-Length: 0
```

Sample Request: Getting Bucket Metadata and CORS Configuration

```
HEAD / HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
Date: WED, 01 Jul 2015 02:30:25 GMT
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:niCQCuGIZpETKIyx1datxHZyYlk=
```



```
Origin:www.example.com
Access-Control-Request-Headers:AllowedHeader_1
```

Sample Response: Getting Bucket Metadata and CORS Configuration

```
HTTP/1.1 200 OK
Server: OBS
x-obs-request-id: BF260000016439C734E0788404623FA8
Content-Type: application/xml
x-obs-storage-class: STANDARD
x-obs-id-2: 32AAAQAAEAABAAAQAAEAABAAAQAAEAABCSxwLpq9Hzf3OnaXr+pI/OPLKdrtiQAF
Date: WED, 01 Jul 2015 02:30:25 GMT
x-obs-bucket-location: region
Access-Control-Allow-Origin: www.example.com
Access-Control-Allow-Methods: POST,GET,HEAD,PUT
Access-Control-Allow-Headers: AllowedHeader_1
Access-Control-Max-Age: 100
Access-Control-Expose-Headers: ExposeHeader_1
x-obs-version: 3.0
Content-Length: 0
```

5.1.5 Obtaining Bucket Location

Functions

This operation obtains the location of a bucket. To use this operation, you must have the permission to read the bucket.

Request Syntax

```
GET /?location HTTP/1.1
Host: bucketname.obs.region.example.com
Date: date
Authorization: authorization
```

Request Parameters

This request contains no parameters.

Request Headers

This request uses common headers. For details, see **Table 3-3**.

Request Elements

This request contains no elements.

Response Syntax

```
HTTP/1.1 status_code
Date: date
Content-Type: type
Content-Length: length

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Location xmlns="http://obs.region.example.com/doc/2015-06-30/">region</Location>
```

Response Headers

The response to the request uses common headers. For details, see **Table 3-19**.

Response Elements

This response contains elements of information about a bucket's region. **Table 5-10** describes the elements.

Table 5-10 Response elements

Element	Description
Location	Indicates the region where the bucket resides. Type: string

Error Responses

No special error responses are returned. For details about error responses, see **Table 6-2**.

Sample Request

```
GET /?location HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
Date: WED, 01 Jul 2015 02:30:25 GMT
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:1DrmbCV+lhz3zV7uywlj7lrh0MY=
```

Sample Response

```
HTTP/1.1 200 OK
Server: OBS
x-obs-request-id: BF260000016435D9F27CB2758E9B41A5
x-obs-id-2: 32AAAQAAEAABAAAQAAEAABAAAQAAEAABCSKWoJmaMyRXqofHgapbETDyI2LM9rUw
Content-Type: application/xml
Date: WED, 01 Jul 2015 02:30:25 GMT
Content-Length: 128

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Location xmlns="http://obs.region.example.com/doc/2015-06-30/">region</Location>
```

5.1.6 Deleting Buckets

Functions

This operation deletes specified buckets. This operation can be performed only by the bucket owner and users who have been authorized (via a policy) with the permission to delete the bucket. The bucket to be deleted must be an empty bucket. If a bucket has an object or a multipart task, the bucket is not empty. You can list objects and multipart upload tasks in a bucket to check whether the bucket is empty.

Note:

If the server returns a **5XX** error or times out when a bucket is being deleted, the system needs to synchronize the bucket information. During this period, the bucket information may be inaccurate. Therefore, wait a while and then check

whether the bucket is successfully deleted. If the bucket can still be queried, send the deletion request again.

Request Syntax

```
DELETE / HTTP/1.1
Host: bucketname.obs.region.example.com
Date: date
Authorization: authorization
```

Request Parameters

This request contains no parameters.

Request Headers

This request uses common request headers. For details, see **Table 3-3**.

Request Elements

This request involves no elements.

Response Syntax

```
HTTP/1.1 status_code
Date: date
```

Response Headers

The response to the request uses common headers. For details, see **Table 3-19**.

Response Elements

This response contains no elements.

Error Responses

No special error responses are returned. For details about error responses, see **Table 6-2**.

Sample Request

```
DELETE / HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
Date: WED, 01 Jul 2015 02:31:25 GMT
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:jZiAT8Vx4azWEvPRMWi0X5BpJMA=
```

Sample Response

```
HTTP/1.1 204 No Content
Server: OBS
x-obs-request-id: BF260000016435DE6D67C35F9B969C47
x-obs-id-2: 32AAAQAAEAABKAAQAAEAABAAAQAAEAABCTukraCnXLsb7lEw4ZKjzDWWhzXdgme3
Date: WED, 01 Jul 2015 02:31:25 GMT
```


5.2 Advanced Bucket Settings

5.2.1 Configuring a Bucket Policy

Functions

This operation creates or modifies policies for buckets. If the specified bucket already has a policy, the policy in the request will overwrite the existing one. There is no limit on the number of bucket policies (statements) for a bucket. However, the total size of JSON descriptions of all bucket policies in a bucket cannot exceed 20 KB.

To perform this operation, the user must be the bucket owner or the bucket owner's IAM user that has permissions required for configuring bucket policies.

Request Syntax

```
PUT /?policy HTTP/1.1
Host: bucketname.obs.region.example.com
Date: date
Authorization: signatureValue
Policy written in JSON
```

Request Parameters

This request contains no message parameters.

Request Headers

This request uses common headers. For details, see **Table 3-3**.

Request Elements

The request body is a JSON string that contains the bucket policy information.

Response Syntax

```
HTTP/1.1 status_code
Date: date
Content-Length: length
```

Response Headers

The response to the request uses common headers. For details, see **Table 3-19**.

Response Elements

This response contains no elements.

Error Responses

No special error responses are returned. For details, see **Table 6-2**.

Sample Request 1

Grant permissions to an OBS tenant.

Grant permissions to the tenant whose ID is **783fc6652cf246c096ea836694f71855**.

For details about how to obtain the tenant ID, see **Obtaining a Domain ID and a User ID**.

```
PUT /?policy HTTP/1.1
Host: examplebucket.obs.region.example.com
Date: WED, 01 Jul 2015 02:32:25 GMT
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:jZiAT8Vx4azWEvPRMWi0X5BpJMA=

{
   "Statement": [
      {
         "Sid": "Stmt1375240018061",
         "Action": [
            "GetBucketLogging"
         ],
         "Effect": "Allow",
         "Resource": "logging.bucket",
         "Principal": {
            "ID": [
               "domain/783fc6652cf246c096ea836694f71855:user/*"
            ]
         }
      }
   ]
}
```

Sample Response 1

```
HTTP/1.1 204 No Content
x-obs-request-id: 7B6DFC9BC71DD58B061285551605709
x-obs-id-2: N0I2REZDOUJDNzFERDU4QjA2MTI4NTU1MTYwNTcwOUFBQUFBQUFBYmJiYmJiYmJD
Date: WED, 01 Jul 2015 02:32:25 GMT
Content-Length: 0
Server: OBS
```

Sample Request 2

Grant permissions to an OBS user.

The user ID is **71f3901173514e6988115ea2c26d1999**, and the account ID is **783fc6652cf246c096ea836694f71855**.

For details about how to obtain the account ID and user ID, see **Obtaining a Domain ID and a User ID**.

```
PUT /?policy HTTP/1.1
Host: examplebucket.obs.region.example.com
Date: WED, 01 Jul 2015 02:33:28 GMT
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:jZiAT8Vx4azWEvPRMWi0X5BpJMA=

{
   "Statement": [
      {
         "Sid": "Stmt1375240018062",
         "Action": [
            "PutBucketLogging"
         ],
         "Effect": "Allow",
         "Resource": "examplebucket",
```



```
        "Principal": {
          "ID": [
            "domain/783fc6652cf246c096ea836694f71855:user/71f3901173514e6988115ea2c26d1999"
          ]
        }
      }
    ]
}
```

Sample Response 2

```
HTTP/1.1 204 No Content
x-obs-request-id: 7B6DFC9BC71DD58B061285551605709
x-obs-id-2: N0I2REZDOUJDNzFERDU4QjA2MTI4NTU1MTYwNTcwOUFBQUFBQUFBYmJiYmJiYmJD
Date: WED, 01 Jul 2015 02:33:28 GMT
Content-Length: 0
Server: OBS
```

Sample Request 3

Deny all users except the specified one all the operation permissions.

The user ID is **71f3901173514e6988115ea2c26d1999**, and the account ID is **783fc6652cf246c096ea836694f71855**.

For details about how to obtain the account ID and user ID, see **Obtaining a Domain ID and a User ID**.

```
PUT /?policy HTTP/1.1
Host: examplebucket.obs.region.example.com
Date: WED, 01 Jul 2015 02:34:34 GMT
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:jZiAT8Vx4azWEvPRMWi0X5BpJMA=

{
   "Statement": [
      {
         "Effect": "Deny",
         "Action": ["*"],
         "Resource": [
            "examplebucket/*",
            "examplebucket"
         ],
         "NotPrincipal": {
            "ID": [
               "domain/783fc6652cf246c096ea836694f71855:user/71f3901173514e6988115ea2c26d1999",
               "domain/783fc6652cf246c096ea836694f71855"
            ]
         }
      }
    ]
}
```

Sample Response 3

```
HTTP/1.1 204 No Content
x-obs-request-id: A603000001604A7DFE4A4AF31E301891
x-obs-id-2: BKOvGmTlt6sda5X4G89PuMO4fabObGYmnpRGkaMba1LqPt0fCACEuCMllAObRK1n
Date: WED, 01 Jul 2015 02:34:34 GMT
Content-Length: 0
Server: OBS
```

Sample Request 4

Request to allow only the specified domain name and external link requests that have no referer headers by using the URL validation whitelist.

URL validation whitelist: **http://storage.example.com**

```
PUT /?policy HTTP/1.1
Host: examplebucket.obs.region.example.com
Date: WED, 01 Jul 2015 02:34:34 GMT
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:jZiAT8Vx4azWEvPRMWi0X5BpJMA=

{
   "Statement": [{
      "Effect": "Deny",
      "Action": [
      "GetObject",
      "GetObjectVersion"
      ],
      "Principal": {
         "ID": ["*"]
      },
      "Resource": ["examplebucket/*"],
      "Condition": {
         "StringNotLike": {
            "Referer": [
            "http://storage.example.com*",
            "${null}"
            ]
         }
      }
   }]
}
```

Sample Response 4

```
HTTP/1.1 204 No Content
x-obs-request-id: A603000001604A7DFE4A4AF31E301891
x-obs-id-2: BKOvGmTlt6sda5X4G89PuMO4fabObGYmnpRGkaMba1LqPt0fCACEuCMllAObRK1n
Date: WED, 01 Jul 2015 02:34:34 GMT
Content-Length: 0
Server: OBS
```

5.2.2 Obtaining Bucket Policy Information

Functions

This operation uses the sub-resources of policy to return the policy information of a specified bucket.

To perform this operation, the user must be the bucket owner or the bucket owner's IAM user that has permissions required for obtaining bucket policies.

This operation cannot be performed in the following scenarios, and the 404 error code "NoSuchBucketPolicy" is returned:

- The specified bucket policy does not exist.
- The standard bucket policy is set to **Private** and no custom bucket policy is configured.

Request Syntax

```
GET /?policy HTTP/1.1
Host: bucketname.obs.region.example.com
Date: date
Authorization: authorization
```


Request Parameters

This request contains no message parameters.

Request Headers

This request uses common headers. For details, see **Table 3-3**.

Request Elements

This request involves no elements.

Response Syntax

```
HTTP/1.1 status_code
Content-Type: application/xml
Date: date
Policy Content
```

Response Headers

The response to the request uses common headers. For details, see **Table 3-19**.

Response Elements

The response body is a JSON string that contains the bucket policy information.

Error Responses

No special error responses are returned. For details, see **Table 6-2**.

Sample Request

```
GET /?policy HTTP/1.1
Host: examplebucket.obs.region.example.com
Date: WED, 01 Jul 2015 02:35:46 GMT
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:jZiAT8Vx4azWEvPRMWi0X5BpJMA=
```

Sample Response

```
HTTP/1.1 200 OK
x-obs-request-id: A603000001604A7DFE4A4AF31E301891
x-obs-id-2: BKOvGmTlt6sda5X4G89PuMO4fabObGYmnpRGkaMba1LqPt0fCACEuCMllAObRK1n
Date: WED, 01 Jul 2015 02:35:46 GMT
Content-Length: 509
Server: OBS

{
   "Statement":[
      {
         "Sid":"Stmt1375240018061",
         "Effect":"Allow",
         "Principal":{
            "ID":[
               "domain/domainiddomainiddomainiddo006666:user/useriduseriduseriduseridus004001",
               "domain/domainiddomainiddomainiddo006667:user/*"
            ]
         },
         "Action":[
            "*"
         ],
```



```
        "Resource":[
           "examplebucket"
        ]
     }
  ]
}
```

5.2.3 Deleting a Bucket Policy

Functions

This operation uses the policy sub-resources to delete the policy of a specified bucket.

To perform this operation, the user must be the bucket owner or the bucket owner's IAM user that has permissions required for deleting bucket policies.

The 204 error code "No Content" is returned regardless of whether a requested bucket policy exists or not.

Request Syntax

```
DELETE /?policy HTTP/1.1
Host: bucketname.obs.region.example.com
Date: date
Authorization: authorization
```

Request Parameters

This request contains no message parameters.

Request Headers

This request uses common headers. For details, see **Table 3-3**.

Request Elements

This request involves no elements.

Response Syntax

```
HTTP/1.1 status_code
Date: date
Content-Type: text/xml
Content-Length: length
```

Response Headers

The response to the request uses common headers. For details, see **Table 3-19**.

Response Elements

This response contains no elements.

Error Responses

No special error responses are returned. For details, see **Table 6-2**.

Sample Request

```
DELETE /?policy HTTP/1.1
Host: examplebucket.obs.region.example.com
Date: WED, 01 Jul 2015 02:36:06 GMT
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:jZiAT8Vx4azWEvPRMWi0X5BpJMA=
```

Sample Response

```
HTTP/1.1 204 No Content
x-obs-request-id: 9006000001643AAAF70BF6152D71BE8A
x-obs-id-2: 32AAAQAAEAABSAAgAAEAABAAAQAAEAABCSB4oWmNX3gVGGLr1cRPWjOhffEbq1XV
Date: WED, 01 Jul 2015 02:36:06 GMT
Server: OBS
```

5.2.4 Configuring a Bucket ACL

Functions

This operation controls access permissions for buckets. By default, only the creator of a bucket has the permission to read and write the bucket. You can also set other access permissions. For example, you can set a public read policy to grant the read permission to all users.

You can configure an ACL when creating a bucket, and modify or obtain the ACLs of existing buckets using the API operations. A bucket ACL supports a maximum of 100 grants. The PUT method is idempotent. With this method, a new bucket ACL will overwrite the previous bucket ACL. To modify or delete an ACL, you just need to create a new one using the PUT method.

Request Syntax

```
PUT /?acl HTTP/1.1
Host: bucketname.obs.region.example.com
Date: date
Authorization: authorization
Content-Type: application/xml
Content-Length: length

<AccessControlPolicy>
   <Owner>
      <ID>ID</ID>
   </Owner>
   <AccessControlList>
      <Grant>
         <Grantee>
            <ID>domainId</ID>
         </Grantee>
         <Permission>permission</Permission>
         <Delivered>false</Delivered>
      </Grant>
   </AccessControlList>
</AccessControlPolicy>
```

Request Parameters

This request contains no parameters.

Request Headers

You can change the ACL of a bucket by using the header settings. Each ACL configured with the header setting has a set of predefined grantees and

authorized permissions. If you want to authorize access permissions by adding the header to a request, you must add the following header and specify the value.

Table 5-11 Optional header for specifying canned ACLs

Name	Description	Mandatory
x-obs-acl	Uses the canned ACL for a bucket. Value options: **private**, **public-read**, **public-read-write**, **public-read-delivered**, **public-read-write-delivered** Type: string	No

Request Elements

This request carries ACL information in elements to specify an ACL. **Table 3-3** describes the elements.

Table 5-12 Additional request elements

Element	Description	Mandatory
Owner	Bucket owner information, including the ID Type: XML	Yes
ID	Account ID of the authorized user Type: string	Yes
Grant	Container for the grantee and the granted permissions A single bucket ACL can contain no more than 100 grants. Type: XML	No
Grantee	Grantee information Type: XML	No
Canned	Grants permissions to all users. Value range: Everyone Type: string	No

Element	Description	Mandatory
Delivered	Indicates whether the bucket ACL is applied to all objects in the bucket. Type: boolean Default value: **false**	No
Permission	Permissions to be granted. Value options: **READ**, **READ_ACP**, **WRITE**, **WRITE_ACP**, **FULL_CONTROL** Type: string	No
AccessControlList	Indicates an ACL, which consists of three elements: **Grant**, **Grantee**, and **Permission**. Type: XML	Yes

Response Syntax

```
HTTP/1.1 status_code
Date: date
Content-Length: length
```

Response Headers

The response to the request uses common headers. For details, see **Table 3-19**.

Response Elements

This response contains no elements.

Error Responses

No special error responses are returned. For details about error responses, see **Table 6-2**.

Sample Request

```
PUT /?acl HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
Date: WED, 01 Jul 2015 02:37:22 GMT
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:iqSPeUBl66PwXDApxjRKk6hlcN4=
Content-Length: 727

<AccessControlPolicy xmlns="http://obs.example.com/doc/2015-06-30/">
  <Owner>
    <ID>b4bf1b36d9ca43d984fbcb9491b6fce9</ID>
  </Owner>
  <AccessControlList>
    <Grant>
      <Grantee>
```



```
      <ID>b4bf1b36d9ca43d984fbcb9491b6fce9</ID>
    </Grantee>
    <Permission>FULL_CONTROL</Permission>
  </Grant>
  <Grant>
    <Grantee>
      <ID>783fc6652cf246c096ea836694f71855</ID>
    </Grantee>
    <Permission>READ</Permission>
    <Delivered>false</Delivered>
  </Grant>
  <Grant>
    <Grantee>
      <Canned>Everyone</Canned>
    </Grantee>
    <Permission>READ_ACP</Permission>
  </Grant>
 </AccessControlList>
</AccessControlPolicy>
```

Sample Response

```
HTTP/1.1 200 OK
Server: OBS
x-obs-request-id: BF2600000164361F2954B4D063164704
x-obs-id-2: 32AAAQAAEAABSAAgAAEAABAAAQAAEAABCT78HTIBuhe0FbtSptrb/akwELtwyPKs
Date: WED, 01 Jul 2015 02:37:22 GMT
Content-Length: 0
```

5.2.5 Obtaining Bucket ACL Information

Functions

This operation returns the ACL information of a bucket. To obtain the ACL of a bucket, you need to have the **READ_ACP** or **FULL_CONTROL** permission for the bucket.

Request Syntax

```
GET /?acl HTTP/1.1
Host: bucketname.obs.region.example.com
Date: date
Authorization: authorization
```

Request Parameters

This request contains no message parameters.

Request Headers

This request uses common headers. For details, see **Table 3-3**.

Request Elements

This request involves no elements.

Response Syntax

```
HTTP/1.1 status_code
Date: date
Content-Length: length
```



```
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<AccessControlPolicy xmlns="http://obs.region.example.com/doc/2015-06-30/">
   <Owner>
      <ID>id</ID>
   </Owner>
   <AccessControlList>
      <Grant>
         <Grantee>
            <ID>id</ID>
         </Grantee>
         <Permission>permission</Permission>
         <Delivered>false</Delivered>
      </Grant>
   </AccessControlList>
</AccessControlPolicy>
```

Response Headers

The response to the request uses common headers. For details, see **Table 3-19**.

Response Elements

This response returns information (in the form of elements) about the bucket ACL. **Table 5-13** describes the elements.

Table 5-13 Response elements

Element	Description
Owner	Bucket owner Type: XML
ID	Account ID Type: string
AccessControlList	Indicates the ACL that records all users who have permissions to access the bucket and the permissions granted to the users. Type: XML
Grant	Container for the grantee and the granted permissions Type: XML
Grantee	Grantee information Type: XML
Canned	Grants permissions to all users. Type: string. The value can only be **Everyone**.

Element	Description
Delivered	Indicates whether the bucket ACL is applied to objects in the bucket. Type: boolean
Permission	Grantee's permission for a bucket Type: string

Error Responses

No special error responses are returned. For details about error responses, see **Table 6-2**.

Sample Request

```
GET /?acl HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
Date: WED, 01 Jul 2015 02:39:28 GMT
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:X7HtzGsIEkzJbd8vo1DRu30vVrs=
```

Sample Response

```
HTTP/1.1 200 OK
Server: OBS
x-obs-request-id: BF260000016436B69D82F14E93528658
x-obs-id-2: 32AAAQAAEAABAAAQAAEAABAAAQAAEAABCSjTh8661+HF5y8uAnTOBIpNO133hji+
Content-Type: application/xml
Date: WED, 01 Jul 2015 02:39:28 GMT
Content-Length: 784

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<AccessControlPolicy xmlns="http://obs.example.com/doc/2015-06-30/">
  <Owner>
    <ID>b4bf1b36d9ca43d984fbcb9491b6fce9</ID>
  </Owner>
  <AccessControlList>
    <Grant>
      <Grantee>
        <ID>b4bf1b36d9ca43d984fbcb9491b6fce9</ID>
      </Grantee>
      <Permission>FULL_CONTROL</Permission>
    </Grant>
    <Grant>
      <Grantee>
        <ID>783fc6652cf246c096ea836694f71855</ID>
      </Grantee>
      <Permission>READ</Permission>
      <Delivered>false</Delivered>
    </Grant>
    <Grant>
      <Grantee>
        <Canned>Everyone</Canned>
      </Grantee>
      <Permission>READ_ACP</Permission>
    </Grant>
  </AccessControlList>
</AccessControlPolicy>
```


5.2.6 Configuring Logging for a Bucket

Functions

When a bucket is created, the logging function is not enabled by default. To generate logs recording operations on buckets, you need to enable the logging function for the bucket. After the logging function is enabled, a log is generated for each operation on a bucket and multiple logs are packed into a log file. When enabling the logging function, you need to specify a location where log files are stored. They can be stored in the bucket for which the logging is enabled, or in other buckets that you have the required permissions. However, the bucket where log files are stored and the bucket for which the logging is enabled must be in the same region.

Log files are generated by OBS and uploaded to the bucket where logs are stored. Therefore, OBS needs to be authorized to upload generated log files. Before configuring the logging function, you need to create an agency for OBS in IAM, the agency name is configured as a parameter of the bucket, and the logging function must be configured under the **LoggingEnabled** tag in the XML file. You only need to authorize the agency with the upload permissions for the target bucket.

Example of agency permissions

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

To disable the bucket logging function, upload a logging file with an empty **BucketLoggingStatus** tag.

By default, a bucket whose storage class is Warm or Cold cannot be used for storing log files. Stored log files occupy storage space in a bucket. Therefore, users are charged for the logging service based on the pricing for data storage.

CAUTION

If the target bucket has KMS encryption enabled, grant the agency access to KMS.

Request Syntax

```
PUT /?logging HTTP/1.1
Host: bucketname.obs.region.example.com
Date: date
Authorization: signatureValue
<?xml version="1.0" encoding="UTF-8"?>
```



```
<BucketLoggingStatus>
  <Agency>agency-name</Agency>
  <LoggingEnabled>
    <TargetBucket>mybucketlogs</TargetBucket>
    <TargetPrefix>mybucket-access_log-/</TargetPrefix>
    <TargetGrants>
      <Grant>
        <Grantee>
          <ID>domainID</ID>
        </Grantee>
        <Permission>READ</Permission>
      </Grant>
    </TargetGrants>
  </LoggingEnabled>
</BucketLoggingStatus>
```

Request Parameters

This request contains no message parameters.

Request Headers

This request uses common headers. For details, see **Table 3-3**.

Request Elements

Table 5-14 Request elements

Element	Description	Mandatory
BucketLoggingStatus	Container for logging status information Type: container	Yes
Agency	Name of the IAM agency created by the owner of the target bucket on IAM. Type: string	You must set this parameter when enabling the logging function. Do not set this parameter when disabling the logging function.
LoggingEnabled	Container for logging information. Present this element when enabling the logging function. Otherwise, absent it. You can add specific logging information in this element. Type: container	You must set this parameter when enabling the logging function. Do not set this parameter when disabling the logging function.

Element	Description	Mandatory
Grant	Container for the grantee and the grantee's logging permissions. It describes who has the permission to access the generated log files. Type: container	No
Grantee	Container for the user that is granted with the logging permission. Type: container	No
ID	Account ID of the authorized user, which is globally unique. Type: string	No
Permission	Permissions of the grantee to the generated logs. Type: string Value options: **FULL_CONTROL**, **READ**, **WRITE**	No
TargetBucket	When enabling the logging function, the owner of the bucket being logged can specify a target bucket to store the generated log files. Ensure that the bucket owner who configures the logging function has the **FULL_CONTROL** permission for the bucket that stores log files. Log files generated for multiple buckets can be stored in the same target bucket. If you do so, you need to specify different TargetPrefixes to classify logs for different buckets. Type: string	You must set this parameter when enabling the logging function. Do not set this parameter when disabling the logging function.

Element	Description	Mandatory
TargetPrefix	You can specify a prefix using this element so that log files are named with this prefix. Type: string	You must set this parameter when enabling the logging function. Do not set this parameter when disabling the logging function.
TargetGrants	Container for granting information. Type: container	No

Naming rules for access logs

```
<TargetPrefix>YYYY-mm-DD-HH-MM-SS-<UniqueString>
```

- *<TargetPrefix>* is the log name prefix specified by the user.
- YYYY-mm-DD-HH-MM-SS indicates the date and time when the log is generated.
- *<UniqueString>* indicates a character string generated by OBS.

The following is an example of a log file name:

```
bucket-log2015-06-29-12-22-07-N7MXLAF1BDG7MPDV
```

- **bucket-log** is the target prefix specified by the user.
- **2015-06-29-12-22-07** indicates the time when the log is generated.
- **N7MXLAF1BDG7MPDV** is a string automatically generated by OBS

Format of bucket access logs

The following shows an access log delivered to the target bucket:

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

Each access log contains the following information:

Table 5-15 Format of bucket access logs

Parameter	Example	Description
BucketOwner	787f2f92b20943998a4fe2ab75eb09b8	ID of the bucket owner
Bucket	bucket	Bucket name
Time	[13/Aug/2015:14:43:42 +0000]	Request timestamp in the *[dd/MMM/yyyy:HH:mm:ss Z]* format
Remote IP	xx.xx.xx.xx	Request IP address

Parameter	Example	Description
Requester	787f2f92b20943998a4fe2ab75eb09b8	ID of the requester • When an account initiates a request, this parameter value is the account ID. When an IAM user initiates a request, this parameter value is the ID of the account where the IAM user belongs. • When an anonymous user initiates a request, this parameter value is **Anonymous**.
RequestID	281599BACAD9376ECE141B842B94535B	Request ID
Operation	REST.GET.BUCKET.LOCATION	Operation
Key	-	Object name
Request-URI	GET /bucket?location HTTP/1.1	Request URI
HTTPStatus	200	Response code
ErrorCode	-	Error code
BytesSent	211	Size of the HTTP response, expressed in bytes
ObjectSize	-	Object size
TotalTime	6	Processing time on the server Unit: ms
Turn-AroundTime	6	Total request processing time Unit: ms
Referer	-	Referer header of the request
User-Agent	HttpClient	User-Agent header of the request
VersionID	-	Version ID contained in a request

Parameter	Example	Description
STSLogUrn	-	Federated authentication and agency information
StorageClass	STANDARD_IA	Current object storage class
TargetStorageClass	GLACIER	Storage class that the object will be transitioned to
DentryName	12456%2Ffile.txt	• For a parallel file system, this field represents an internal identifier of a file or directory. Its value consists of a parent directory's inode number and a file or directory name and is displayed in the URL-encoded format. • For a bucket, the value of this field is **-**.

Response Syntax

```
HTTP/1.1 status_code
Date: date
Content-Length: length
```

Response Headers

The response to the request uses common headers. For details, see **Table 3-19**.

Response Elements

This response contains no elements.

Error Responses

No special error responses are returned. For details about error responses, see **Table 6-2**.

Sample Request

```
PUT /?logging HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
Date: WED, 01 Jul 2015 02:40:06 GMT
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:mCOjER/L4ZZUY9qr6AOnkEiwvVk=
Content-Length: 528
```



```
<?xml version="1.0" encoding="UTF-8"?>
<BucketLoggingStatus>
  <Agency>agencyGrantPutLogging</Agency>
  <LoggingEnabled>
    <TargetBucket>log-bucket</TargetBucket>
    <TargetPrefix>mybucket-access_log-/</TargetPrefix>
    <TargetGrants>
      <Grant>
        <Grantee>
          <ID>783fc6652cf246c096ea836694f71855</ID>
        </Grantee>
        <Permission>READ</Permission>
      </Grant>
    </TargetGrants>
  </LoggingEnabled>
</BucketLoggingStatus>
```

Sample Response

```
HTTP/1.1 200 OK
Server: OBS
x-obs-request-id: BF26000001643663CE53B6AF31C619FD
x-obs-id-2: 32AAAQAAEAABSAAkpAIAABAAAQAAEAABCT9CjuOx8cETSRbqkm35s1dL/tLhRNdZ
Date: WED, 01 Jul 2015 02:40:06 GMT
Content-Length: 0
```

5.2.7 Obtaining a Bucket Logging Configuration

Functions

This operation queries the logging status of a bucket. It uses the logging sub-resource to return the logging status of a bucket.

Only the bucket owner or users granted the **GetBucketLogging** permission can query the bucket logging status.

Request Syntax

```
GET /?logging HTTP/1.1
Host: bucketname.obs.region.example.com
Date: date
Authorization: authorization
```

Request Parameters

This request contains no message parameters.

Request Headers

This request uses common headers. For details, see **Table 3-3**.

Request Elements

This request involves no elements.

Response Syntax

```
HTTP/1.1 status_code
Content-Type: application/xml
Date: date
Content-Length: length
```



```
<?xml version="1.0" encoding="UTF-8"?>
<BucketLoggingStatus xmlns="http://obs.region.example.com/doc/2015-06-30/">
<Agency>agency-name</Agency>
<LoggingEnabled>
   <TargetBucket>bucketName</TargetBucket>
   <TargetPrefix>prefix</TargetPrefix>
      <TargetGrants>
         <Grant>
            <Grantee>
               <ID>id</ID>
            </Grantee>
            <Permission>permission</Permission>
         </Grant>
      </TargetGrants>
   </LoggingEnabled>
</BucketLoggingStatus>
```

Response Headers

The response to the request uses common headers. For details, see **Table 3-19**.

Response Elements

This response contains elements to specify the bucket logging status. **Table 5-16** describes the elements.

Table 5-16 Response elements

Element	Description
BucketLoggingStatus	Container for logging status information Type: container
Agency	Name of the agency created by the owner of the logging bucket for uploading log files by OBS Type: string
LoggingEnabled	Container for logging information. This element enables or disables the logging function. Present this element when enabling the logging. Otherwise, absent it. Type: container
Grant	Container for the grantee and the granted permissions Type: container
Grantee	Container for the user that is granted with the logging permission Type: container
ID	Grantee domain ID, a globally unique ID Type: string

Element	Description
Permission	Logging permission granted to the grantee for a bucket. The bucket owner is automatically granted the **FULL_CONTROL** permission when creating the bucket. Logging permissions control access to different logs. Type: string Value options: **FULL_CONTROL**, **READ**, **WRITE**
TargetBucket	When enabling the logging function, the owner of the bucket being logged can specify a target bucket to store the generated log files. Log files generated for multiple buckets can be stored in the same target bucket. If you do so, you need to specify different TargetPrefixes to classify logs for different buckets. Type: string
TargetPrefix	You can specify a prefix using this element so that log files are named with this prefix. Type: string
TargetGrants	Container for granting information Type: container

Error Responses

No special error responses are returned. For details about error responses, see **Table 6-2**.

Sample Request

```
GET /?logging HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
Date: WED, 01 Jul 2015 02:42:46 GMT
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:hUk+jTnR07hcKwJh4ousF2E1U3E=
```

Sample Response

```
HTTP/1.1 200 OK
Server: OBS
x-obs-request-id: BF260000016436B8EEE7FBA2AA3335E3
x-obs-id-2: 32AAAQAAEAABAAAQAAEAABAAAQAAEAABCShuQJoWFpS77C8bOv1mqURv0UY+0ejx
Content-Type: application/xml
Date: WED, 01 Jul 2015 02:42:46 GMT
Content-Length: 429

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<BucketLoggingStatus xmlns="http://obs.example.com/doc/2015-06-30/">
  <Agency>agency-name</Agency>
  <LoggingEnabled>
    <TargetBucket>log-bucket</TargetBucket>
    <TargetPrefix>mybucket-access_log-/</TargetPrefix>
```



```
  <TargetGrants>
    <Grant>
      <Grantee>
        <ID>b4bf1b36d9ca43d984fbcb9491b6fce9</ID>
      </Grantee>
      <Permission>READ</Permission>
    </Grant>
  </TargetGrants>
 </LoggingEnabled>
</BucketLoggingStatus>
```

5.2.8 Configuring Bucket Lifecycle Rules

Functions

This operation configures lifecycle rules that can delete or migrate objects from a bucket at a specified time. Typical application scenarios:

- Delete periodically uploaded files. Some files uploaded periodically need only to be retained for only one week or one month.
- Delete files that are frequently accessed within a certain period of time but are seldom accessed afterward. You can archive these files and then schedule the time for deletion.
- The minimum time for the transition of the bucket storage to Warm or to Cold can be configured. The value ranges from **24** to **8640**.

You can perform this operation to create or update the lifecycle configuration of a bucket.

NOTE

- Expired objects deleted based on a lifecycle rule cannot be recovered.

To perform this operation, you must have the **PutLifecycleConfiguration** permission. By default, only the bucket owner can perform this operation. The bucket owner can grant the permission to other users by configuring the bucket policy or user policy.

The lifecycle configuration enables OBS to delete objects and transition object storage classes at a scheduled time. To prevent a user from doing so, the following permissions granted to the user must be revoked:

- DeleteObject
- DeleteObjectVersion
- PutLifecycleConfiguration

If you want to forbid a user to set the bucket lifecycle configuration, revoke the **PutLifecycleConfiguration** permission from the user.

Request Syntax

```
PUT /?lifecycle HTTP/1.1
Host: bucketname.obs.region.example.com
Content-Length: length
Date: date
Authorization: authorization
Content-MD5: MD5
<?xml version="1.0" encoding="UTF-8"?>
<LifecycleConfiguration>
```



```
  <Rule>
     <ID>id</ID>
     <Prefix>prefix</Prefix>
     <Status>status</Status>
     <Expiration>
        <Days>days</Days>
     </Expiration>
     <NoncurrentVersionExpiration>
        <NoncurrentDays>days</NoncurrentDays>
     </NoncurrentVersionExpiration>
     <Transition>
      <Days>30</Days>
       <StorageClass>WARM</StorageClass>
     </Transition>
     <Transition>
      <Days>60</Days>
      <StorageClass>COLD</StorageClass>
     </Transition>
     <NoncurrentVersionTransition>
      <NoncurrentDays>30</NoncurrentDays>
      <StorageClass>WARM</StorageClass>
     </NoncurrentVersionTransition>
     <NoncurrentVersionTransition>
      <NoncurrentDays>60</NoncurrentDays>
      <StorageClass>COLD</StorageClass>
     </NoncurrentVersionTransition>
  </Rule>
</LifecycleConfiguration>
```

Request Parameters

This request contains no parameters.

Request Headers

Table 5-17 lists the request header.

Table 5-17 Request headers

Header	Description	Mandatory
Content-MD5	Base64-encoded 128-bit MD5 digest of the message according to RFC 1864. Type: string Example: **n58IG6hfM7vqI4K0vnWpog==**	Yes

Request Elements

In this request body, you need to specify the lifecycle configuration in XML format. **Table 5-18** describes the specific configuration elements.

- If the versioning of a bucket is enabled or suspended, you can set **NoncurrentVersionTransition** or **NoncurrentVersionExpiration** to control the lifecycle of historical object versions. The lifecycle of a historical version depends on the time when it becomes a historical one (time when the version is replaced by a new version) and the value of **NoncurrentDays**. For object deletion, if **NoncurrentDays** is set to **1**, an object version will be deleted only after it becomes a historical one for one day. If the version V1 of object A is

created on the first date of a month and new version V2 is uploaded on the fifth date of the month, V1 becomes a historical version. At 00:00 on the seventh date of the month, V1 will expire. If an object version does not meet the deletion conditions, but **NoncurrentDays** is set to **1** and **StorageClass** is set to **WARM**, the version transitions to the Warm storage class one day after it has become a historical version. For example, the V1 version of object A is created on the first day of a month, and its new version V2 is uploaded on the fifth day of the month. Then V1 becomes a historical version. One day later, that is, at 0 o'clock of the seventh day, V1 transitions to the Warm storage class. The deletion or transition of the object after the expiration time may be delayed. The delay is within 48 hours.

- Objects are processed according to the following procedures, if their latest versions meet the expiration rule and versioning is enabled or suspended for the bucket.
  - Versioning enabled:

    If the latest object version is not a delete marker, a new delete marker will be inserted for the object.

    If the latest object version is a delete marker and is the only version of the object, this latest version will be deleted.

    If the object of the latest version has the DeleteMarker and the object has other versions, all versions of the object remain unchanged.
  - Versioning suspended:

    If the latest version of the object does not have the DeleteMarker and is not the null version, the object generates a new DeleteMarker for the null version.

    If the latest version of the object does not have the DeleteMarker but is the null version, this null version is overwritten by a new DeleteMarker generated for the null version.

    If the latest object version is a delete marker and is the only version of the object, this latest version will be deleted.

    If the object of the latest version has the DeleteMarker and the object has other versions, all versions of the object remain unchanged.
- The following lists the processing when the versioning is enabled or suspended for a bucket and objects of the latest versions meet the transition rules:
  - If the latest version of the object has the DeleteMarker, the storage class of this version will not be transitioned.
  - If the latest version of the object does not have the DeleteMarker and meets the transition rule, the storage class of this version will be transitioned.

Table 5-18 Response elements for lifecycle configuration

Name	Description	Mandatory
Date	Specifies that OBS executes lifecycle rules for objects before the specified date. The date must be compliant with the ISO8601 format, and the time must be compliant with the UTC format of 00:00:00. For example, **2018-01-01T00:00:00.000Z** indicates that objects whose last modification time is earlier than **2018-01-01T00:00:00.000Z** are deleted or transitioned to another storage class. Objects whose last modification time is equal to or later than the specified time are not deleted or transitioned to another storage class. Type: string Parent: Expiration, Transition	Required if the **Days** element is absent.
Days	Specifies the number of days (since the latest update to the latest object version) after which the lifecycle rule takes effect. Type: integer Parent: Expiration, Transition	Required if the **Date** element is absent.
StorageClass	The storage class to which the object is transitioned. Type: string Value options: **WARM**, **COLD** Parent: Transition, NoncurrentVersion-Transition	Required if the **Transition** or **NoncurrentVersionTransition** element is present.
Transition	Transition time and the object storage class after transition (valid only for the latest object version). Type: XML Child: Date or Days, StorageClass Parent: Rule	Required if the **NoncurrentVersionTransition**, **Expiration**, or **NoncurrentVersionExpiration** element is absent.

Name	Description	Mandatory
Expiration	Container for the object expiration rule (only applicable to the latest versions of objects). Type: XML Child: Date or Days Parent: Rule	Required if **Transition**, **NoncurrentVersionTransition**, or **NoncurrentVersionExpiration** is absent.
ID	Unique identifier of a rule. The value can contain a maximum of 255 characters. Type: string Parent: Rule	No
LifecycleConfiguration	Container for lifecycle rules. You can add multiple rules. The total size of the rules cannot exceed 20 KB. Type: XML Child: Rule Parent: none	Yes
NoncurrentDays	Number of days when the specified rule takes effect after the object becomes a historical version (only applicable to an object's historical version). Type: integer Parent: NoncurrentVersionExpiration, NoncurrentVersionTransition	Required if the **NoncurrentVersionExpiration** or **NoncurrentVersionTransition** element is present.
NoncurrentVersionTransition	Transition time of historical object versions and the object storage class after transition. Type: XML Child: NoncurrentDays, StorageClass Parent: Rule	Required if the **Transition**, **Expiration**, or **NoncurrentVersionExpiration** element is absent.

Name	Description	Mandatory
NoncurrentVersionExpiration	Container for the expiration time of objects' historical versions. If versioning is enabled or suspended for a bucket, you can set **NoncurrentVersionExpiration** to delete historical versions of objects that match the lifecycle rule (only applicable to the historical versions of objects). Type: XML Child: NoncurrentDays Parent: Rule	No
Prefix	Object name prefix that identifies one or more objects to which the rule applies. Type: string Parent: Rule Constraints: 1. When you configure a lifecycle rule by specifying a prefix, if the specified prefix and the prefix of an existing lifecycle rule overlap, OBS regards these two rules as one and forbids you to configure this rule. For example, if there is a rule with the object prefix **abc** configured in the system, another rule with the object prefix starting with **abc** cannot be configured. 2. If there is already a lifecycle rule that is based on an object prefix, you are not allowed to configure another rule that is applied to the entire bucket.	Yes
Rule	Container for a specific lifecycle rule. Type: container Parent: LifecycleConfiguration	Yes
Status	Indicates whether the rule is enabled. Type: string Parent: Rule Value options: **Enabled**, **Disabled**	Yes

Response Syntax

```
HTTP/1.1 status_code
Date: date
Content-Length: length
```


Response Headers

The response to the request uses common headers. For details, see **Table 3-19**.

Response Elements

This response contains no elements.

Error Responses

No special error responses are returned. For details about error responses, see **Table 6-2**.

Sample Request

```
PUT /?lifecycle HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
Date: WED, 01 Jul 2015 03:05:34 GMT
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:DpSAlmLX/BTdjxU5HOEwflhM0WI=
Content-MD5: ujCZn5p3fmczNiQQxdsGaQ==
Content-Length: 919

<?xml version="1.0" encoding="utf-8"?>
<LifecycleConfiguration>
  <Rule>
    <ID>delete-2-days</ID>
    <Prefix>test/</Prefix>
    <Status>Enabled</Status>
    <Expiration>
      <Days>70</Days>
    </Expiration>
    <NoncurrentVersionExpiration>
      <NoncurrentDays>70</NoncurrentDays>
    </NoncurrentVersionExpiration>
    <Transition>
      <Days>30</Days>
      <StorageClass>WARM</StorageClass>
    </Transition>
    <Transition>
      <Days>60</Days>
      <StorageClass>COLD</StorageClass>
    </Transition>
    <NoncurrentVersionTransition>
      <NoncurrentDays>30</NoncurrentDays>
      <StorageClass>WARM</StorageClass>
    </NoncurrentVersionTransition>
    <NoncurrentVersionTransition>
      <NoncurrentDays>60</NoncurrentDays>
      <StorageClass>COLD</StorageClass>
    </NoncurrentVersionTransition>
  </Rule>
</LifecycleConfiguration>
```

Sample Response

```
HTTP/1.1 200 OK
Server: OBS
x-obs-request-id: BF26000001643670AC06E7B9A7767921
x-obs-id-2: 32AAAQAAEAABSAAgAAEAABAAAQAAEAABCSvK6z8HV6nrJh49gsB5vqzpgtohkiFm
Date: WED, 01 Jul 2015 03:05:34 GMT
Content-Length: 0
```


5.2.9 Obtaining Bucket Lifecycle Configuration

Functions

This operation obtains the bucket lifecycle configuration.

To perform this operation, you must have the **GetLifecycleConfiguration** permission. By default, only the bucket owner can perform this operation. The bucket owner can grant the permission to other users by configuring the bucket policy or user policy.

Request Syntax

```
GET /?lifecycle HTTP/1.1
Host: bucketname.obs.region.example.com
Date: date
Authorization: authorization
```

Request Parameters

This request contains no message parameters.

Request Headers

This request uses common headers. For details, see **Table 3-3**.

Request Elements

This request involves no elements.

Response Syntax

```
HTTP/1.1 status_code
Date: date
Content-Type: application/xml
Date: date
Content-Length: length

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<LifecycleConfiguration xmlns="http://obs.region.example.com/doc/2015-06-30/">
   <Rule>
      <ID>id</ID>
      <Prefix>prefix</Prefix>
      <Status>status</Status>
      <Expiration>
         <Date>date</Date>
      </Expiration>
      <NoncurrentVersionExpiration>
         <NoncurrentDays>days</NoncurrentDays>
      </NoncurrentVersionExpiration>
      <Transition>
       <Date>date</Date>
       <StorageClass>WARM</StorageClass>
      </Transition>
      <Transition>
       <Date>date</Date>
       <StorageClass>COLD</StorageClass>
      </Transition>
      <NoncurrentVersionTransition>
       <NoncurrentDays>30</NoncurrentDays>
       <StorageClass>WARM</StorageClass>
```



```
      </NoncurrentVersionTransition>
      <NoncurrentVersionTransition>
       <NoncurrentDays>60</NoncurrentDays>
       <StorageClass>COLD</StorageClass>
      </NoncurrentVersionTransition>
   </Rule>
</LifecycleConfiguration>
```

Response Headers

The response to the request uses common headers. For details, see **Table 3-19**.

Response Elements

This response contains elements to detail the configuration. **Table 5-19** describes the elements.

Table 5-19 Response elements for lifecycle configuration

Element	Description
Date	Specifies that OBS executes lifecycle rules for objects before the specified date. The date must be compliant with the ISO8601 format, and the time must be compliant with the UTC format of 00:00:00. For example, **2018-01-01T00:00:00.000Z** indicates that objects whose last modification time is earlier than **2018-01-01T00:00:00.000Z** are deleted or transitioned to another storage class. Objects whose last modification time is equal to or later than the specified time are not deleted or transitioned to another storage class. Type: string Parent: Expiration, Transition
Days	Specifies the number of days (since the latest update to the latest object version) after which the lifecycle rule is executed. Type: integer Parent: Expiration, Transition
StorageClass	The storage class to which the object is transitioned. Type: string Value options: **WARM**, **COLD** Parent: Transition, NoncurrentVersionTransition

Element	Description
Transition	Transition time and the object storage class after transition (valid only for the latest object version). Type: XML Child: Date or Days Parent: Rule
Expiration	Container for the object expiration rule. Type: XML Child: Date or Days Parent: Rule
ID	Unique identifier of a rule. The value can contain a maximum of 255 characters. Type: string Parent: Rule
LifecycleConfiguration	Container for lifecycle rules. You can add multiple rules. The total size of the rules cannot exceed 20 KB. Type: XML Child: Rule Parent: none
NoncurrentDays	Number of days when the specified rule takes effect after the object becomes a historical version. Type: integer Parent: NoncurrentVersionExpiration, NoncurrentVersionTransition
NoncurrentVersionTransition	Transition time of historical object versions and the object storage class after transition. Type: XML Child: NoncurrentDays, StorageClass Parent: Rule
NoncurrentVersionExpiration	Container for the expiration time of objects' historical versions. If versioning is enabled or suspended for a bucket, you can set **NoncurrentVersionExpiration** to delete objects whose life cycles have expired. Type: XML Child: NoncurrentDays Parent: Rule

Element	Description
Prefix	Object name prefix identifying one or more objects to which the rule applies. Type: string Parent: Rule
Rule	Container for a specific lifecycle rule. Type: container Parent: LifecycleConfiguration
Status	Indicates whether the rule is enabled. Type: string Parent: Rule Value options: **Enabled**, **Disabled**

Error Responses

Table 5-20 describes possible special errors in the request.

Table 5-20 Special error

Error Code	Description	HTTP Status Code
NoSuchLifecycleConfiguration	The bucket lifecycle configuration does not exist.	404 Not Found

For other errors, see **Table 6-2**.

Sample Request

```
GET /?lifecycle HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
Date: WED, 01 Jul 2015 03:06:56 GMT
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:/Nof9FCNANfzIXDS0NDp1IfDu8I=
```

Sample Response

```
HTTP/1.1 200 OK
Server: OBS
x-obs-request-id: BF260000016436BA5684FF5A10370EDB
x-obs-id-2: 32AAAQAAEAABAAAQAAEAABAAAQAAEAABCSEMKZSIeboCA1eAukgYOOAd7oX3ZONn
Content-Type: application/xml
Date: WED, 01 Jul 2015 03:06:56 GMT
Content-Length: 919

<?xml version="1.0" encoding="utf-8"?>
<LifecycleConfiguration>
  <Rule>
    <ID>delete-2-days</ID>
```



```
  <Status>Enabled</Status>
  <Expiration>
    <Days>2</Days>
  </Expiration>
  <NoncurrentVersionExpiration>
    <NoncurrentDays>5</NoncurrentDays>
  </NoncurrentVersionExpiration>
  <Transition>
    <Days>30</Days>
    <StorageClass>WARM</StorageClass>
  </Transition>
  <Transition>
    <Days>60</Days>
    <StorageClass>COLD</StorageClass>
  </Transition>
  <NoncurrentVersionTransition>
    <NoncurrentDays>30</NoncurrentDays>
    <StorageClass>WARM</StorageClass>
  </NoncurrentVersionTransition>
  <NoncurrentVersionTransition>
    <NoncurrentDays>60</NoncurrentDays>
    <StorageClass>COLD</StorageClass>
  </NoncurrentVersionTransition>
 </Rule>
</LifecycleConfiguration>
```

5.2.10 Deleting Lifecycle Rules

Functions

This operation deletes the lifecycle configuration of a bucket. After the lifecycle configuration of a bucket is deleted, OBS will not automatically delete objects in that bucket.

To perform this operation, you must have the **PutLifecycleConfiguration** permission. By default, only the bucket owner can perform this operation. The bucket owner can grant the permission to other users by configuring the bucket policy or user policy.

Request Syntax

```
DELETE /?lifecycle HTTP/1.1
Host: bucketname.obs.region.example.com
Date: date
Authorization: Authorization
```

Request Parameters

This request contains no message parameters.

Request Headers

This request uses common headers. For details, see **Table 3-3**.

Request Elements

This request involves no elements.

Response Syntax

```
HTTP/1.1 status_code
Date: date
```



```
Content-Type: text/xml
Date: date
```

Response Headers

The response to the request uses common headers. For details, see **Table 3-19**.

Response Elements

This response contains no elements.

Error Responses

No special error responses are returned. For details about error responses, see **Table 6-2**.

Sample Request

```
DELETE /?lifecycle HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
Date: WED, 01 Jul 2015 03:12:22 GMT
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:5DGAS7SBbMC1YTC4tNXY57Zl2Fo=
```

Sample Response

```
HTTP/1.1 204 No Content
Server: OBS
x-obs-request-id: BF260000016436C2550A1EEA97614A98
x-obs-id-2: 32AAAQAAEAABSAAgAAEAABAAAQAAEAABCSB7A0KZEBOCutgcfZvaGVthTGOJSuyk
Date: WED, 01 Jul 2015 03:12:22 GMT
```

5.2.11 Configuring Versioning for a Bucket

Functions

This operation restores an object that is mistakenly overwritten or deleted. You can use versioning to save, query, and restore objects of different versions. Versioning allows you to easily recover lost data due to misoperations or program faults. Versioning can also be used for retaining and archiving data.

By default, versioning is disabled for a bucket.

You can perform this operation to enable or suspend versioning for a bucket.

After versioning is enabled for a bucket:

- OBS creates a unique version ID for each uploaded object. Namesake objects are not overwritten and are distinguished by their own version IDs.
- You can download objects by specifying version IDs. By default, the latest object is downloaded if the version ID is not specified.
- You can specify a version ID to permanently delete a specific object. If an object is deleted with no version ID specified, only a delete marker with a unique version ID is generated, but the object is not physically deleted.

- The latest objects in a bucket are returned by default after a GET Object request. You can also send a request to obtain a bucket's objects with all version IDs.
- Except delete markers, storage space occupied by objects with all version IDs, excluding object metadata, is billed.

After versioning is suspended for a bucket:

- Existing objects with version IDs are not affected.
- The system creates version ID **null** to an uploaded object and the object will be overwritten after a namesake one is uploaded.
- You can download objects by specifying version IDs. By default, the latest object is downloaded if the version ID is not specified.
- You can specify a version ID to delete a specific object. If an object is deleted with no version ID specified, OBS creates a delete marker with a version ID of **null** and deletes the object whose version ID is **null**.
- Except delete markers, storage space occupied by objects with all version IDs, excluding object metadata, is billed.

Only the bucket owner can set versioning for the bucket.

Request Syntax

```
PUT /?versioning HTTP/1.1
Host: bucketname.obs.region.example.com
Date: date
Authorization: authorization
Content-Length: length

<VersioningConfiguration>
   <Status>status</Status>
</VersioningConfiguration>
```

Request Parameters

This request contains no parameters.

Request Headers

This request uses common headers. For details, see **Table 3-3**.

Request Elements

This request contains elements to configure the bucket versioning in XML format. **Table 5-21** lists the request elements.

Table 5-21 Elements for configuring bucket versioning

Element	Description	Mandatory
VersioningConfiguration	Root node for configuring versioning Parent: none	Yes

Element	Description	Mandatory
Status	Versioning status of the bucket Type: string Parent: VersioningConfiguration Value options: **Enabled**, **Suspended**	Yes

Response Syntax

```
HTTP/1.1 status_code
Date: date

Content-Length: length
```

Response Headers

The response to the request uses common headers. For details, see **Table 3-19**.

Response Elements

This response contains no elements.

Error Responses

No special error responses are returned. For details about error responses, see **Table 6-2**.

Sample Request

```
PUT /?versioning HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
Date: WED, 01 Jul 2015 03:14:18 GMT
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:sc2PM13Wlfcoc/YZLK0MwsI2Zpo=
Content-Length: 89

<VersioningConfiguration>
   <Status>Enabled</Status>
</VersioningConfiguration>
```

Sample Response

```
HTTP/1.1 200 OK
Server: OBS
x-obs-request-id: BF26000001643672B973EEBC5FBBF909
x-obs-id-2: 32AAAQAAEAABSAAgAAEAABAAAQAAEAABCSH6rPRHjQCa62fcNpCCPs7+1Aq/hKzE
Date: Date: WED, 01 Jul 2015 03:14:18 GMT
Content-Length: 0
```

5.2.12 Obtaining Bucket Versioning Status

Functions

This operation allows a bucket owner to get the versioning status of the bucket.

If versioning is not configured for a bucket, no versioning status information will be returned following this operation.

Request Syntax

```
GET /?versioning HTTP/1.1
Host: bucketname.obs.region.example.com
Date: date
Authorization: authorization
```

Request Parameters

This request contains no message parameters.

Request Headers

This request uses common headers. For details, see **Table 3-3**.

Request Elements

This request involves no elements.

Response Syntax

```
HTTP/1.1 status_code
Date: date
Content-Type: type
Content-Length: length

<VersioningConfiguration xmlns="http://obs.region.example.com/doc/2015-06-30/">
   <Status>status</Status>
</VersioningConfiguration>
```

Response Headers

The response to the request uses common headers. For details, see **Table 3-19**.

Response Elements

This response contains elements to specify the bucket versioning status. **Table 5-22** describes the elements.

Table 5-22 Response elements

Element	Description
VersioningConfiguration	Element of versioning status information. Type: container
Status	Versioning status of the bucket. Type: string Value options: **Enabled**, **Suspended**

Error Responses

No special error responses are returned. For details about error responses, see **Table 6-2**.

Sample Request

```
GET /?versioning HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
Date: WED, 01 Jul 2015 03:15:20 GMT
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:4N5qQIoluLO9xMY0m+8lIn/UWXM=
```

Sample Response

```
HTTP/1.1 200 OK
Server: OBS
x-obs-request-id: BF260000016436BBA4930622B4FC9F17
x-obs-id-2: 32AAAQAAEAABAAAQAAEAABAAAQAAEAABCSQIrNJ5/Ag6EPN8DAwWlPWgBc/xfBnx
Content-Type: application/xml
Date: WED, 01 Jul 2015 03:15:20 GMT
Content-Length: 180

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<VersioningConfiguration xmlns="http://obs.example.com/doc/2015-06-30/">
  <Status>Enabled</Status>
</VersioningConfiguration>
```

5.2.13 Configuring Event Notification for a Bucket

Functions

This operation notifies users of their operations on buckets, allowing users know events happened on buckets in a timely manner.

By default, the notification function of a bucket is not enabled, and the **NotificationConfiguration** element is **null**. If you want to disable the function, set the **NotificationConfiguration** element to **null**.

```
<NotificationConfiguration>
</NotificationConfiguration>
```

After receiving a request for configuring event notification, OBS verifies whether the specified SMN topic exists and whether the topic is authorized to OBS. If the topic exists and is authorized to OBS, OBS sends a test notification to the topic subscriber.

To perform this operation, you must have the **PutBucketNotification** permission. By default, the permission is granted to the bucket owner only. However, it can be granted to other users by configuring the bucket policy.

Request Syntax

```
PUT /?notification HTTP/1.1
Host: bucketname.obs.region.example.com
Date: date
Authorization: authorization string

<NotificationConfiguration>
   <TopicConfiguration>
      <Id>ConfigurationId</Id>
```



```
    <Filter>
      <Object>
        <FilterRule>
          <Name>prefix</Name>
          <Value>prefix-value</Value>
        </FilterRule>
        <FilterRule>
          <Name>suffix</Name>
          <Value>suffix-value</Value>
        </FilterRule>
      </Object>
    </Filter>
    <Topic>TopicARN</Topic>
    <Event>event-type</Event>
    <Event>event-type</Event>
    ...
  </TopicConfiguration>
  ...
</NotificationConfiguration>
```

Request Parameters

This request contains no message parameters.

Request Headers

This request uses common headers. For details, see **Table 3-3**.

Request Elements

This request contains elements to specify the notification configuration for the bucket in XML format. For details about the configuration elements, see **Table 5-23**.

Table 5-23 Request elements for notification function configuration

Element	Description	Mandatory
NotificationConfiguration	Root element for configuring the event notification function of a bucket. If the sub element is **null**, the function is disabled. Type: container Parent: none Child: zero or multiple TopicConfiguration elements	Yes
TopicConfiguration	Element for configuring the event notification topic. Type: container Parent: NotificationConfiguration Child: Id, Filter, Topic, and one or more Event elements	No

Element	Description	Mandatory
Topic	URN of the event notification topic. When OBS detects a specific event in the bucket, it publishes a notification message to the topic. The topic value can be found in SMN topics. Type: string Parent: TopicConfiguration Template: <Topic>urn:smn:region:project_id:smn_topic</Topic> Example: <Topic>urn:smn:*exampleRegion*:d745b885f14941369b2d2138e7a65bef:obs_test</Topic>	Required if **TopicConfiguration** is added
Id	Unique ID of each event notification. If the user does not specify an ID, the system assigns an ID automatically. Type: string Parent: TopicConfiguration	No
Filter	Element used to store rules of filtering object names. Type: container Parent: TopicConfiguration Child: Object	No
Object	Element that defines the filtering rule. The rule filters objects based on the prefixes and suffixes of object names. Type: container Parent: Filter Child: one or more FilterRule elements	No
FilterRule	Element that defines key-value pairs of the filtering rule Type: container Parent: Object Child: Name and Value	No
Name	Prefix or suffix of object names for filtering Type: string Parent: FilterRule Value options: **prefix**, **suffix**	No

Element	Description	Mandatory
Value	Key word of object names. Based on the prefix or suffix defined by **Name**, enter the key word for filtering objects. A longer string of characters delivers a more accurate filtering result. A maximum of 1024 characters are supported. Type: string Parent: FilterRule	No
Event	Type of events that need to be notified **NOTE** Multiple event types can be added in one TopicConfiguration element. Type: string Value options: The following values can be used to upload an object: • ObjectCreated:Put • ObjectCreated:Post • ObjectCreated:Copy • ObjectCreated:CompleteMultipartUpload Or use wildcard characters to support all upload operations: • ObjectCreated:* The following values can be used to delete an object: • ObjectRemoved:Delete • ObjectRemoved:DeleteMarkerCreated Or use wildcard characters to support all delete operations: • ObjectRemoved:* Parent: TopicConfiguration	Required if TopicConfiguration is added

Response Syntax

```
HTTP/1.1 status_code
Date: date
Content-Length: length
Content-Type: type
```


Response Headers

The response to the request uses common headers. For details, see **Table 3-19**.

Response Elements

This response contains no elements.

Error Responses

When this operation is being called, the system checks whether the **NotificationConfiguration** element is valid and whether the configuration is valid. The following table lists the common errors and possible causes of this operation.

Table 5-24 Error codes and possible causes

Error Code	Description	HTTP Status Code
InvalidArgument	Possible causes of this error are: • The specified event is not supported. • The specified URN does not exist or is incorrect. • The specified region in the URN is different as the region where the bucket resides. • The specified filtering rules overlap.	400 Bad Request
AccessDenied	The operator is not the bucket owner and not granted with the **PutBucketNotification** permission.	403 Forbidden

Sample Request

```
PUT /?notification HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
Date: WED, 01 Jul 2015 03:15:45 GMT
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:uRTt8YTkAqJCUfWfYkveEcIGAC0=
Content-Length: 538

<NotificationConfiguration>
  <TopicConfiguration>
    <Id>ConfigurationId</Id>
    <Filter>
      <Object>
        <FilterRule>
          <Name>prefix</Name>
          <Value>object</Value>
        </FilterRule>
        <FilterRule>
          <Name>suffix</Name>
          <Value>txt</Value>
```



```
      </FilterRule>
    </Object>
  </Filter>
  <Topic>urn:smn:region:4b29a3cb5bd64581bda5714566814bb7:tet555</Topic>
  <Event>ObjectCreated:Put</Event>
 </TopicConfiguration>
</NotificationConfiguration>
```

Sample Response

```
HTTP/1.1 200 OK
Server: OBS
x-obs-request-id: 9046000001643C8E80C19FAC4D8068E3
x-obs-id-2: 32AAAQAAEAABSAAkgAIAABAAAQAAEAABCTFAxJPTib3GkcQ7nVVs4C8Z6NNcfVDu
Date: WED, 01 Jul 2015 03:15:46 GMT
Content-Length: 0
```

5.2.14 Obtaining the Event Notification Configuration of a Bucket

Functions

This operation obtains the notification configuration of a bucket.

To perform this operation, you must have the **GetBucketNotification** permission. By default, the permission is granted to the bucket owner only. However, it can be granted to other users by configuring the bucket policy or user policy.

Request Syntax

```
GET /?notification HTTP/1.1
Host: bucketname.obs.region.example.com
Date: date
Authorization: authorization
```

Request Parameters

This request contains no message parameters.

Request Headers

This request uses common headers. For details, see **Table 3-3**.

Request Elements

This request involves no elements.

Response Syntax

```
HTTP/1.1 status_code
Content-Type: type
Date: date
Content-Length: length

<?xml version="1.0" encoding="UTF-8"?>
<NotificationConfiguration xmlns="http://obs.example.com/doc/2015-06-30/">
   <TopicConfiguration>
      <Id>ConfigurationId</Id>
      <Filter>
         <Object>
```

```
            <FilterRule>
               <Name>prefix</Name>
               <Value>prefix-value</Value>
            </FilterRule>
            <FilterRule>
               <Name>suffix</Name>
               <Value>suffix-value</Value>
            </FilterRule>
         </Object>
      </Filter>
      <Topic>TopicARN</Topic>
      <Event>event-type</Event>
      <Event>event-type</Event>
      ...
   </TopicConfiguration>
</NotificationConfiguration>
```

Response Headers

The response to the request uses common headers. For details, see **Table 3-19**.

Response Elements

This response contains elements to detail the configuration. **Table 5-25** describes the elements.

Table 5-25 Response elements for configuring event notifications

Element	Description
NotificationConfiguration	Element for configuring the event notification function of a bucket. If this element is **null**, the function is disabled. Type: container Parent: none Child: one or more TopicConfiguration elements
TopicConfiguration	Element for configuring the event notification topic. Type: container Parent: NotificationConfiguration Child: Id, Filter, Topic, and one or more Event elements
Topic	URN of the event notification topic. After detecting a specific event in the bucket, OBS sends a message to the topic. Type: string Parent: TopicConfiguration
Id	Unique ID of each event notification. If the user does not specify an ID, the system assigns an ID automatically. Type: string Parent: TopicConfiguration

Element	Description
Filter	Element used to store rules of filtering object names. Type: container Parent: TopicConfiguration Child: Object
Object	Element used to store rules of filtering object names. Type: container Parent: TopicConfiguration
FilterRule	Element that defines key-value pairs of the filtering rule. Type: container Parent: Object Child: Name and Value
Name	Prefix or suffix of object names for filtering Type: string Parent: FilterRule Value options: **prefix**, **suffix**
Value	Keywords of object names so that objects can be filtered based on the prefixes or suffixes Type: string Parent: FilterRule

Element	Description
Event	Type of events that need to be notified **NOTE** Multiple event types can be added in one TopicConfiguration element. Type: string Value options: The following values can be used to upload an object: • ObjectCreated:Put • ObjectCreated:Post • ObjectCreated:Copy • ObjectCreated:CompleteMultipartUpload Or use wildcard characters to support all upload operations: • ObjectCreated:* The following values can be used to delete an object: • ObjectRemoved:Delete • ObjectRemoved:DeleteMarkerCreated Or use wildcard characters to support all delete operations: • ObjectRemoved:* Parent: TopicConfiguration

Error Responses

No special error responses are returned. For details about error responses, see **Table 6-2**.

Sample Request

```
GET /?notification HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
Date: WED, 01 Jul 2015 03:16:32 GMT
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:r5+2zwPTKwupMg6lkeTUUqPcHfQ=
```

Sample Response

```
HTTP/1.1 200 OK
Server: OBS
x-obs-request-id: 900B000001643FDDD751B37BA87590D8
x-obs-id-2: 32AAAQAAEAABAAAQAAEAABAAAQAAEAABCSJRBSladan5ZCVw6ZIY/DAs0zs6z7Hh
Content-Type: application/xml
Date: WED, 01 Jul 2015 03:16:32 GMT
Content-Length: 490

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<NotificationConfiguration xmlns="http://obs.example.com/doc/2015-06-30/">
  <TopicConfiguration>
```



```
  <Topic>urn:smn:region:4b29a3cb5bd64581bda5714566814bb7:tet522</Topic>
  <Id>ConfigurationId</Id>
  <Filter>
    <Object>
      <FilterRule>
        <Name>prefix</Name>
        <Value>object</Value>
      </FilterRule>
      <FilterRule>
        <Name>suffix</Name>
        <Value>txt</Value>
      </FilterRule>
    </Object>
  </Filter>
  <Event>ObjectCreated:Put</Event>
 </TopicConfiguration>
</NotificationConfiguration>
```

5.2.15 Configuring Storage Class for a Bucket

Functions

This operation sets or updates the default storage class of a bucket.

To perform this operation, you must have the **PutBucketStoragePolicy** permission. By default, only the bucket owner can perform this operation. The bucket owner can grant the permission to other users by configuring the bucket policy or user policy.

If you do not specify a storage class when uploading or copying an object, or initiating a multipart upload, the object inherits the bucket's storage class.

The default storage class of a bucket is Standard.

Request Syntax

```
PUT /?storageClass HTTP/1.1
Host: bucketname.obs.region.example.com
Date: date
Content-Type: type
Content-Length: length
Authorization: authorization

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<StorageClass xmlns="http://obs.example.com/doc/2015-06-30/">STANDARD</StorageClass>
```

Request Parameters

This request contains no parameters.

Request Headers

This request uses common headers. For details, see **Table 3-3**.

Request Elements

This request needs an additional element to specify the default bucket storage class. For details, see **Table 5-26**.

Table 5-26 Additional request elements

Element	Description	Mandatory
StorageClass	Specifies the default storage class for a bucket. Type: string Value options: **STANDARD**, **WARM**, **COLD** The available storage classes are as follows: Standard (**STANDARD**), Warm (**WARM**), Cold (**COLD**).	Yes

Response Syntax

```
HTTP/1.1 status_code
Date: date
```

Response Headers

The response to the request uses common headers. For details, see **Table 3-19**.

Response Elements

This response contains no elements.

Error Responses

No special error responses are returned. For details about error responses, see **Table 6-2**.

Sample Request

```
PUT /?storageClass HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
Date: WED, 01 Jul 2015 03:18:19 GMT
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:Tf6XbndPx/yNgfAVQ6KIXr7tMj4=
Content-Length: 87

<StorageClass xmlns="http://obs.example.com/doc/2015-06-30/">STANDARD</StorageClass>
```

Sample Response

```
HTTP/1.1 200 OK
Server: OBS
x-obs-request-id: BF2600000164368E704B571F328A8797
x-obs-id-2: 32AAAQAAEAABSAAgAAEAABAAAQAAEAABCSIsw3tPtUn6damTI5acQmQAcEfmTwl3
Date: WED, 01 Jul 2015 03:18:19 GMT
Content-Length: 0
```


5.2.16 Obtaining Bucket Storage Class Information

Functions

This operation obtains the default storage class of a bucket.

To perform this operation, you must have the **GetBucketStoragePolicy** permission. By default, only the bucket owner can perform this operation. The bucket owner can grant the permission to other users by configuring the bucket policy or user policy.

Request Syntax

```
GET /?storageClass HTTP/1.1
Host: bucketname.obs.region.example.com
Date: date
Authorization: authorization
```

Request Parameters

This request contains no message parameters.

Request Headers

This request uses common headers. For details, see **Table 3-3**.

Request Elements

This request contains no elements.

Response Syntax

```
HTTP/1.1 status_code
Date: date
Content-Type: type
Content-Length: length

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>

<StorageClass xmlns="http://obs.example.com/doc/2015-06-30/">STANDARD</StorageClass>
```

Response Headers

The response to the request uses common headers. For details, see **Table 3-19**.

Response Elements

This response contains elements to provide details about the storage class information of a bucket. **Table 5-27** describes the elements.

Table 5-27 Response elements

Element	Description
StorageClass	Default storage class of the bucket. Type: string. For details about the enumeration types, see **Table 5-26**.

Error Responses

No special error responses are returned. For details about error responses, see **Table 6-2**.

Sample Request

```
GET /?storageClass HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
Date: WED, 01 Jul 2015 03:20:28 GMT
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:0zVTSdKG6OFCIH2dKvmsVGYCQyw=
```

Sample Response

```
HTTP/1.1 200 OK
Server: OBS
x-obs-request-id: BF260000016436BE45820FDF3A65B42C
x-obs-id-2: 32AAAQAAEAABAAAQAAEAABAAAQAAEAABCSCju1CZy3ZfRVW5hiNd024lRFdUoqWy
Content-Type: application/xml
Date: WED, 01 Jul 2015 03:20:28 GMT
Content-Length: 142

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>

<StorageClass xmlns="http://obs.example.com/doc/2015-06-30/">STANDARD</StorageClass>
```

5.2.17 Configuring Tags for a Bucket

Functions

This operation adds tags to a bucket.

After tags are added to a bucket, all service detail records (SDRs) generated by the requests for this bucket will have the same tags. You can categorize the SDRs for detailed cost analysis. For example, if a running application uploads data to a bucket, you can tag the bucket with the application name. In this manner, the costs on the application can be analyzed using tags in SDRs.

To perform this operation, you must have the **PutBucketTagging** permission. By default, only the bucket owner can delete the tags of a bucket. The bucket owner can allow other users to perform this operation by setting a bucket policy or granting them the permission.

NOTE

- A bucket can have up to 10 tags.
- A tag key and key value can contain a maximum of 36 and 43 characters, respectively.
- Tag keys and values cannot contain commas (,), asterisks (*), vertical bars (|), slashes (/), less-than signs (<), greater-than signs (>), equal signs (=), backslashes (\), or ASCII control character code (0x00 to 0x1F). These tag keys and values must be URL encoded before being sent to a server.

Request Syntax

```
PUT /?tagging HTTP/1.1
Host: bucketname.obs.region.example.com
Date: date
Authorization: authorization string
Content-MD5: md5
<Tagging>
   <TagSet>
      <Tag>
         <Key>Tag Name</Key>
         <Value>Tag Value</Value>
      </Tag>
   </TagSet>
</Tagging>
```

Request Parameters

This request contains no message parameters.

Request Headers

Table 5-28 lists the request header.

Table 5-28 Request headers

Header	Description	Mandatory
Content-MD5	Base64-encoded 128-bit MD5 digest of the message according to RFC 1864. Type: string Example: **n58IG6hfM7vqI4K0vnWpog==**	Yes

Request Elements

In this request, you must configure bucket tags in the request body. The tag configuration is uploaded in XML format. Table 5-29 describes the configuration elements.

Table 5-29 Bucket tag configuration elements

Header	Description	Mandatory
Tagging	Root element for TagSet and Tag Type: container Parent: none	Yes
TagSet	Element of the tag set Type: container Parent: Tagging	Yes
Tag	Information element of Tag Type: container Parent: TagSet	Yes
Key	Tag name Type: string Parent: Tag	Yes
Value	Tag value Type: string Parent: Tag	Yes

Response Syntax

```
HTTP/1.1 status_code
x-obs-request-id: request id
x-obs-id-2: id
Content-Length: length
Date: date
```

Response Headers

The response to the request uses common headers. For details, see **Table 3-19**.

Response Elements

This response contains no elements.

Error Responses

In addition to common error codes, this API also returns other error codes. The following table lists common errors and possible causes. For details, see **Table 5-30**.

Table 5-30 Bucket tag configuration errors

Error Code	Description	HTTP Status Code
InvalidTagError	An invalid tag is provided when configuring bucket tags.	400 Bad Request
MalformedXMLError	An incorrect XML format is provided when configuring bucket tags.	400 Bad Request

Sample Request

This example adds a tag whose key is **TagKey(Name1)** and value is **TagValue(Value1)** to bucket **examplebucket**.

```
PUT /?tagging HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
Date: Wed, 27 Jun 2018 13:22:50 GMT
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:Pf1ZyGvVYg2BzOjokZ/BAeR1mEQ=
Content-MD5: MnAEvkfQIGnBpchOE2U6Og==
Content-Length: 182

<Tagging xmlns="http://obs.example.com/doc/2015-06-30/">
  <TagSet>
    <Tag>
      <Key>TagKey%28Name1%29</Key>
      <Value>TagValue%28Value1%29</Value>
    </Tag>
  </TagSet>
</Tagging>
```

Sample Response

```
HTTP/1.1 204 No Content
Server: OBS
x-obs-request-id: BF26000001643FEBA09B1ED46932CD07
x-obs-id-2: 32AAAQAAEAABSAAgAAEAABAAAQAAEAABCSEZp87iEirC6DggPB5cN49pSvHBWClg
Date: Wed, 27 Jun 2018 13:22:50 GMT
```

5.2.18 Obtaining Bucket Tags

Functions

This operation obtains information about tags of a bucket.

To perform this operation, you must have the **GetBucketTagging** permission. By default, only the bucket owner can obtain the tags of a bucket. The bucket owner can allow other users to perform this operation by setting a bucket policy or granting them the permission.

Request Syntax

```
GET /?tagging HTTP/1.1
Host: bucketname.obs.region.example.com
```



```
Date: date
Authorization: authorization string
```

Request Parameters

This request contains no message parameters.

Request Headers

This request uses common headers. For details, see **Table 3-3**.

Request Elements

This request involves no elements.

Response Syntax

```
HTTP/1.1 status_code
x-obs-request-id: request id
x-obs-id-2: id
Content-Type: application/xml
Content-Length: length
Date: date
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Tagging xmlns="http://obs.example.com/doc/2015-06-30/">
   <TagSet>
      <Tag>
         <Key>key</Key>
         <Value>value</Value>
      </Tag>
   </TagSet>
</Tagging>
```

Response Headers

The response to the request uses common headers. For details, see **Table 3-19**.

Response Elements

This response contains elements to detail bucket tag configuration. **Table 5-31** describes the elements.

Table 5-31 Elements for configuring bucket tags

Element	Description
Tagging	Element of the tag set and tag. Type: container Parent: none
TagSet	Element of the tag set. Type: container Parent: Tagging

Element	Description
Tag	Element of the tag information. Type: container Parent: TagSet
Key	Tag name. Type: string Parent: Tag
Value	Tag value. Type: string Parent: Tag

Error Responses

In addition to common error codes, this API also returns other error codes. The following table lists common errors and possible causes. For details, see **Table 5-32**.

Table 5-32 Bucket tag configuration errors

Error Code	Description	HTTP Status Code
NoSuchTagSet	The specified bucket does not have any tags.	404 Not Found

Sample Request

```
GET /?tagging HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
Date: Wed, 27 Jun 2018 13:25:44 GMT
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:H1INcyc5i0XlHqYTfuzkPxLZUPM=
```

Sample Response

```
HTTP/1.1 200 OK
x-obs-request-id: 0002B7532E0000015BEB35330C5884X1
x-obs-id-2: s12w20LYNQqSb7moq4ibgJwmQRSmVQV+rFBqplOGYkXUpXeS/nOmbkyD+E35K79j
Content-Type: application/xml
Date: Wed, 27 Jun 2018 13:25:44 GMT
Content-Length: 441

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Tagging xmlns="http://obs.example.com/doc/2015-06-30/">
  <TagSet>
    <Tag>
      <Key>TagName1</Key>
      <Value>TageSetVaule1</Value>
    </Tag>
```



```
  </TagSet>
</Tagging>
```

5.2.19 Deleting Tags

Functions

This operation deletes the tags of a bucket.

To perform this operation, you must have the **DeleteBucketTagging** permission. By default, only the bucket owner can delete the tags of a bucket. The bucket owner can allow other users to perform this operation by setting a bucket policy or granting them the permission.

Request Syntax

```
DELETE /?tagging HTTP/1.1
Host: bucketname.obs.region.example.com
Date: date
Authorization: authorization string
```

Request Parameters

This request contains no message parameters.

Request Headers

This request uses common headers. For details, see **Table 3-3**.

Request Elements

This request involves no elements.

Response Syntax

```
HTTP/1.1 status_code
x-obs-request-id: request id
x-obs-id-2: id
Content-Length: length
Date: date
```

Response Headers

The response to the request uses common headers. For details, see **Table 3-19**.

Response Elements

This response contains no elements.

Error Responses

No special error responses are returned. For details about error responses, see **Table 6-2**.

Sample Request

```
DELETE /?tagging HTTP/1.1
User-Agent: curl/7.19.7
```



```
Host: examplebucket.obs.region.example.com
Accept: */*
Date: Wed, 27 Jun 2018 13:46:58 GMT
Authorization: authorization string
```

Sample Response

```
HTTP/1.1 204 No Content
x-obs-request-id: 0002B7532E0000015BEB2C212E53A17L
x-obs-id-2: CqT+86nnOkB+Cv9KZoVgZ28pSgMF+uGQBUC68flvkQeq6CxoCz65wWFMNBpXvea4
Content-Length: 0
Date: Wed, 27 Jun 2018 13:46:58 GMT
```

5.2.20 Configuring Bucket Storage Quota

Functions

The bucket storage quota must be a positive integer in the unit of byte. The maximum storage quota is 2^{63} – 1 bytes. The default bucket storage quota is **0**, indicating that the bucket storage quota is not limited.

NOTE

1. For a bucket that has a specified storage quota, you can change the quota to **0** to cancel the quota limitation.
2. The bucket storage quota verification depends on how much space is used in the bucket. However, the used storage space is measured at the background. Therefore, bucket storage quotas may not take effect immediately, and delay is expected. The used storage space in a bucket may exceed the bucket storage quota, or the used storage space may remain unchanged after data is deleted from the bucket.
3. For details about the API for querying used storage space, see **Obtaining Storage Information of a Bucket**.
4. If the used storage space in a bucket reaches the upper limit of the bucket storage quota, object upload will fail and the HTTP status code 403 Forbidden will be returned, indicating **InsufficientStorageSpace**. In this case, you can increase the quota, cancel the quota limitation (by changing the quota to **0**), or delete unwanted objects from the bucket.

Request Syntax

```
PUT /?quota HTTP/1.1
Host: bucketname.obs.region.example.com
Date: date
Content-Length: length
Authorization: authorization

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Quota xmlns="http://obs.region.example.com/doc/2015-06-30/">
   <StorageQuota>value</StorageQuota>
</Quota>
```

Request Parameters

This request contains no parameters.

Request Headers

This request uses common headers. For details, see **Table 3-3**.

Request Elements

This request uses an additional element to specify a bucket quota. **Table 5-33** describes the element.

Table 5-33 Additional request elements

Element	Description	Mandatory
StorageQuota	Specifies the bucket storage quota. The unit is byte. Type: integer	Yes

Response Syntax

```
HTTP/1.1 status_code
Date: date
Content-Length: length
```

Response Headers

The response to the request uses common headers. For details, see **Table 3-19**.

Response Elements

This response contains no elements.

Error Responses

No special error responses are returned. For details about error responses, see **Table 6-2**.

Sample Request

```
PUT /?quota HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
Date: WED, 01 Jul 2015 03:24:37 GMT
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:k/rbwnYaqYf0Ae6F0M3OJQ0dmI8=
Content-Length: 106

<Quota xmlns="http://obs.region.example.com/doc/2015-06-30/">
  <StorageQuota>10240000</StorageQuota>
</Quota>
```

Sample Response

```
HTTP/1.1 100 Continue
HTTP/1.1 200 OK
Server: OBS
x-obs-request-id: BF260000016435E09A2BCA388688AA08
x-obs-id-2: 32AAAQAAEAABSAAgAAEAABAAAQAAEAABCSHbmBecv7ohDSvqaRObpxzgzJ9+l8xT
Date: WED, 01 Jul 2015 03:24:37 GMT
Content-Length: 0
```


5.2.21 Querying Bucket Storage Quota

Functions

A bucket owner can query the bucket storage quota, but a bucket owner who is frozen due to arrears cannot. The bucket storage quota is measured by byte. **0** indicates that no upper limit is set.

Request Syntax

```
GET /?quota HTTP/1.1
Host: bucketname.obs.region.example.com
Date: date
Authorization: authorization
```

Request Parameters

This request contains no message parameters.

Request Headers

This request uses common headers. For details, see **Table 3-3**.

Request Elements

This request contains no elements.

Response Syntax

```
HTTP/1.1 status_code
Date: date
Content-Type: application/xml
Content-Length: length

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Quota xmlns="http://obs.region.example.com/doc/2015-06-30/">
   <StorageQuota>quota</StorageQuota>
</Quota>
```

Response Headers

The response to the request uses common headers. For details, see **Table 3-19**.

Response Elements

This response contains elements of information about the bucket quota. **Table 5-34** describes the elements.

Table 5-34 Response elements

Element	Description
Quota	Bucket storage quota. This element contains the StorageQuota element. Type: XML

Element	Description
StorageQuota	Bucket storage quota quantity. The unit is byte. Type: string

Error Responses

No special error responses are returned. For details about error responses, see **Table 6-2**.

Sample Request

```
GET /?quota HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
Date: WED, 01 Jul 2015 03:27:45 GMT
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:8m4bW1gFCNeXQlfu45uO2gpo7l8=
```

Sample Response

```
HTTP/1.1 200 OK
Server: OBS
x-obs-request-id: BF260000016436B55D8DED9AE26C4D18
x-obs-id-2: 32AAAQAAEAABAAAQAAEAABAAAQAAEAABCSs2Q5vz5AfpAJ/CMNgCfo2hmDowp7M9
Content-Type: application/xml
Date: WED, 01 Jul 2015 03:27:45 GMT
Content-Length: 150

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Quota xmlns="http://obs.example.com/doc/2015-06-30/">
  <StorageQuota>0</StorageQuota>
</Quota>
```

5.2.22 Obtaining Storage Information of a Bucket

Functions

This operation queries the number of bucket objects and the space occupied by the objects. The size of the object space is a positive integer, measured by bytes.

NOTE

Because OBS bucket storage statistics are measured in the background, the storage information is not updated in real time. For this reason, you are advised not to perform real-time verification on the storage information.

Request Syntax

```
GET /?storageinfo HTTP/1.1
Host: bucketname.obs.region.example.com
Date: date
Authorization: authorization
```

Request Parameters

This request contains no parameters.

Request Headers

This request uses common headers. For details, see **Table 3-3**.

Request Elements

This request contains no elements.

Response Syntax

```
HTTP/1.1 status_code
Date: date
Content-Type: type
Content-Length: length
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<GetBucketStorageInfoResult xmlns="http://obs.region.example.com/doc/2015-06-30/">
<Size>size</Size>
<ObjectNumber>number</ObjectNumber>
</GetBucketStorageInfoResult>
```

Response Headers

The response to the request uses common headers. For details, see **Table 3-19**.

Response Elements

This response contains elements of information about the used storage capacity of a bucket. **Table 5-35** describes the elements.

Table 5-35 Response elements

Element	Description
GetBucketStorageInfoResult	Request result that saves bucket storage information, including the stored data size and the number of objects Type: XML
Size	Size of stored data Type: long
ObjectNumber	Number of objects returned Type: integer

Error Responses

No special error responses are returned. For details about error responses, see **Table 6-2**.

Sample Request

```
GET /?storageinfo HTTP/1.1
User-Agent: curl/7.29.0
```



```
Host: examplebucket.obs.region.example.com
Accept: */*
Date: WED, 01 Jul 2015 03:31:18 GMT
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:bLcdeJGYWw/eEEjMhPZx2MK5R9U=
```

Sample Response

```
HTTP/1.1 200 OK
Server: OBS
x-obs-request-id: BF260000016435DD2958BFDCDB86B55E
x-obs-id-2: 32AAAQAAEAABAAAQAAEAABAAAQAAEAABCSitZctaPYVnat49fVMd1O+OWIP1yrg3
Content-Type: application/xml
WED, 01 Jul 2015 03:31:18 GMT
Content-Length: 206

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<GetBucketStorageInfoResult xmlns="http://obs.example.com/doc/2015-06-30/">
  <Size>25490</Size>
  <ObjectNumber>24</ObjectNumber>
</GetBucketStorageInfoResult>
```

5.2.23 Configuring a Custom Domain Name for a Bucket

Functions

OBS uses the PUT method to configure a custom domain name for a bucket. After the configuration is successful, you can access the bucket through the domain name.

Ensure that the custom domain name can correctly resolve to the OBS service through DNS.

Request Syntax

```
PUT /?customdomain=domainname HTTP/1.1
User-Agent: curl/7.29.0
Host: bucketname.obs.region.example.com
Accept: */*
Date: date
Authorization: authorization string
Content-Length: 0
```


Request Parameters

Table 5-36 Request parameters

Parameter	Description	Mandatory
customdomain	Custom domain name of a bucket. Type: string, which must meet the naming conventions of domain names. Specifications: The value contains a maximum of 256 characters. No default value. Constraints: A bucket can have a maximum of 30 domain names. A custom domain name can be used for only one bucket.	Yes

Request Header

This request uses common headers. For details, see **Table 3-3**.

Request Elements

This request involves no elements.

Response Syntax

```
HTTP/1.1 200 OK
Server: OBS
x-obs-request-id: request id
x-obs-id-2:  id
Date: date
Content-Length: 0
```

Response Headers

The response to the request uses common headers. For details, see **Table 3-19**.

Response Elements

This response contains no elements.

Error Responses

No special error responses are returned. For details about error responses, see **Table 6-2**.

Sample Request

```
PUT /?customdomain=obs.ccc.com HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
```



```
Date: Mon, 14 Jan 2019 08:31:36 +0000
Authorization: OBS UDSIAMSTUBTEST000094:u2kJF4kENs6KlIDcAZpAKSKPtnc=
Content-Length: 0
```

Sample Response

```
HTTP/1.1 200 OK
Server: OBS
x-obs-request-id: 000001697692CC5380E9D272E6D8F830
x-obs-id-2: 32AAAQAAEAABSAAgAAEAABAAAQAAEAABCSsfu2GXj9gScHhFnrrTPY2cFOEZuvta
Date: Wed, 13 Mar 2019 10:22:05 GMT
Content-Length: 0
```

5.2.24 Obtaining the Custom Domain Name of a Bucket

Functions

OBS uses the GET method to obtain the custom domain name of a bucket.

Request Syntax

```
GET /?customdomain HTTP/1.1
User-Agent: curl/7.29.0
Host: bucketname.obs.region.example.com
Accept: */*
Date: date
Authorization: authorization string
```

Request Parameters

This request message does not contain the request parameters.

Request Header

This request uses common headers. For details, see **Table 3-3**.

Request Elements

This request involves no elements.

Response Syntax

```
HTTP/1.1 200 OK
Server: OBS
x-obs-request-id: request id
x-obs-id-2: id
Content-Type: application/xml
Date: date
Content-Length: 272

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ListBucketCustomDomainsResult xmlns="http://obs.example.com/doc/2015-06-30/">
  <Domains>
    <DomainName>domainname</DomainName>
    <CreateTime>createtime</CreateTime>
  </Domains>
</ListBucketCustomDomainsResult>
```

Response Headers

The response to the request uses common headers. For details, see **Table 3-19**.

Response Elements

The response returns the custom domain name of the bucket in the form of message elements. **Table 5-37** lists details about each element.

Table 5-37 Response elements

Element	Description
ListBucketCustomDomainsResult	Container of the returned result Type: container Child: Domains Parent: none
Domains	Element indicating the custom domain name Type: container Child: DomainName and CreateTime Parent: ListBucketCustomDomainsResult
DomainName	Custom domain name Type: string Child: none Parent: Domains
CreateTime	Time when a custom domain name is created Type: string, which must be a UTC time. Child: none Parent: Domains

Error Responses

No special error responses are returned. For details about error responses, see **Table 6-2**.

Sample Request

```
GET /?customdomain HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
Date: Mon, 14 Jan 2019 08:31:45 +0000
Authorization: OBS UDSIAMSTUBTEST000094:veTm8B18MPLFqNyGh2wmQqovZ2U=
```

Sample Response

```
HTTP/1.1 200 OK
Server: OBS
x-obs-request-id: 000001697693130C80E9D2D29FA84FC2
x-obs-id-2: 32AAAQAAEAABAAAQAAEAABAAAQAAEAABCSM80AI9weqGUsIFJScVxSKlG4DmypX9
Content-Type: application/xml
Date: Wed, 13 Mar 2019 10:22:24 GMT
Content-Length: 272
```



```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ListBucketCustomDomainsResult xmlns="http://obs.example.com/doc/2015-06-30/">
  <Domains>
    <DomainName>obs.ccc.com</DomainName>
    <CreateTime>2019-03-13T10:22:05.912Z</CreateTime>
  </Domains>
</ListBucketCustomDomainsResult>
```

5.2.25 Deleting the Custom Domain Name of a Bucket

Functions

OBS uses the DELETE method to delete the custom domain name of a bucket.

Request Syntax

```
DELETE /?customdomain=domainname HTTP/1.1
User-Agent: curl/7.29.0
Host: bucketname.obs.region.example.com
Accept: */*
Date: date
Authorization: authorization string
```

Request Parameters

Table 5-38 Request parameters

Parameter	Description	Mandatory
customdomain	Specifies the custom domain name to be deleted. Type: string, which must meet the naming conventions of domain names. Specifications: The value contains a maximum of 256 characters. No default value.	Yes

Request Header

This request uses common headers. For details, see **Table 3-3**.

Request Elements

This request involves no elements.

Response Syntax

```
HTTP/1.1 204 No Content
Server: OBS
x-obs-request-id: request id
x-obs-id-2: id
Date: date
```


Response Headers

The response to the request uses common headers. For details, see **Table 3-19**.

Response Elements

This response contains no elements.

Error Responses

No special error responses are returned. For details about error responses, see **Table 6-2**.

Sample Request

```
DELETE /?customdomain=obs.ccc.com HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
Date: Mon, 14 Jan 2019 08:27:50 +0000
Authorization: OBS UDSIAMSTUBTEST000094:ACgHHA1z+dqZhqS7D2SbU8ugluw=
```

Sample Response

```
HTTP/1.1 204 No Content
Server: OBS
x-obs-request-id: 000001697694073F80E9D3D43BB10B8F
x-obs-id-2: 32AAAQAAEAABSAAgAAEAABAAAQAAEAABCSyjWyXNRPSnFymJW0AI59GKpW0Qm9UJ
Date: Wed, 13 Mar 2019 10:23:26 GMT
```

5.2.26 Configuring Bucket Encryption

Functions

OBS uses the PUT method to create or update the default server-side encryption for a bucket.

After you configure encryption for a bucket, objects uploaded to this bucket will be encrypted with the bucket encryption settings you specified. Available encryption methods include server-side encryption with KMS-managed keys (SSE-KMS) and server-side encryption with customer-provided keys (SSE-C). For details, see **Server-Side Encryption**.

To perform this operation, you must have the **PutEncryptionConfiguration** permission. By default, the bucket owner has this permission and can grant it to others.

Request Syntax (SSE-KMS)

```
PUT /?encryption  HTTP/1.1
User-Agent: curl/7.29.0
Host: bucketname.obs.region.example.com
Accept: */*
Date: date
Authorization: authorization string
Content-Length: length

<ServerSideEncryptionConfiguration>
   <Rule>
      <ApplyServerSideEncryptionByDefault>
```



```
        <SSEAlgorithm>kms</SSEAlgorithm>
        <KMSMasterKeyID>kmskeyid-value</KMSMasterKeyID>
      </ApplyServerSideEncryptionByDefault>
   </Rule>
</ServerSideEncryptionConfiguration>
```

Request Parameters

This request contains no message parameters.

Request Headers

This request uses common headers. For details, see **Table 3-3**.

Request Elements

In this request, you need to carry the bucket encryption configuration in the request body. The bucket encryption configuration information is uploaded in the XML format. **Table 5-39** lists the configuration elements.

Table 5-39 Configuration elements of bucket encryption

Header	Description	Mandatory
ServerSideEncryption-Configuration	Root element of the default encryption configuration of a bucket. Type: container Parent: none Child: Rule	Yes
Rule	Sub-element of the default encryption configuration of a bucket. Type: container Parent: ServerSideEncryptionConfiguration Child: ApplyServerSideEncryptionByDefault	Yes
ApplyServerSideEncryp-tionByDefault	Sub-element of the default encryption configuration of a bucket. Type: container Parent: Rule Child: SSEAlgorithm and KMSMasterKeyID	Yes
SSEAlgorithm	Server-side encryption algorithm used for the default encryption configuration of a bucket. Type: string Value options: **kms** Parent: ApplyServerSideEncryptionByDefault	Yes

Header	Description	Mandatory
KMSMasterKeyID	Customer master key (CMK) used in SSE-KMS encryption mode. If you do not specify this header, the default master key will be used. Type: string Valid value formats are as follows: 1. *regionID*:*domainID*:**key/***key_id* 2. *key_id* In the preceding formats: • *regionID* indicates the ID of the region where the key belongs. • *domainID* indicates the ID of the domain to which the key belongs. For details, see **Obtaining a Domain ID and a User ID**. • *key_id* indicates the ID of the key created in KMS. Parent: ApplyServerSideEncryptionByDefault	No
ProjectID	ID of the project where the KMS master key belongs when SSE-KMS is used. If the project is not the default one, you must use this parameter to specify the project ID. Type: string Value options: 1. Project ID that matches **KMSMasterKeyID**. 2. If **KMSMasterKeyID** is not specified, do not set the project ID. Parent: ApplyServerSideEncryptionByDefault **NOTE** When a custom key in a non-default IAM project is used to encrypt objects, only the key owner can upload or download the encrypted objects.	No

Response Syntax

```
HTTP/1.1 status_code
Date: date
Content-Length: length
```

Response Headers

The response to the request uses common headers. For details, see **Table 3-19**.

Response Elements

This response contains no elements.

Error Responses

No special error responses are returned. For details about error responses, see **Table 6-2**.

Sample Request

```
PUT /?encryption HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
Date:  Thu, 21 Feb 2019 03:05:34 GMT
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:DpSAlmLX/BTdjxU5HOEwflhM0WI=
Content-Length: 778

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ServerSideEncryptionConfiguration xmlns="http://obs.region.example.com/doc/2015-06-30/">
   <Rule>
      <ApplyServerSideEncryptionByDefault>
         <SSEAlgorithm>kms</SSEAlgorithm>
         <KMSMasterKeyID>4f1cd4de-ab64-4807-920a-47fc42e7f0d0</KMSMasterKeyID>
      </ApplyServerSideEncryptionByDefault>
   </Rule>
</ServerSideEncryptionConfiguration>
```

Sample Response

```
HTTP/1.1 200 OK
Server: OBS
x-obs-request-id: BF26000001643670AC06E7B9A7767921
x-obs-id-2: 32AAAQAAEAABSAAgAAEAABAAAQAAEAABCSvK6z8HV6nrJh49gsB5vqzpgtohkiFm
Date: Thu, 21 Feb 2019 03:05:34 GMT
Content-Length: 0
```

5.2.27 Obtaining Bucket Encryption Configuration

Functions

OBS uses the GET method to obtain the encryption configuration of a specified bucket.

To perform this operation, you must have the **GetEncryptionConfiguration** permission. By default, only the bucket owner can delete the tags of a bucket. The bucket owner can allow other users to perform this operation by setting a bucket policy or granting them the permission.

Request Syntax

```
GET /?encryption  HTTP/1.1
User-Agent: curl/7.29.0
Host: bucketname.obs.region.example.com
Accept: */*
Date: date
Authorization: authorization string
```


Request parameters

This request contains no message parameters.

Request Headers

This request uses common headers. For details, see **Table 3-3**.

Request Elements

This request involves no elements.

Response Syntax

```
HTTP/1.1 status_code
x-obs-request-id: request id
x-obs-id-2: id
Content-Type: application/xml
Content-Length: length
Date: date

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ServerSideEncryptionConfiguration xmlns="http://obs.region.example.com/doc/2015-06-30/">
   <Rule>
      <ApplyServerSideEncryptionByDefault>
         <SSEAlgorithm>kms</SSEAlgorithm>
         <KMSMasterKeyID>kmskeyid-value</KMSMasterKeyID>
         <ProjectID>projectid</ProjectID>
      </ApplyServerSideEncryptionByDefault>
   </Rule>
</ServerSideEncryptionConfiguration>
```

Response Headers

The response to the request uses common headers. For details, see **Table 3-19**.

Response Elements

This response contains the following elements to detail bucket encryption configuration:

Table 5-40 Configuration elements of bucket encryption

Header	Description
ServerSideEncryptionConfiguration	Root element of the default encryption configuration of a bucket. Type: container Parent: none Child: Rule

Header	Description
Rule	Sub-element of the default encryption configuration of a bucket. Type: container Parent: ServerSideEncryptionConfiguration Child: ApplyServerSideEncryptionByDefault
ApplyServerSideEncryptionBy-Default	Sub-element of the default encryption configuration of a bucket. Type: container Parent: Rule Child: SSEAlgorithm and KMSMasterKeyID
SSEAlgorithm	The server-side encryption algorithm used for encryption configuration of a bucket. Type: string Value options: **kms** Parent: ApplyServerSideEncryptionByDefault
KMSMasterKeyID	ID of the customer master key (CMK) used for SSE-KMS. Type: string Parent: ApplyServerSideEncryptionByDefault
ProjectID	ID of the project where the KMS master key belongs when SSE-KMS is used. Type: string Parent: ApplyServerSideEncryptionByDefault **NOTE** When a custom key in a non-default IAM project is used to encrypt objects, only the key owner can upload or download the encrypted objects.

Error Responses

In addition to common error codes, this API also returns others. The following table lists common errors and possible causes. For details, see **Table 5-41**.

Table 5-41 Error codes related to getting bucket encryption configuration

Error Code	Description	HTTP Status Code
NoSuchEncryptionConfi-guration	The specified bucket does not have any encryption configurations	404 Not Found

Sample Request

```
GET /?encryption HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
Date:  Thu, 21 Feb 2019 03:05:34 GMT
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:DpSAlmLX/BTdjxU5HOEwflhM0WI=
```

Sample Response

```
HTTP/1.1 200 OK
Server: OBS
x-obs-request-id: BF26000001643670AC06E7B9A7767921
x-obs-id-2: 32AAAQAAEAABSAAgAAEAABAAAQAAEAABCSvK6z8HV6nrJh49gsB5vqzpgtohkiFm
Date: Thu, 21 Feb 2019 03:05:34 GMT
Content-Length: 788

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ServerSideEncryptionConfiguration xmlns="http://obs.region.example.com/doc/2015-06-30/">
   <Rule>
      <ApplyServerSideEncryptionByDefault>
         <SSEAlgorithm>kms</SSEAlgorithm>
         <KMSMasterKeyID>4f1cd4de-ab64-4807-920a-47fc42e7f0d0</KMSMasterKeyID>
      </ApplyServerSideEncryptionByDefault>
   </Rule>
</ServerSideEncryptionConfiguration>
```

5.2.28 Deleting the Encryption Configuration of a Bucket

Functions

OBS uses the DELETE method to delete the encryption configuration of a specified bucket.

To perform this operation, you must have the **PutEncryptionConfiguration** permission. By default, only the bucket owner can delete the tags of a bucket. The bucket owner can allow other users to perform this operation by setting a bucket policy or granting them the permission.

Request Syntax

```
DELETE /?encryption HTTP/1.1
User-Agent: curl/7.29.0
Host: bucketname.obs.region.example.com
Accept: */*
Date: date
Authorization: authorization string
```

Request parameters

This request contains no message parameters.

Request Headers

This request uses common headers. For details, see **Table 3-3**.

Request Elements

This request involves no elements.

Response Syntax

```
HTTP/1.1 status_code
Server: OBS
x-obs-request-id: request id
x-obs-id-2: id
Date: date
```

Response Headers

The response to the request uses common headers. For details, see **Table 3-19**.

Response Elements

This response contains no elements.

Error Responses

No special error responses are returned. For details about error responses, see **Table 6-2**.

Sample Request

```
DELETE /examplebucket?encryption HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
Date: Tue, 08 Jan 2019 13:18:35 +0000
Authorization: OBS UDSIAMSTUBTEST000001:UT9F2YUgaFu9uFGMmxFj2CBgQHs=
```

Sample Response

```
HTTP/1.1 204 No Content
Server: OBS
x-obs-request-id: 000001682D993B666808E265A3F6361D
x-obs-id-2: 32AAAQAAEAABAAAQAAEAABAAAQAAEAABCSyB46jGSQsu06m1nyIeKxTuJ+H27ooC
Date: Tue, 08 Jan 2019 13:14:03 GMT
```

5.3 Static Website Hosting

5.3.1 Configuring Static Website Hosting for a Bucket

Functions

OBS allows you to store static web page resources such as HTML web pages, flash files, videos, and audios in a bucket. When a client accesses these resources from the website endpoint of the bucket, the browser can directly resolve and present the resources to the client. This operation is applicable to:

- Redirecting all requests to a website endpoint.
- Adding routing rules that redirect specific requests.

You can perform this operation to create or update the website configuration of a bucket.

To perform this operation, you must have the **PutBucketWebsite** permission. By default, only the bucket owner can perform this operation. The bucket owner can grant the permission to other users by configuring the bucket policy or user policy.

NOTE

Avoid using periods (.) in the destination bucket name. Otherwise, failures in client authentication certificate may occur when users use HTTPS for access.

The maximum size of a network configuration request for a bucket is 10 KB.

Request Syntax

```
PUT /?website HTTP/1.1
Host: bucketname.obs.region.example.com
Content-Length: length
Date: date
Authorization: authorization
<WebsiteConfiguration>
   <RedirectAllRequestsTo>
      <HostName>hostName</HostName>
   </RedirectAllRequestsTo>
</WebsiteConfiguration>
```

Request Parameters

This request contains no parameters.

Request Headers

This request uses common headers. For details, see **Table 3-3**.

Request Elements

This request contains elements to specify the website configuration in XML format.

- To redirect all website requests sent to the bucket's website endpoint, add the elements as described in **Table 5-42**.

  Table 5-42 Elements for redirecting all website requests

Element	Description	Mandatory
WebsiteConfiguration	Root node configured on the website Type: container Parent: none	Yes

Element	Description	Mandatory
RedirectAllRequestsTo	Describes the redirection behavior for every request to this bucket's website endpoint. If this element is present, no other siblings are allowed. Type: container Parent: WebsiteConfiguration	Yes
HostName	Name of the host where requests will be redirected Type: string Parent: RedirectAllRequestsTo	Yes
Protocol	The HTTP or HTTPS protocol used in redirecting requests. The default protocol is HTTP. Type: string Parent: RedirectAllRequestsTo	No

- To configure redirection rules, add the elements as described in **Table 5-43**.

  Table 5-43 Elements for adding rules that redirect requests

Element	Description	Mandatory
WebsiteConfiguration	Root element for the website configuration Type: container Parent: none	Yes
IndexDocument	***Suff*** element Type: container Parent: WebsiteConfiguration	Yes

Element	Description	Mandatory
Suffix	*Suffix* that is appended to a request initiated for a directory on the website endpoint. For example, if the *suffix* is **index.html** and you request for **samplebucket/images/**, the data that is returned will be for the object with the key name **images/index.html** in the **samplebucket** bucket. *Suffix* cannot be empty or contain slashes (/). Type: string Parent: IndexDocument	Yes
ErrorDocument	*Key* element Type: container Parent: WebsiteConfiguration	No
Key	Object key that is used when a 4XX error occurs. This element identifies the page that is returned when a 4XX error occurs. Type: string Parent: ErrorDocument Condition: Required when **ErrorDocument** is specified.	No
RoutingRules	***Routing*** element Type: container Parent: WebsiteConfiguration	No
RoutingRule	Element of a redirection rule. A redirection rule contains a **Condition** and a **Redirect**. When the **Condition** is matched, **Redirect** takes effect. Type: container Parent: RoutingRules At least the *RoutingRule* element is required.	Yes
Condition	Element for describing a condition that must be met for the specified redirection to apply. Type: container Parent: RoutingRule	No

Element	Description	Mandatory
KeyPrefixEquals	Object key name prefix when the redirection is applied. Example: • To redirect the request for object **ExamplePage.html**, the **KeyPrefixEquals** is set to **ExamplePage.html**. Type: string Parent: Condition Condition: Required when the ancestor element **Condition** is specified and sibling **HttpErrorCodeReturnedEquals** is not specified. If two conditions are specified, both conditions must be true for the **Redirect** to be applied.	No
HttpErrorCodeReturnedEquals	HTTP error code returned after the **Redirect** has taken effect. The specified **Redirect** is applied only when the error code returned equals this value. Example: • If you want to redirect requests to **NotFound.html** when HTTP error code 404 is returned, set HttpErrorCodeReturnedEquals to 404 in **Condition**, and set **ReplaceKeyWith** to **NotFound.html** in **Redirect**. Type: string Parent: Condition Condition: Required when ancestor element **Condition** is specified and sibling **KeyPrefixEquals** is not specified. If multiple conditions are specified, the **Redirect** takes effect only after all conditions are met.	No

Element	Description	Mandatory
Redirect	Element for redirection information. You can redirect requests to another host, to another web page, or with another protocol. You can specify an error code to be returned after an error. Type: container Parent: RoutingRule	Yes
Protocol	Protocol used in the redirection request Type: string Parent: Redirect Value options: **http**, **https** Condition: Not required if one of the siblings is present.	No
HostName	Host name used in the redirection request. Type: string Parent: Redirect Condition: Not required if one of the siblings is present.	No
ReplaceKeyPrefixWith	The object name prefix used in the redirection request. OBS replaces the value of **KeyPrefixEquals** with the value you specified here for **ReplaceKeyPrefixWith**. Example: To redirect all requests for **docs** (objects in the **docs** directory) to **documents** (objects in the **documents** directory), set **KeyPrefixEquals** to **docs** under **Condition** and **ReplaceKeyPrefixWith** to **documents** under **Redirect**. This way, requests for object **docs/a.html** will be redirected to **documents/a.html**. Type: string Parent: Redirect Condition: Not required if one of the siblings is present. Can be present only if ReplaceKeyWith is not provided.	No

Element	Description	Mandatory
ReplaceKeyWith	The object name used in the redirection request. OBS replaces the entire object name in the request with the value you specified here for **ReplaceKeyWith**. Example: To redirect requests for all objects in the **docs** directory to **documents/error.html**, set **KeyPrefixEquals** to **docs** under **Condition** and **ReplaceKeyWith** to **documents/error.html** under **Redirect**. This way, requests for both objects **docs/a.html** and **docs/b.html** will be redirected to **documents/error.html**. Type: string Parent: Redirect Condition: Not required if one of the siblings is present. Can be present only if **ReplaceKeyPrefixWith** is not provided.	No
HttpRedirectCode	HTTP status code returned after the redirection request Type: string Parent: Redirect Condition: Not required if one of the siblings is present.	No

Response Syntax

```
HTTP/1.1 status_code
Date: date
Content-Length: length
```

Response Headers

The response to the request uses common headers. For details, see **Table 3-19**.

Response Elements

This response contains no elements.

Error Responses

No special error responses are returned. For details about error responses, see **Table 6-2**.

Sample Request: Redirecting All Requests for a Bucket to Another Bucket or URL

```
PUT /?website HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
Date: WED, 01 Jul 2015 03:40:29 GMT
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:pUK7Yp0yebnq4P6gqzVjoS7whoM=
Content-Length: 194

<WebsiteConfiguration xmlns="http://obs.example.com/doc/2015-06-30/">
  <RedirectAllRequestsTo>
    <HostName>www.example.com</HostName>
  </RedirectAllRequestsTo>
</WebsiteConfiguration>
```

Sample Response: Redirecting All Requests for a Bucket to Another Bucket or URL

```
HTTP/1.1 200 OK
Server: OBS
x-obs-request-id: BF2600000164360D144670B9D02AABC6
x-obs-id-2: 32AAAQAAEAABSAAgAAEAABAAAQAAEAABCSItqMZ/AoFUX97l1xx8s67V3cCQtXWk
Date: WED, 01 Jul 2015 03:40:29 GMT
Content-Length: 0
```

5.3.2 Obtaining the Static Website Hosting Configuration of a Bucket

Functions

You can perform this operation to get the static website hosting configuration of a bucket.

To perform this operation, you must have the **GetBucketWebsite** permission. By default, only the bucket owner can perform this operation. The bucket owner can grant the permission to other users by configuring the bucket policy or user policy.

Request Syntax

```
GET /?website HTTP/1.1
Host: bucketname.obs.region.example.com
Date: date
Authorization: authorization
```

Request Parameters

This request contains no message parameters.

Request Headers

This request uses common headers. For details, see **Table 3-3**.

Request Elements

This request involves no elements.

Response Syntax

```
HTTP/1.1 status_code
Date: date
Content-Type: type
Content-Length: length
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<WebsiteConfiguration xmlns="http://obs.region.example.com/doc/2015-06-30/">
   <RedirectAllRequestsTo>
      <HostName>hostName</HostName>
   </RedirectAllRequestsTo>
</WebsiteConfiguration>
```

Response Headers

The response to the request uses common headers. For details, see **Table 3-19**.

Response Elements

This response contains elements the same as those used by the PutBucketWebsite request. For details, see **Request Elements**.

Error Responses

Table 5-44 describes possible special errors in this request.

Table 5-44 Special error

Error Code	Description	HTTP Status Code
NoSuchWebsiteConfiguration	The website configuration does not exist.	404 Not Found

For other errors, see **Table 6-2**.

Sample Request

```
GET /?website HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
Date: WED, 01 Jul 2015 03:41:54 GMT
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:Yxt1Ru+feHE0S94R7dcBp+hfLnI=
```

Sample Response

```
HTTP/1.1 200 OK
Server: OBS
x-obs-request-id: BF2600000164363442EC03A8CA3DD7F5
x-obs-id-2: 32AAAQAAEAABAAAQAAEAABAAAQAAEAABCSFbGOmlN0BVp1kbwN3har8jbVvtKEKN
Content-Type: application/xml
Date: WED, 01 Jul 2015 03:41:54 GMT
Content-Length: 250

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<WebsiteConfiguration xmlns="http://obs.region.example.com/doc/2015-06-30/">
  <RedirectAllRequestsTo>
    <HostName>www.example.com</HostName>
```



```
  </RedirectAllRequestsTo>
</WebsiteConfiguration>
```

5.3.3 Deleting the Static Website Hosting Configuration of a Bucket

Functions

You can perform this operation to delete the website configuration of a bucket.

To perform this operation, you must have the **DeleteBucketWebsite** permission. By default, only the bucket owner can perform this operation. The bucket owner can grant the permission to other users by configuring the bucket policy or user policy.

Request Syntax

```
DELETE /?website HTTP/1.1
Host: bucketname.obs.region.example.com
Date: date
Authorization: authorization
```

Request Parameters

This request contains no message parameters.

Request Headers

This request uses common headers. For details, see **Table 3-3**.

Request Elements

This request involves no elements.

Response Syntax

```
HTTP/1.1 status_code
Date: date
Content-Type: type
Content-Length: length
```

Response Headers

The response to the request uses common headers. For details, see **Table 3-19**.

Response Elements

This response contains no elements.

Error Responses

No special error responses are returned. For details about error responses, see **Table 6-2**.

Sample Request

```
DELETE /?website HTTP/1.1
User-Agent: curl/7.29.0
Host: bucketname.obs.region.example.com
Accept: */*
Date: WED, 01 Jul 2015 03:44:37 GMT
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:AZ1b0N5eLknxNOe/c0BISV1bEqc=
```

Sample Response

```
HTTP/1.1 204 No Content
Server: OBS
x-obs-request-id: BF260000016436378623OE2001DC0807
x-obs-id-2: 32AAAQAAEAABSAAgAAEAABAAAQAAEAABCSFUG4fEyDRgzUiEY2i71bJndBCy+wUZ
Date: WED, 01 Jul 2015 03:44:37 GMT
```

5.3.4 Configuring Bucket CORS

Functions

Cross-origin resource sharing (CORS) is a standard mechanism proposed by World Wide Web Consortium (W3C) and allows cross-origin requests from clients. For standard web page requests, the scripts and contents at one website cannot interact with those at another website due to the existence of the Same Origin Policy (SOP).

OBS allows buckets to store static web resources. The buckets of OBS can serve as website resources if the buckets are properly used (for details, see **Configuring Static Website Hosting for a Bucket**). A website in OBS can respond to requests of another websites only after CORS is properly configured.

Typical application scenarios are as follows:

- With the support of CORS, you can use JavaScript and HTML5 to construct web applications and directly access the resources in OBS without the need to use proxy servers for transfer.
- You can enable the dragging function of HTML 5 to directly upload files to the OBS (with the upload progress displayed) or update the OBS contents using web applications.
- Hosts external web pages, style sheets, and HTML 5 applications in different origins. Web fonts or pictures on OBS can be shared by multiple websites.

To perform this operation, you must have the **PutBucketCORS** permission. By default, only the bucket owner can perform this operation. The bucket owner can grant the permission to other users by configuring the bucket policy or user policy.

Request Syntax

```
PUT /?cors HTTP/1.1
Host: bucketname.obs.region.example.com
Content-Length: length
Date: date
Authorization: authorization
Content-MD5: MD5
<?xml version="1.0" encoding="UTF-8"?>
<CORSConfiguration>
   <CORSRule>
      <ID>id</ID>
      <AllowedMethod>method</AllowedMethod>
```



```
    <AllowedOrigin>origin</AllowedOrigin>
    <AllowedHeader>header</AllowedHeader>
    <MaxAgeSeconds>seconds</MaxAgeSeconds>
    <ExposeHeader>header</ExposeHeader>
  </CORSRule>
</CORSConfiguration>
```

Request Parameters

This request contains no parameters.

Request Headers

This request uses common headers and CORS request headers. For details, see **Table 3-3** and **Table 5-45**.

Table 5-45 CORS request header

Header	Description	Mandatory
Content-MD5	Base64-encoded 128-bit MD5 digest of the message according to RFC 1864 Type: string Example: **n58IG6hfM7vqI4K0vnWpog==**	Yes

Request Elements

In this request body, you must configure the CORS rules for a bucket in XML format. **Table 5-46** describes the specific configuration elements.

Table 5-46 CORS configuration elements

Element	Description	Mandatory
CORSConfiguration	Root node of **CORSRule** and its capacity cannot exceed 64 KB. Type: container Parent: none	Yes
CORSRule	CORS rules. **CORSConfiguration** can contain a maximum of 100 rules. Type: container Parent: CORSConfiguration	Yes
ID	Unique identifier of a rule. The value can contain a maximum of 255 characters. Type: string Parent: CORSRule	No

Element	Description	Mandatory
AllowedMethod	Method allowed by a CORS rule Type: string Value options: **GET**, **PUT**, **HEAD**, **POST**, **DELETE** Parent: CORSRule	Yes
AllowedOrigin	Origins that are allowed in the CORS rule. Only English domain names are supported for configuring origins, and regular expressions can be used for matching origins. Each **AllowedOrigin** allows one wildcard character (*) at most. Type: string Parent: CORSRule	Yes
AllowedHeader	Headers that are allowed in a PutBucketCORS request via the **Access-Control-Request-Headers** header. If a CORS request contains **Access-Control-Request-Headers**, this request is considered valid only when it matches the configuration of **AllowedHeader**. The match is based on regular expressions. Each **AllowedHeader** can contain at most one wildcard (*) and cannot contain spaces. Type: string Parent: CORSRule	No
MaxAgeSeconds	The time in seconds that the client can cache CORS responses. Each CORSRule can contain only one MaxAgeSeconds. It can be set to a negative value. Type: integer Parent: CORSRule	No
ExposeHeader	An additional header in CORS responses. The header provides additional information for clients. It cannot contain spaces. Type: string Parent: CORSRule	No

Response Syntax

```
HTTP/1.1 status_code

Date: date
Content-Length: length
```


Response Headers

The response to the request uses common headers. For details, see **Table 3-19**.

Response Elements

This response contains no elements.

Error Responses

No special error responses are returned. For details about error responses, see **Table 6-2**.

Sample Request

```
PUT /?cors HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
Date: WED, 01 Jul 2015 03:51:52 GMT
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:lq7BGoqE9yyhdEwE6KojJ7ysVxU=
Content-MD5: NGLzvw81f/A2C9PiGO0aZQ==
Content-Length: 617

<?xml version="1.0" encoding="utf-8"?>
<CORSConfiguration>
  <CORSRule>
    <AllowedMethod>POST</AllowedMethod>
    <AllowedMethod>GET</AllowedMethod>
    <AllowedMethod>HEAD</AllowedMethod>
    <AllowedMethod>PUT</AllowedMethod>
    <AllowedMethod>DELETE</AllowedMethod>
    <AllowedOrigin>www.example.com</AllowedOrigin>
    <AllowedHeader>AllowedHeader_1</AllowedHeader>
    <AllowedHeader>AllowedHeader_2</AllowedHeader>
    <MaxAgeSeconds>100</MaxAgeSeconds>
    <ExposeHeader>ExposeHeader_1</ExposeHeader>
    <ExposeHeader>ExposeHeader_2</ExposeHeader>
  </CORSRule>
</CORSConfiguration>
```

Sample Response

```
HTTP/1.1 100 Continue
HTTP/1.1 200 OK
Server: OBS
x-obs-request-id: BF26000001643627112BD03512FC94A4
x-obs-id-2: 32AAAQAAEAABSAAgAAEAABAAAQAAEAABCSYi6wLC4bkrvuS9sqnlRjxK2a5Fe3ry
Date: WED, 01 Jul 2015 03:51:52 GMT
Content-Length: 0
```

5.3.5 Obtaining the CORS Configuration of a Bucket

Functions

You can perform this operation to obtain CORS configuration information about a specified bucket.

To perform this operation, you must have the **GetBucketCORS** permission. By default, only the bucket owner can perform this operation. The bucket owner can grant the permission to other users by configuring the bucket policy or user policy.

Request Syntax

```
GET /?cors HTTP/1.1
Host: bucketname.obs.region.example.com
Date: date
Authorization: authorization
```

Request Parameters

This request contains no message parameters.

Request Headers

This request uses common headers. For details, see **Table 3-3**.

Request Elements

This request involves no elements.

Response Syntax

```
HTTP/1.1 status_code
Content-Type:  application/xml
Date: date
Content-Length: length

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<CORSConfiguration xmlns="http://obs.region.example.com/doc/2015-06-30/">
   <CORSRule>
      ...
   </CORSRule>
</CORSConfiguration>
```

Response Headers

The response to the request uses common headers. For details, see **Table 3-19**.

Response Elements

This response contains elements to detail the configuration. **Table 5-47** describes the elements.

Table 5-47 CORS configuration elements

Element	Description
CORSConfiguration	Root node of **CORSRules** and its capacity cannot exceed 64 KB. Type: container Parent: none
CORSRule	CORS rule. CORSConfiguration can contain a maximum of 100 rules. Type: container Parent: CORSConfiguration

Element	Description
ID	Unique identifier of a rule. The value can contain a maximum of 255 characters. Type: string Parent: CORSRule
AllowedMethod	Method allowed by a CORS rule. Type: string Value options: **GET**, **PUT**, **HEAD**, **POST**, **DELETE** Parent: CORSRule
AllowedOrigin	Indicates an origin that is allowed by a CORS rule. It is a character string and can contain a wildcard (*), and allows one wildcard character (*) at most. Type: string Parent: CORSRule
AllowedHeader	Indicates which headers are allowed in a PUT Bucket CORS request via the **Access-Control-Request-Headers** header. If a request contains **Access-Control-Request-Headers**, only a CORS request that matches the configuration of AllowedHeader is considered as a valid request. Each AllowedHeader can contain at most one wildcard (*) and cannot contain spaces. Type: string Parent: CORSRule
MaxAgeSeconds	Response time of CORS that can be cached by a client. It is expressed in seconds. Each CORSRule can contain only one MaxAgeSeconds. It can be set to a negative value. Type: integer Parent: CORSRule
ExposeHeader	Indicates a supplemented header in CORS responses. The header provides additional information for clients. It cannot contain spaces. Type: string Parent: CORSRule

Error Responses

Table 5-48 describes possible special errors in this request.

Table 5-48 Special error

Error Code	Description	HTTP Status Code
NoSuchCORSConfiguration	Indicates that the CORS configuration of buckets does not exist.	404 Not Found

For other errors, see **Table 6-2**.

Sample Request

```
GET /?cors HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
Date: WED, 01 Jul 2015 03:54:36 GMT
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:WJGghTrPQQXRuCx5go1fHyE+Wwg=
```

Sample Response

```
HTTP/1.1 200 OK
Server: OBS
x-obs-request-id: BF2600000164363593F10738B80CACBE
x-obs-id-2: 32AAAQAAEAABAAAQAAEAABAAAQAAEAABCSpngvwC5TskcLGh7Fz5KRmCFIayuY8p
Content-Type: application/xml
Date: WED, 01 Jul 2015 03:54:36 GMT
Content-Length: 825

<?xml version="1.0" encoding="utf-8"?>
<CORSConfiguration xmlns="http://obs.region.example.com/doc/2015-06-30/">
  <CORSRule>
    <ID>783fc6652cf246c096ea836694f71855</ID>
    <AllowedMethod>POST</AllowedMethod>
    <AllowedMethod>GET</AllowedMethod>
    <AllowedMethod>HEAD</AllowedMethod>
    <AllowedMethod>PUT</AllowedMethod>
    <AllowedMethod>DELETE</AllowedMethod>

    <AllowedOrigin>obs.example.com</AllowedOrigin>
    <AllowedOrigin>www.example.com</AllowedOrigin>
    <AllowedHeader>AllowedHeader_1</AllowedHeader>
    <AllowedHeader>AllowedHeader_2</AllowedHeader>
    <MaxAgeSeconds>100</MaxAgeSeconds>
    <ExposeHeader>ExposeHeader_1</ExposeHeader>
    <ExposeHeader>ExposeHeader_2</ExposeHeader>
  </CORSRule>
</CORSConfiguration>
```

5.3.6 Deleting the CORS Configuration of a Bucket

Functions

This operation is used to delete the CORS configuration of a bucket. After the CORS configuration is deleted, the bucket and objects in it cannot be accessed by requests from other websites.

To perform this operation, you must have the **PutBucketCORS** permission.

Request Syntax

```
DELETE /?cors HTTP/1.1
Host: bucketname.obs.region.example.com
Date: date
Authorization: authorization
```

Request Parameters

This request contains no message parameters.

Request Headers

This request uses common headers. For details, see **Table 3-3**.

Request Elements

This request involves no elements.

Response Syntax

```
HTTP/1.1 status_code
Date: date
Content-Type:  application/xml
Content-Length: length
```

Response Headers

The response to the request uses common headers. For details, see **Table 3-19**.

Response Elements

This response contains no elements.

Error Responses

No special error responses are returned. For details about error responses, see **Table 6-2**.

Sample Request

```
DELETE /?cors HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
Date: WED, 01 Jul 2015 03:56:41 GMT
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:mKUs/uIPb8BP0ZhvMd4wEy+EbiI=
```

Sample Response

```
HTTP/1.1 204 No Content
Server: OBS
x-obs-request-id: BF26000001643639F290185BB27F793A
x-obs-id-2: 32AAAQAAEAABSAAgAAEAABAAAQAAEAABCSLWMRFJfckapW+ktT/+1AnAz7XlNU0b
Date: WED, 01 Jul 2015 03:56:41 GMT
```


5.3.7 OPTIONS Bucket

Functions

OPTIONS refers to pre-requests that are sent to servers by clients. Generally, the requests are used to check whether clients have permissions to perform operations on servers. Only after a pre-request is returned successfully, clients start to execute the follow-up requests.

The OBS allows buckets to store static web resources. OBS buckets can serve as website resources if the buckets are properly used. In this scenario, buckets in the OBS serve as servers to process OPTIONS pre-requests from clients.

OBS can process OPTIONS pre-requests only after CORS is configured for buckets in OBS. For details about CORS, see **Configuring Bucket CORS**.

Differences Between OPTIONS Bucket and OPTIONS Object

With the OPTIONS Object, you need to specify an object name in the URL, but an object name is not required with the OPTIONS Bucket, which uses the bucket domain name as the URL. The request lines of the two methods are as follows:

```
OPTIONS /object HTTP/1.1
OPTIONS / HTTP/1.1
```

Request Syntax

```
OPTIONS / HTTP/1.1
Host: bucketname.obs.region.example.com
Date: date
Authorization: authorization
Origin: origin
Access-Control-Request-Method: method
```

Request Parameters

This request contains no message parameters.

Request Headers

This request uses the headers described in **Table 5-49**.

Table 5-49 OPTIONS request headers

Header	Description	Mandatory
Origin	Origin of the cross-domain request specified by the pre-request. Generally, it is a domain name set in CORS. Type: string	Yes
Access-Control-Request-Method	An HTTP method that can be used by a request. The request can use multiple method headers. Type: string Value options: **GET**, **PUT**, **HEAD**, **POST**, **DELETE**	Yes

Header	Description	Mandatory
Access-Control-Request-Headers	HTTP headers of a request. The request can use multiple HTTP headers. Type: string	No

Request Elements

This request involves no elements.

Response Syntax

```
HTTP/1.1 status_code
Content-Type: application/xml
Access-Control-Allow-Origin: origin
Access-Control-Allow-Methods: method
Access-Control-Allow-Header: header
Access-Control-Max-Age: time
Access-Control-Expose-Headers: header
Date: date
Content-Length: length
```

Response Headers

The response uses the following headers as described in **Table 5-50**.

Table 5-50 CORS response headers

Header	Description
Access-Control-Allow-Origin	If the origin of a request meets server CORS configuration requirements, the response contains the origin. Type: string
Access-Control-Allow-Headers	If the headers of a request meet server CORS configuration requirements, the response contains the headers. Type: string
Access-Control-Max-Age	Value of MaxAgeSeconds in the CORS configuration of a server Type: integer
Access-Control-Allow-Methods	If the Access-Control-Request-Method of a request meets server CORS configuration requirements, the response contains the methods in the rule. Type: string Value options: **GET**, **PUT**, **HEAD**, **POST**, **DELETE**

Header	Description
Access-Control-Expose-Headers	Value of ExposeHeader in the CORS configuration of a server Type: string

Response Elements

This response contains no elements.

Error Responses

Table 5-51 describes possible special errors in the request.

Table 5-51 Special error

Error Code	Description	HTTP Status Code
Bad Request	Invalid Access-Control-Request-Method: null When CORS and OPTIONS are configured for a bucket, no method header is added.	400 BadRequest
Bad Request	Insufficient information. Origin request header needed. When CORS and OPTIONS are configured for a bucket, no origin header is added.	400 BadRequest
AccessForbidden	CORSResponse: This CORS request is not allowed. This is usually because the evaluation of Origin, request method / Access-Control-Request-Method or Access-Control-Request-Headers are not whitelisted by the resource's CORS specification. When CORS and OPTIONS are configured for a bucket, origin, method, and headers do not match any rule.	403 Forbidden

For other errors, see Table 6-2.

Sample Request

```
OPTIONS / HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
```



```
Accept: */*
Date: WED, 01 Jul 2015 04:02:15 GMT
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:7RqP1vjemo6U+Adv9/Y6eGzWrzA=
Origin: www.example.com
Access-Control-Request-Method: PUT
```

Sample Response

```
HTTP/1.1 200 OK
Server: OBS
x-obs-request-id: BF260000016436314E8FF936946DBC9C
Access-Control-Allow-Origin: www.example.com
Access-Control-Allow-Methods: POST,GET,HEAD,PUT,DELETE
Access-Control-Max-Age: 100
Access-Control-Expose-Headers: ExposeHeader_1,ExposeHeader_2
Access-Control-Allow-Credentials: true
x-obs-id-2: 32AAAQAAEAABAAAQAAEAABAAAQAAEAABCTlYimJvOyJncCLNm5y/iz6MAGLNxTuS
Date: WED, 01 Jul 2015 04:02:15 GMT
Content-Length: 0
```

5.3.8 OPTIONS Object

Functions

For details, see **OPTIONS Bucket**.

Differences Between OPTIONS Bucket and OPTIONS Object

With the OPTIONS Object, you need to specify an object name in the URL, but an object name is not required with the OPTIONS Bucket, which uses the bucket domain name as the URL. The request lines of the two methods are as follows:

```
OPTIONS /object HTTP/1.1
OPTIONS / HTTP/1.1
```

Request Syntax

```
OPTIONS /object HTTP/1.1
Host: bucketname.obs.region.example.com
Date: date
Authorization: authorization
Origin: origin
Access-Control-Request-Method: method
```

Request Parameters

This request contains no message parameters.

Request Headers

Table 5-52 describes headers used by this request.

Table 5-52 OPTIONS request headers

Header	Description	Mandatory
Origin	Origin of the cross-domain request specified by the pre-request. Generally, it is a domain name set in CORS. Type: string	Yes
Access-Control-Request-Method	Indicates an HTTP method that can be used by a request. The request can use multiple method headers. Type: string Value options: **GET**, **PUT**, **HEAD**, **POST**, **DELETE**	Yes
Access-Control-Request-Headers	Indicates the HTTP headers of a request. The request can use multiple HTTP headers. Type: string	No

Request Elements

This request involves no elements.

Response Syntax

```
HTTP/1.1 status_code
Content-Type: type
Access-Control-Allow-Origin: origin
Access-Control-Allow-Methods: method
Access-Control-Allow-Header: header
Access-Control-Max-Age: time
Access-Control-Expose-Headers: header
Date: date
Content-Length: length
```

Response Headers

The request uses the headers described in **Table 5-53**.

Table 5-53 CORS request headers

Header	Description
Access-Control-Allow-Origin	If the origin of a request meets server CORS configuration requirements, the response contains the origin. Type: string
Access-Control-Allow-Headers	If the headers of a request meet server CORS configuration requirements, the response contains the headers. Type: string

Header	Description
Access-Control-Max-Age	Value of MaxAgeSeconds in the CORS configuration of a server. Type: integer
Access-Control-Allow-Methods	If the Access-Control-Request-Method of a request meets server CORS configuration requirements, the response contains the methods in the rule. Type: string Value options: **GET**, **PUT**, **HEAD**, **POST**, **DELETE**
Access-Control-Expose-Headers	Indicates ExposeHeader in the CORS configuration of a server. Type: string

Response Elements

This response contains no elements.

Error Responses

Table 5-54 describes possible special errors in the request.

Table 5-54 Special error

Error Code	Description	HTTP Status Code
Bad Request	Invalid Access-Control-Request-Method: null When CORS and OPTIONS are configured for a bucket, no method header is added.	400 BadRequest
Bad Request	Insufficient information. Origin request header needed. When CORS and OPTIONS are configured for a bucket, no origin header is added.	400 BadRequest

Error Code	Description	HTTP Status Code
AccessForbidden	CORSResponse: This CORS request is not allowed. This is usually because the evaluation of Origin, request method/Access-Control-Request-Method or Access-Control-Request-Headers are not whitelisted by the resource's CORS spec. When CORS and OPTIONS are configured for a bucket, origin, method, and headers do not match any rule.	403 Forbidden

For other errors, see **Table 6-2**.

Sample Request

```
OPTIONS /object_1 HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
Date: WED, 01 Jul 2015 04:02:19 GMT
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:bQZG9c2aokAJsHOOkuVBK6cHZZQ=
Origin: www.example.com
Access-Control-Request-Method: PUT
```

Sample Response

```
HTTP/1.1 200 OK
Server: OBS
x-obs-request-id: BF26000001643632D12EFCE1C1294555
Access-Control-Allow-Origin: www.example.com
Access-Control-Allow-Methods: POST,GET,HEAD,PUT,DELETE
Access-Control-Max-Age: 100
Access-Control-Expose-Headers: ExposeHeader_1,ExposeHeader_2
Access-Control-Allow-Credentials: true
x-obs-id-2: 32AAAQAAEAABAAAQAAEAABAAAQAAEAABCS+DXV4zZetbTqFehhEcuXywTa/mi3T3
Date: WED, 01 Jul 2015 04:02:19 GMT
Content-Length: 0
```

5.4 Operations on Objects

5.4.1 Uploading an Object - PUT

Functions

After creating a bucket in OBS, you can use this operation to upload an object to the bucket. This operation uploads an object to a bucket. To use this operation, you must have the write permission for the bucket.

NOTE

The name of each object in a bucket must be unique.

With versioning not enabled, if an object to be uploaded has the same name as an existing object in the bucket, the newly uploaded object will overwrite the existing one. To protect data from being corrupted during transmission, you can add the **Content-MD5** header in the request. After receiving the uploaded object, OBS compares the provided MD5 value to the MD5 value it calculates. If the two values do not match, OBS reports an error.

You can also specify the value of the **x-obs-acl** parameter to configure an access control policy for the object. If the **x-obs-acl** parameter is not specified when an anonymous user uploads an object, the object can be accessed by all OBS users by default.

This operation supports server-side encryption.

For a single upload, the size of the object to be uploaded ranges [0, 5 GB]. To upload a file greater than 5 GB, see **Operations on Multipart Upload**.

OBS does not have real folders. To facilitate data management, OBS provides a method to simulate a folder by adding a slash (/) to the object name, for example, **test/123.jpg**. You can simulate **test** as a folder and **123.jpg** as the name of a file under the **test** folder. However, the object key remains **test/123.jpg**. Objects named in this format appear as folders on the console. When you upload an object larger than 0 in size using this format, an empty folder will be displayed on the console, but the occupied storage capacity is the actual object size.

Differences Between PUT and POST 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
```

NOTE

In a PUT request, if you write the message body in POST format, the object uploaded to OBS will be displayed in a form.

For details about POST upload, see **Uploading an Object - POST**.

Versioning

If versioning is enabled for a bucket, the system automatically generates a unique version ID for the requested object in this bucket and returns the version ID in response header **x-obs-version-id**. If versioning is suspended for the bucket, the object version ID is **null**. For details about the versioning statuses of a bucket, see **Configuring Versioning for a Bucket**.

Request Syntax

```
PUT /ObjectName HTTP/1.1
Host: bucketname.obs.region.example.com
Content-Type: application/xml
Content-Length: length
Authorization: authorization
Date: date
<Optional Additional Header>
<object Content>
```

Request Parameters

This request contains no parameters.

Request Headers

This request uses common headers. For details, see **Table 3-3**. The request can use additional headers, as listed in **Table 5-55**.

NOTE

OBS supports the six HTTP request headers: Cache-Control, Expires, Content-Encoding, Content-Disposition, Content-Type, and Content-Language. If these headers are carried in an object upload request, their values are saved. You can also call the metadata modification API, provided by OBS, to change the values of the six headers. When the object is downloaded or queried, the saved values are set for corresponding HTTP headers and returned to the client.

Table 5-55 Request headers

Header	Description	Mandatory
Content-MD5	Base64-encoded 128-bit MD5 digest of the message according to RFC 1864. Type: string Example: **n58IG6hfM7vqI4K0vnWpog==**	No
x-obs-acl	This header can be added to set access control policies for objects when creating the objects. The access control policies are the predefined common policies, including **private**, **public-read**, **public-read-write**. Type: string Note: This header is a predefined policy expressed in a character string. Example: **x-obs-acl: public-read**	No

Header	Description	Mandatory
x-obs-grant-read	When creating an object, you can use this header to grant all users in an account the permissions to read the object and obtain the object metadata. Type: string Example: **x-obs-grant-read: id=domainID**. If multiple accounts are authorized, separate them with commas (,).	No
x-obs-grant-read-acp	When creating an object, you can use this header to grant all users in an account the permissions to obtain the object ACL. Type: string Example: **x-obs-grant-read-acp: id=domainID**. If multiple accounts are authorized, separate them with commas (,).	No
x-obs-grant-write-acp	When creating an object, you can use this header to grant all users in an account the permission to write the object ACL. Type: string Example: **x-obs-grant-write-acp: id=domainID**. If multiple accounts are authorized, separate them with commas (,).	No
x-obs-grant-full-control	When creating an object, you can use this header to grant all users in an account the permissions to read the object, obtain the object metadata and ACL, and write the object ACL. Type: string Example: **x-obs-grant-full-control: id=domainID**. If multiple accounts are authorized, separate them with commas (,).	No
x-obs-storage-class	When creating an object, you can use this header to specify the storage class for the object. If you do not use this header, the object storage class is the default storage class of the bucket. Type: string Storage class options: **STANDARD** (Standard), **WARM** (Warm), **COLD** (Cold). These values are case sensitive. Example: **x-obs-storage-class: STANDARD**	No

Header	Description	Mandatory
x-obs-meta-*	When creating an object, you can use a header starting with **x-obs-meta-** to define object metadata in an HTTP request. The user-defined metadata will be returned in the response when you retrieve the object or query the object metadata. Type: string Example: **x-obs-meta-test: test metadata** Constraint: Both user-defined metadata keys and their values must conform to US-ASCII standards.	No
x-obs-website-redirect-location	If a bucket is configured with the static website hosting function, it will redirect requests for this object to another object in the same bucket or to an external URL. OBS stores the value of this header in the object metadata. In the following example, the request header sets the redirection to an object (**anotherPage.html**) in the same bucket: x-obs-website-redirect-location:/anotherPage.html In the following example, the request header sets the object redirection to an external URL: x-obs-website-redirect-location:http://www.example.com/ Type: string Default value: none Constraint: The value must be prefixed by a slash (/), **http://**, or **https://**. The length of the value cannot exceed 2 KB.	No
x-obs-server-side-encryption	Indicates that SSE-KMS is used. Type: string Example: **x-obs-server-side-encryption: kms**	No. This header is required when SSE-KMS is used.

Header	Description	Mandatory
x-obs-server-side-encryption-kms-key-id	**Explanation**: The key used to encrypt objects. This header can be specified using either of the following formats: 1. *regionID*:*domainID*:**key/***key_id*: *regionID* indicates the ID of the region where the key belongs. *domainID* indicates the ID of the tenant where the key belongs. *key_id* indicates the ID of the key created in KMS on the DEW console. An example is given as follows: **x-obs-server-side-encryption-kms-key-id:** *region*:**exampledomainid: key/4f1cd4de-ab64-4807-920a-47fc42e7f0d0**. 2. *key_id*: It indicates the ID of the key created in KMS on the DEW console. An example is given as follows: **x-obs-server-side-encryption-kms-key-id: 4f1cd4de-ab64-4807-920a-47fc42e7f0d0**. **Restrictions**: This header can be used only when you set the **x-obs-server-side-encryption** header to **kms**. **Default value**: If you choose the KMS encryption but do not specify this header, the default master key will be used. If there is no such a default master key, OBS will create one and use it by default.	No
x-obs-server-side-encryption-customer-algorithm	Indicates the encryption algorithm when SSE-C is used. Type: string Example: **x-obs-server-side-encryption-customer-algorithm: AES256** Constraint: This header must be used together with **x-obs-server-side-encryption-customer-key** and **x-obs-server-side-encryption-customer-key-MD5**.	No. This header is required when SSE-C is used.
x-obs-server-side-encryption-customer-key	Indicates the key for encrypting objects when SSE-C is used. Type: string Example: **x-obs-server-side-encryption-customer-key:K7QkYpBkM5+hca27fsNkUnNVaobncnLht/rCB2o/9Cw=** Constraint: This header is a Base64-encoded 256-bit key and must be used together with **x-obs-server-side-encryption-customer-algorithm** and **x-obs-server-side-encryption-customer-key-MD5**.	No. This header is required when SSE-C is used.

Header	Description	Mandatory
x-obs-server-side-encryption-customer-key-MD5	Indicates the MD5 value of the encryption key when SSE-C is used. The MD5 value is used to check whether any error occurs during the transmission of the key. Type: string Example: **x-obs-server-side-encryption-customer-key-MD5:4XvB3tbNTN+tIEVa0/fGaQ==** Constraint: This header is a Base64-encoded 128-bit MD5 value and must be used together with **x-obs-server-side-encryption-customer-algorithm** and **x-obs-server-side-encryption-customer-key**.	No. This header is required when SSE-C is used.
success-action-redirect	Indicates the address (URL) to which a successfully responded request is redirected. • If the value is valid and the request is successful, OBS returns status code 303. **Location** contains **success_action_redirect** as well as the bucket name, object name, and object ETag. • If this parameter value is invalid, OBS ignores this parameter. In such case, the **Location** header is the object address, and OBS returns the response code based on whether the operation succeeds or fails. Type: string	No
x-obs-expires	Specifies when an object expires. It is measured in days. Once the object expires, it is automatically deleted. (The validity calculates from the object's creation time.) You can configure this field when uploading an object or modify this field by using the metadata modification API after the object is uploaded. Type: integer Example: **x-obs-expires:3**	No

Request Elements

This request contains no elements. Its body contains only the content of the requested object.

Response Syntax

```
HTTP/1.1 status_code
Content-Length: length
Content-Type: type
```


Response Headers

The response to the request uses common headers. For details, see **Table 3-19**.

In addition to the common response headers, the headers listed in **Table 5-56** may be used.

Table 5-56 Additional response headers

Header	Description
x-obs-version-id	Object version ID. If versioning is enabled for the bucket, the object version ID will be returned. Type: string
x-obs-server-side-encryption	This header is included in a response if SSE-KMS is used. Type: string Example: **x-obs-server-side-encryption:kms**
x-obs-server-side-encryption-kms-key-id	Indicates the master key ID. This header is included in a response when SSE-KMS is used. Type: string Format: *regionID*:*domainID*:**key/***key_id* *regionID* indicates the ID of the region where the key belongs. *domainID* indicates the ID of the tenant where the key belongs. *key_id* indicates the key ID used in this encryption. Example: **x-obs-server-side-encryption-kms-key-id:***region***:domainiddomainiddomainid-doma0001:key/4f1cd4de-ab64-4807-920a-47fc42e7f0d0**
x-obs-server-side-encryption-customer-algorithm	Indicates the encryption algorithm. This header is included in a response when SSE-C is used. Type: string Example: **x-obs-server-side-encryption-customer-algorithm: AES256**
x-obs-server-side-encryption-customer-key-MD5	Indicates the MD5 value of the key for encrypting objects. This header is included in a response when SSE-C is used. Type: string Example: **x-obs-server-side-encryption-customer-key-MD5:4XvB3tbNTN+tIEVa0/fGaQ==**

Header	Description
x-obs-storage-class	This header is returned when the storage class of an object is not Standard. The value can be **WARM** or **COLD**. Type: string

Response Elements

This response contains no elements.

Error Responses

No special error responses are returned. For details about error responses, see **Table 6-2**.

Sample Request: Uploading an Object

```
PUT /object01 HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
Date: WED, 01 Jul 2015 04:11:15 GMT
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:gYqplLq30dEX7GMi2qFWyjdFsyw=
Content-Length: 10240
Expect: 100-continue

[1024 Byte data content]
```

Sample Response: Uploading an Object

```
HTTP/1.1 200 OK
Server: OBS
x-obs-request-id: BF2600000164364C10805D385E1E3C67
ETag: "d41d8cd98f00b204e9800998ecf8427e"
x-obs-id-2: 32AAAWJAMAABAAAQAAEAABAAAQAAEAABCTzu4Jp2lquWuXsjnLyPPiT3cfGhqPoY
Date: WED, 01 Jul 2015 04:11:15 GMT
Content-Length: 0
```

Sample Request: Uploading an Object (with the ACL Configured)

```
PUT /object01 HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
Date: WED, 01 Jul 2015 04:13:55 GMT
x-obs-grant-read:id=52f24s3593as5730ea4f722483579ai7,id=a93fcas852f24s3596ea8366794f7224
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:gYqplLq30dEX7GMi2qFWyjdFsyw=
Content-Length: 10240
Expect: 100-continue

[1024 Byte data content]
```

Sample Response: Uploading an Object (with the ACL Configured)

```
HTTP/1.1 200 OK
Server: OBS
x-obs-request-id: BB7800000164845759E4F3B39ABEE55E
ETag: "d41d8cd98f00b204e9800998ecf8427e"
x-obs-id-2: 32AAAQAAEAABAAAQAAEAABAAAQAAEAABCSReVRNuas0knI+Y96iXrZA7BLUgj06Z
```



```
Date: WED, 01 Jul 2015 04:13:55 GMT
Content-Length: 0
```

Sample Request: Uploading an Object to a Versioned Bucket

```
PUT /object01 HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
Date: WED, 01 Jul 2015 04:17:12 GMT
x-obs-storage-class: WARM
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:uFVJhp/dJqj/CJIVLrSZ0gpw3ng=
Content-Length: 10240
Expect: 100-continue

[1024 Byte data content]
```

Sample Response: Uploading an Object to a Versioned Bucket

```
HTTP/1.1 200 OK
Server: OBS
x-obs-request-id: DCD2FC9CAB78000001439A51DB2B2577
ETag: "d41d8cd98f00b204e9800998ecf8427e"
X-OBS-ID-2: GcVgfeOJHx8JZHTHrRqkPsbKdB583fYbr3RBbHT6mMrBstReVILBZbMAdLiBYy1l
Date: WED, 01 Jul 2015 04:17:12 GMT
x-obs-version-id: AAABQ4q2M9_c0vycq3gAAAAAVURTRkha
Content-Length: 0
```

Sample Request: Uploading an Object (with Its MD5 Specified)

```
PUT /object01 HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
Date: WED, 01 Jul 2015 04:17:50 GMT
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:uFVJhp/dJqj/CJIVLrSZ0gpw3ng=
Content-Length: 10
Content-MD5: 6Afx/PgtEy+bsBjKZzihnw==
Expect: 100-continue

1234567890
```

Sample Response: Uploading an Object (with Its MD5 Specified)

```
HTTP/1.1 200 OK
Server: OBS
x-obs-request-id: BB7800000164B165971F91D82217D105
X-OBS-ID-2: 32AAAUJAIAABAAAQAAEAABAAAQAAEAABCSEKhBpS4BB3dSMNqMtuNxQDD9XvOw5h
ETag: "1072e1b96b47d7ec859710068aa70d57"
Date: WED, 01 Jul 2015 04:17:50 GMT
Content-Length: 0
```

Sample Request: Uploading an Object (with Website Hosting Configured)

If static website hosting has been configured for a bucket, you can configure parameters as follows when you upload an object. Then, users will be redirected when they download the object.

```
PUT /object01 HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
Date: WED, 01 Jul 2015 04:17:12 GMT
x-obs-website-redirect-location: http://www.example.com/
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:uFVJhp/dJqj/CJIVLrSZ0gpw3ng=
Content-Length: 10240
```



```
Expect: 100-continue

[1024 Byte data content]
```

Sample Response: Uploading an Object (with Website Hosting Configured)

```
HTTP/1.1 200 OK
Server: OBS
x-obs-request-id: DCD2FC9CAB78000001439A51DB2B2577
x-obs-id-2: 32AAAUJAIAABAAAQAAEAABAAAQAAEAABCTmxB5ufMj/7/GzP8TFwTbp33u0xhn2Z
ETag: "1072e1b96b47d7ec859710068aa70d57"
Date: WED, 01 Jul 2015 04:17:12 GMT
x-obs-version-id: AAABQ4q2M9_c0vycq3gAAAAAVURTRkha
Content-Length: 0
```

Sample Request: Uploading an Object Using a Signed URL

```
PUT /object02?
AccessKeyId=H4IPJX0TQTHTHEBQQCEC&Expires=1532688887&Signature=EQmDuOhaLUrzrzRNZxwS72CXeX
M%3D HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
Content-Length: 1024

[1024 Byte data content]
```

Sample Response: Uploading an Object Using a Signed URL

```
HTTP/1.1 200 OK
Server: OBS
x-obs-request-id: DCD2FC9CAB78000001439A51DB2B2577
x-obs-id-2: 32AAAUJAIAABAAAQAAEAABAAAQAAEAABCTmxB5ufMj/7/GzP8TFwTbp33u0xhn2Z
ETag: "1072e1b96b47d7ec859710068aa70d57"
Date: Fri, 27 Jul 2018 10:52:31 GMT
x-obs-version-id: AAABQ4q2M9_c0vycq3gAAAAAVURTRkha
Content-Length: 0
```

Sample Request: Uploading an Object (with a Storage Class Specified)

```
PUT /object01 HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
Date: WED, 01 Jul 2015 04:15:07 GMT
x-obs-storage-class: WARM
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:uFVJhp/dJqj/CJIVLrSZ0gpw3ng=
Content-Length: 10240
Expect: 100-continue

[1024 Byte data content]
```

Sample Response: Uploading an Object (with a Storage Class Specified)

```
HTTP/1.1 200 OK
Server: OBS
x-obs-request-id: BB7800000164846A2112F98BF970AA7E
ETag: "d41d8cd98f00b204e9800998ecf8427e"
x-obs-id-2: a39E0UgAIAABAAAQAAEAABAAAQAAEAABCTPOUJu5XlNyU32fvKjM/92MQZK2gtoB
Date: WED, 01 Jul 2015 04:15:07 GMT
Content-Length: 0
```


5.4.2 Uploading an Object - POST

Functions

This operation uploads an object to a bucket. To use this operation, you must have the write permission for the bucket.

NOTE

The name of each object in a bucket must be unique.

With versioning not enabled, if an object to be uploaded has the same name as an existing object in the bucket, the newly uploaded object will overwrite the existing one. To protect data from being corrupted during transmission, you can add the **Content-MD5** parameter in the form field. After receiving the uploaded object, OBS compares the provided MD5 value to the MD5 value it calculates. If the two values do not match, OBS reports an error. You can also specify the value of the **x-obs-acl** parameter to configure an access control policy for the object.

You can also upload an object using the POST method.

For a single upload, the size of the object to be uploaded ranges [0, 5 GB]. To upload a file greater than 5 GB, see **Operations on Multipart Upload**.

This operation supports server-side encryption.

Differences Between PUT and POST 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
```

For details about PUT upload, see **Uploading an Object - PUT**.

Versioning

If versioning is enabled for a bucket, the system automatically generates a unique version ID for the requested object in this bucket and returns the version ID in response header **x-obs-version-id**. If versioning is suspended for a bucket, the version ID of the requested object in this bucket is **null**. For details about the versioning statuses of a bucket, see **Configuring Versioning for a Bucket**.

Request Syntax

```
POST / HTTP/1.1
Host: bucketname.obs.region.example.com
User-Agent: browser_data
Accept: file_types
Accept-Language: Regions
Accept-Encoding: encoding
Accept-Charset: character_set
```



```
Keep-Alive: 300
Connection: keep-alive
Content-Type: multipart/form-data; boundary=9431149156168
Content-Length: length


--9431149156168
Content-Disposition: form-data; name="key"

acl
--9431149156168
Content-Disposition: form-data; name="success_action_redirect"

success_redirect
--9431149156168
Content-Disposition: form-data; name="content-Type"

content_type
--9431149156168
Content-Disposition: form-data; name="x-obs-meta-uuid"

uuid
--9431149156168
Content-Disposition: form-data; name="x-obs-meta-tag"

metadata
--9431149156168
Content-Disposition: form-data; name="AccessKeyId"

access-key-id
--9431149156168
Content-Disposition: form-data; name="policy"

encoded_policy
--9431149156168
Content-Disposition: form-data; name="signature"

signature=
--9431149156168
Content-Disposition: form-data; name="file"; filename="MyFilename"
Content-Type: image/jpeg

file_content
--9431149156168
Content-Disposition: form-data; name="submit"

Upload to OBS
--9431149156168--
```

Request Parameters

This request contains no parameters.

Request Headers

This request uses common headers. For details, see **Table 3-3**.

If you want to get CORS configuration information, you must use the headers in **Table 5-57**.

Table 5-57 Request headers for obtaining CORS configuration

Header	Description	Mandatory
Origin	Origin of the cross-domain request specified by the pre-request. Generally, it is a domain name. Type: string	Yes
Access-Control-Request-Headers	Indicates the HTTP headers of a request. The request can use multiple HTTP headers. Type: string	No

Request Elements

This request uses form elements. **Table 5-58** describes the form elements.

Table 5-58 Form elements

Parameter	Description	Mandatory
file	Specifies the object content uploaded. Both the file name and file path are ignored and will not be used as the object name. The object name is the value of parameter **key**. Type: binary content or text Constraint: This parameter must be the last parameter in a form. Otherwise, parameters after this parameter will be all discarded. Additionally, each request contains only one file parameter.	Yes
key	Indicates the name of the object to be created. Type: string	Yes
AccessKeyId	Access key ID (AK) of the requester. Type: string Constraint: This parameter is mandatory if there is security policy parameter **policy** or **signature** in the request.	Yes when the constraint is met.

Parameter	Description	Mandatory
policy	Indicates the security policy in the request. For details about the policy format, see the policy format in **Authentication of Signature Carried in the Table Uploaded Through a Browser**. Type: string Constraint: This parameter is mandatory if the bucket provides the **AccessKeyId** (or **signature**).	Yes when the constraint is met.
signature	Indicates a signature string calculated based on StringToSign. Type: string Constraint: This parameter is mandatory if the bucket provides the **AccessKeyId** (or **policy**).	Yes when the constraint is met.
token	Specifies the AK, signature, and security policy of the request initiator. The priority of a token is higher than that of a specified AK, the request signature, and the security policy of the request initiator. Type: string Example: In HTML: <input type= "text" name="token" value="ak:signature:policy" />	No
x-obs-acl	When creating an object, you can add this header to set the permission control policy for the object. The predefined common policies are as follows: **private**, **public-read**, **public-read-write**, **public-read-delivered**, and **public-read-write-delivered**. Type: string Examples: In POLICY: {"acl": "public-read" } In HTML: <input type="text" name="acl" value="public-read" />	No

Parameter	Description	Mandatory
x-obs-grant-read	When creating an object, you can use this header to grant all users in an account the permissions to read the object and obtain the object metadata. Type: string Examples: In POLICY: {'grant-read': 'id=domainId1' }, In HTML: <input type="text" name="grant-read" value="id=domainId1" />	No
x-obs-grant-read-acp	When creating an object, you can use this header to grant all users in an account the permission to obtain the object ACL. Type: string Examples: In POLICY: {"grant-read-acp": "id=domainId1" }, In HTML: <input type="text" name="grant-read-acp" value="id=domainId1" />	No
x-obs-grant-write-acp	When creating an object, you can use this header to grant all users in an account the permission to write the object ACL. Type: string Examples: In POLICY: {"grant-write-acp": "id=domainId1" }, In HTML: <input type="text" name="grant-write-acp" value="id=domainId1" />	No
x-obs-grant-full-control	When creating an object, you can use this header to grant all users in an account the permissions to read the object, obtain the object metadata and ACL, and write the object ACL. Type: string Examples: In POLICY: {"grant-full-control": "id=domainId1" }, In HTML: <input type="text" name="grant-full-control" value="id=domainId1" />	No

Parameter	Description	Mandatory
x-obs-storage-class	When creating an object, you can use this header to specify the storage class for the object. If you do not use this header, the object storage class is the default storage class of the bucket. Type: string Storage class options: **STANDARD** (Standard), **WARM** (Warm), **COLD** (Cold). These values are case sensitive. Examples: In POLICY: {"storage-class": "STANDARD" }, In HTML: <input type="text" name="x-obs-storage-class" value="STANDARD" />	No
Cache-Control, Content-Type, Content-Disposition, Content-Encoding Expires	Standard HTTP headers. OBS records those headers. If you download the object or send the HEAD Object request, those parameter values are returned. Type: string Examples: In POLICY: ["starts-with", "$Content-Type", "text/"], In HTML: <input type="text" name="content-type" value="text/plain" />	No
success_action_redirect	Indicates the address (URL) to which a successfully responded request is redirected. • If the value is valid and the request is successful, OBS returns status code 303. **Location** contains **success_action_redirect** as well as the bucket name, object name, and object ETag. • If this parameter value is invalid, OBS ignores this parameter. In such case, the **Location** header is the object address, and OBS returns the response code based on whether the operation succeeds or fails. Type: string Examples: In POLICY: {"success_action_redirect": "http://123458.com"}, In HTML: <input type="text" name="success_action_redirect" value="http://123458.com" />	No

Parameter	Description	Mandatory
x-obs-meta-*	Indicates user-defined metadata. When creating an object, you can use this header or a header starting with **x-obs-meta-** to define object metadata in an HTTP request. The user-defined metadata will be returned in the response when you retrieve the object or query the object metadata. Type: string Examples: In POLICY: {" x-obs-meta-test ": " test metadata " }, In HTML: <input type="text" name=" x-obs-meta-test " value=" test metadata " />	No
success_action_status	Indicates the status code returned after the request is successfully received. Possible values are **200**, **201**, and **204**. ● If this parameter is set to **200** or **204**, the body in the OBS response message is empty. ● If this parameter is set to **201**, the OBS response message contains an XML document that describes the response to the request. ● If the request does not include this parameter or the parameter value is invalid, OBS returns status code **204**. Type: string Examples: In POLICY: ["starts-with", "$success_action_status", ""], In HTML: <input type="text" name="success_action_status" value="200" />	No
x-obs-website-redirect-location	If a bucket is configured with the static website hosting function, it will redirect requests for this object to another object in the same bucket or to an external URL. OBS stores the value of this header in the object metadata. Default value: none Constraint: The value must be prefixed by a slash (/), **http://**, or **https://**. The length of the value cannot exceed 2 KB.	No

Parameter	Description	Mandatory
x-obs-server-side-encryption	Indicates that SSE-KMS is used. Type: string Example: **x-obs-server-side-encryption:kms**	No. This header is required when SSE-KMS is used.
x-obs-server-side-encryption-kms-key-id	Indicates the master key when SSE-KMS is used. If this header is not provided, the default master key will be used. If there is no such a default master key, OBS will create one and use it by default. Type: string The following two formats are supported: - *regionID*:*domainID*:**key/***key_id* 2. *key_id* *regionID* indicates the ID of the region where the key belongs. *domainID* indicates the ID of the tenant where the key belongs. *key_id* indicates the ID of the key created in KMS. Examples: - x-obs-server-side-encryption-kms-key-id: *region*:domainiddomainiddomainiddo-ma0001:key/4f1cd4de-ab64-4807-920a-47fc42e7f0d0 - x-obs-server-side-encryption-kms-key-id:4f1cd4de-ab64-4807-920a-47fc42e7f0d0	No
x-obs-server-side-encryption-customer-algorithm	Indicates the encryption algorithm when SSE-C is used. Type: string Example: **x-obs-server-side-encryption-customer-algorithm:AES256** Constraint: This header must be used together with **x-obs-server-side-encryption-customer-key** and **x-obs-server-side-encryption-customer-key-MD5**.	No. This header is required when SSE-C is used.

Parameter	Description	Mandatory
x-obs-server-side-encryption-customer-key	Indicates the key for encrypting objects when SSE-C is used. Type: string Example: **x-obs-server-side-encryption-customer-key:K7QkYpBkM5+hca27fsNkUnNVaobncnLht/rCB2o/9Cw=** Constraint: This header is a Base64-encoded 256-bit key and must be used together with **x-obs-server-side-encryption-customer-algorithm** and **x-obs-server-side-encryption-customer-key-MD5**.	No. This header is required when SSE-C is used.
x-obs-server-side-encryption-customer-key-MD5	Indicates the MD5 value of the encryption key when SSE-C is used. The MD5 value is used to check whether any error occurs during the transmission of the key. Type: string Example: **x-obs-server-side-encryption-customer-key-MD5:4XvB3tbNTN+tIEVa0/fGaQ==** Constraint: This header is a Base64-encoded 128-bit MD5 value and must be used together with **x-obs-server-side-encryption-customer-algorithm** and **x-obs-server-side-encryption-customer-key**.	No. This header is required when SSE-C is used.
x-obs-expires	Specifies when an object expires. It is measured in days. Once the object expires, it is automatically deleted. (The calculation starts from when the object was last modified). Type: integer Example: **x-obs-expires:3**	No

Response Syntax

```
HTTP/1.1 status_code
Content-Type: application/xml
Location: location
Date: date
ETag: etag
```

Response Headers

The response to the request uses common headers. For details, see **Table 3-19**.

In addition to the common response headers, the headers listed in **Table 5-59** may be used.

Table 5-59 Additional response headers

Header	Description
x-obs-version-id	Object version ID. If versioning is enabled for the bucket, the object version ID will be returned. A string **null** will be returned if the bucket housing the object has versioning suspended. Type: string
Access-Control-Allow-Origin	Indicates that the origin is included in the response if the origin in the request meets the CORS configuration requirements when CORS is configured for buckets. Type: string
Access-Control-Allow-Headers	Indicates that the headers are included in the response if headers in the request meet the CORS configuration requirements when CORS is configured for buckets. Type: string
Access-Control-Max-Age	Indicates MaxAgeSeconds in the CORS configuration of the server when CORS is configured for buckets. Type: integer
Access-Control-Allow-Methods	Indicates that methods in the rule are included in the response if Access-Control-Request-Method in the request meets the CORS configuration requirements when CORS is configured for buckets. Type: string Value options: **GET**, **PUT**, **HEAD**, **POST**, **DELETE**
Access-Control-Expose-Headers	Value of **ExposeHeader** in the CORS configuration of a server when CORS is configured for buckets. Type: string
x-obs-server-side-encryption	This header is included in a response if SSE-KMS is used. Type: string Example: **x-obs-server-side-encryption:kms**

Header	Description
x-obs-server-side-encryption-kms-key-id	Indicates the master key ID. This header is included in a response when SSE-KMS is used. Type: string Format: *regionID*:*domainID*:**key/***key_id* *regionID* indicates the ID of the region where the key belongs. *domainID* indicates the ID of the tenant where the key belongs. *key_id* indicates the key ID used in this encryption. Example: **x-obs-server-side-encryption-kms-key-id:***region***:domainiddomainiddomainid-doma0001:key/4f1cd4de-ab64-4807-920a-47fc42e7f0d0**
x-obs-server-side-encryption-customer-algorithm	Indicates the encryption algorithm. This header is included in a response when SSE-C is used. Type: string Example: **x-obs-server-side-encryption-customer-algorithm:AES256**
x-obs-server-side-encryption-customer-key-MD5	Indicates the MD5 value of the key for encrypting objects. This header is included in a response when SSE-C is used. Type: string Example: **x-obs-server-side-encryption-customer-key-MD5:4XvB3tbNTN+tIEVa0/fGaQ==**

Response Elements

This response contains no elements.

Error Responses

No special error responses are returned. For details about error responses, see **Table 6-2**.

Sample Request: Uploading an Object Using POST

```
POST / HTTP/1.1
Date: WED, 01 Jul 2015 04:15:23 GMT
Host: examplebucket.obs.region.example.com
Content-Type: multipart/form-data; boundary=7db143f50da2
Content-Length: 2424
Origin: www.example.com
Access-Control-Request-Headers:acc_header_1

--7db143f50da2
Content-Disposition: form-data; name="key"
```



```
object01
--7db143f50da2
Content-Disposition: form-data; name="acl"

public-read
--7db143f50da2
Content-Disposition: form-data; name="content-type"

text/plain
--7db143f50da2
Content-Disposition: form-data; name="expires"

WED, 01 Jul 2015 04:16:15 GMT
--7db143f50da2
Content-Disposition: form-data; name="AccessKeyId"

14RZT432N80TGDF2Y2G2
--7db143f50da2
Content-Disposition: form-data; name="policy"

ew0KICAiZXhaaXJhdGlvbiI6ICIyMDE1LTA3LTAxVDEyOjAwOjAwLjAwMFoiLA0KICAiY29uZGl0aW9ucyI6IFsNCiAgICB7ImJ1Y2tldCI6ICJleG1hcGxlYnVja2V0IiB9LA0KICAgIHsiYWNsIjogInB1YmxpYy1yZWFkIiB9LA0KICAgIHsiRXhhaXJlcyI6ICIxMDAwIiB9LA0KICAgIFsiZXEiLCAiJGtleSIsICJvYmplY3QwMSJdLA0KICAgIFsic3RhcnRzLXdpdGgiLCAiJENvbnRlbnQtVHlwZSIsICJ0ZXh0LyJdLA0KICBdDQp9DQo=
--7db143f50da2
Content-Disposition: form-data; name="signature"

Vk6rwO0Nq09BLhvNSIYwSJTRQ+k=
--7db143f50da2
Content-Disposition: form-data; name="x-obs-persistent-headers"

test:dmFsdWUx
--7db143f50da2
Content-Disposition: form-data; name="x-obs-grant-read"

id=52f24s3593as5730ea4f722483579xxx
--7db143f50da2
Content-Disposition: form-data; name="x-obs-server-side-encryption"

kms
--7db143f50da2
Content-Disposition: form-data; name="x-obs-website-redirect-location"

http://www.example.com/
--7db143f50da2
Content-Disposition: form-data; name="file"; filename="C:\Testtools\UpLoadFiles\object\1024Bytes.txt"
Content-Type: text/plain

01234567890
--7db143f50da2
Content-Disposition: form-data; name="submit"

Upload
--7db143f50da2--
```

Sample Response: Uploading an Object Using POST

After CORS is configured for a bucket, the response contains the **Access-Control-*** information.

```
HTTP/1.1 204 No Content
x-obs-request-id: 90E2BA00C26C00000133B442A90063FD
x-obs-id-2: OTBFMkJBMDBDMjZDMDAwMDAxMzNCNDQyQTkwMDYzRkRBQUFBQUFBQWJiYmJiYmJi
Access-Control-Allow-Origin: www.example.com
Access-Control-Allow-Methods: POST,GET,HEAD,PUT
Access-Control-Allow-Headers: acc_header_01
Access-Control-Max-Age: 100
Access-Control-Expose-Headers: exp_header_01
Content-Type: text/xml
```



```
Location: http://examplebucket.obs.region.example.com/object01
Date: WED, 01 Jul 2015 04:15:23 GMT
ETag: "ab7abb0da4bca5323ab6119bb5dcd296"
```

Sample Request: Uploading an Object (with x-obs-acl and a Storage Class Specified)

Upload an object with the x-obs-acl, storage class, and redirection header fields carried in the request message.

Before encoding, the policy content is as follows:

```
{
   "expiration":"2018-07-17T04:54:35Z",
   "conditions":[
      {
         "content-type":"text/plain"
      },
      {
         "x-obs-storage-class":"WARM"
      },
      {
         "success_action_redirect":"http://www.example.com"
      },
      {
         "x-obs-acl":"public-read"
      },
      [
         "starts-with",
         "$bucket",
         ""
      ],
      [
         "starts-with",
         "$key",
         ""
      ]
   ]
}
```

Sample request:

```
POST / HTTP/1.1
Host: examplebucket.obs.region.example.com
Accept-Encoding: identity
Content-Length: 947
Content-Type: multipart/form-data; boundary=9431149156168
User-Agent: OBS/Test

--9431149156168
Content-Disposition: form-data; name="x-obs-acl"

public-read
--9431149156168
Content-Disposition: form-data; name="AccessKeyId"

H4IPJX0TQTHTHEBQQCEC
--9431149156168
Content-Disposition: form-data; name="key"

my-obs-object-key-demo
--9431149156168
Content-Disposition: form-data; name="signature"

WNwv8P1ZiWdqPQqjXeLmAfzPDAI=
--9431149156168
Content-Disposition: form-data; name="policy"
```



```
eyJleHBpcmF0aW9uIjoiMjAxOC0wNy0xN1QwODozNDoyM1oiLCAiY29uZGl0aW9ucyI6W3siY29udGVudC10eX
BlIjoidGV4dC9wbGFpbiJ9LHsieC1vYnMtYWNsIjoicHVibGljLXJlYWQifSxbInN0YXJ0cy13aXRoIiwgIiRidWNrZXQiL
CAiIl0sWyJzdGFydHMtd2l0aCIsICIka2V5IiwgIiJdXX0=
--9431149156168
Content-Disposition: form-data; name="content-type"

text/plain
--9431149156168
Content-Disposition: form-data; name="file"; filename="myfile"
Content-Type: text/plain

c2c6cd0f-898e-11e8-aab6-e567c91fb541
52b8e8a0-8481-4696-96f3-910635215a78

--9431149156168--
```

Sample Response: Uploading an Object (with x-obs-acl and a Storage Class Specified)

```
HTTP/1.1 204 No Content
Server: OBS
Location: http://examplebucket.obs.region.example.com/my-obs-object-key-demo
ETag: "17a83fc8d431273405bd266114b7e034"
x-obs-request-id: 5DEB00000164A728A7C7F4E032214CFA
x-obs-id-2: 32AAAUJAIAABAAAQAAEAABAAAQAAEAABCSwj2PcBE0YcoLHUDO7GSj+rVByzjflA
Date: Tue, 17 Jul 2018 07:33:36 GMT
```

Sample Request: Using a Token for Authentication

```
POST / HTTP/1.1
Content-Type:multipart/form-data; boundary=9431149156168
Content-Length: 634
Host: examplebucket.obs.region.example.com

--9431149156168
Content-Disposition: form-data; name="key"
obj01

--9431149156168
Content-Disposition: form-data; name="token"
UDSIAMSTUBTEST002538:XsVcTzR2/
A284oE4VH9qPndGcuE=:eyJjb25kaXRpb25zIjogW3siYnVja2V0IjogInRlc3QzMDAzMDU4NzE2NjI2ODkzNjcuMT
IifSwgeyJDb250ZW50LVR5cGUiOiAiYXBwbGljYXRpb24veG1sIn0sIFsiZXEiLCAiJGtleSIsICJvYmoudHh0Il1dLCAiZ
XhwaXJhdGlvbiI6ICIyMDIyLTA5LTA5VDEyOjA5OjI3WiJ9

--9431149156168
Content-Disposition: form-data; name="file"; filename="myfile"
Content-Type: text/plain
01234567890

--9431149156168--
Content-Disposition: form-data; name="submit"
Upload to OBS
```

Sample Response: Using a Token for Authentication

```
HTTP/1.1 204 No Content
Server: OBS
Location: http://examplebucket.obs.region.example.com/my-obs-object-key-demo
ETag: "7eda50a430fed940023acb9c4c6a2fff"
x-obs-request-id: 000001832010443D80F30B649B969C47
x-obs-id-2: 32AAAUgAIAABAAAQAAEAABAAAQAAEAABCTj0yO9KJd5In+i9pzTgCDVG9vMnk7O/
Date: Fri,09Sep 2022 02: 24:40 GMT
```

Sample Request: Specifying an Object Expiration Time

```
POST / HTTP/1.1
Date: WED, 01 Jul 2015 04:15:23 GMT
```



```
Host: examplebucket.obs.region.example.com
Content-Type: multipart/form-data; boundary=14882896926023390562087O
Content-Length: 1639
Origin: www.example.com
Access-Control-Request-Headers:acc_header_1

--14882896926023390562087O
Content-Disposition: form-data; name="key"

object01
--14882896926023390562087O
Content-Disposition: form-data; name="ObsAccessKeyId"

55445349414d535455425445535430303030303
--14882896926023390562087O
Content-Disposition: form-data; name="signature"

396246666f6f42793872792f7a3958524f6c44334e4e69763950553d--7db143f50da2
--14882896926023390562087O
Content-Disposition: form-data; name="policy"

65794a6c65484270636d463061573975496a6f694d6a41794d7930774e6930784e565178...
--14882896926023390562087O
Content-Disposition: form-data; name="x-obs-expires"

4
--14882896926023390562087O
Content-Disposition: form-data; name="file"; filename="test.txt"
Content-Type: text/plain

01234567890
--14882896926023390562087O
Content-Disposition: form-data; name="submit"

Upload
--14882896926023390562087O--
```

Sample Response: Specifying an Object Expiration Time

```
HTTP/1.1 204 No Content
Server: OBS
Date: Thu, 15 Jun 2023 12:39:03 GMT
Connection: keep-alive
Location: http://examplebucket.obs.region.example.com/my-obs-object-key-demo
x-obs-expiration: expiry-date="Tue, 20 Jun 2023 00:00:00 GMT"
ETag: "d41d8cd98f00b204e9800998ecf8427e"
x-obs-request-id: 00000188BF11049553064911000FC30D
x-obs-id-2: 32AAAUJAIAABAAAQAAEAABAAAQAAEAABCSwj2PcBE0YcoLHUDO7GSj+rVByzjflA
x-forward-status: 0x40020000000001
x-dae-api-type: REST.POST.OBJECT
```

Sample Request: Specifying a Status Code

Set the status code of a successful action to 200.

```
POST /srcbucket HTTP/1.1
User-Agent: PostmanRuntime/7.26.8
Accept: */*
Postman-Token: 667dcc44-1c48-41ba-9e41-9f87d8975089
Host: obs.region.example.com
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Content-Type: multipart/form-data; boundary=--------------------------285613759795901770404350
Content-Length: 1134

----------------------------285613759795901770404350
Content-Disposition: form-data; name="key"
```



```
obj
----------------------------2856137597959017704043 50
Content-Disposition: form-data; name="ObsAccessKeyId"

XXXXXXXXXXXXXXX000003
----------------------------2856137597959017704043 50
Content-Disposition: form-data; name="signature"

9rc4bVhDPQ7eHtw17hWtYxLnBWU=
----------------------------2856137597959017704043 50
Content-Disposition: form-data; name="policy"

eyJleHBpcmF0aW9uIjoiMjAyMy0wNi0xNVQxNDoxMTozNFoiLCAiY29uZGl0aW9ucyI6W3siYnVja2V0Ijoic3JjYnV
ja2V0MiJ9LHsic3VjY2Vzc19hY3Rpb25fc3RhdHVzIjoiMjAwIn0seyJjb250ZW50LXR5cGUiOiJ0ZXh0L3BsYWluIn0s
eyJrZXkiOiIzMzMifSxdfQ==
----------------------------2856137597959017704043 50
Content-Disposition: form-data; name="success_action_status"

200
----------------------------2856137597959017704043 50
Content-Disposition: form-data; name="file"; filename="test.txt"
Content-Type: text/plain


----------------------------2856137597959017704043 50
Content-Disposition: form-data; name="submit"

Upload to OBS
----------------------------2856137597959017704043 50--
```

Sample Response: Specifying a Status Code

Response to the configuration of success status code 200

```
HTTP/1.1 200 OK
Server: OBS
Date: Thu, 15 Jun 2023 13:12:51 GMT
Content-Length: 0
Connection: keep-alive
Location: http://obs.region.example.com/srcbucket/obj
ETag: "d41d8cd98f00b204e9800998ecf8427e"
x-obs-request-id: 00000188BF2FF55F5306426E000FE366
x-obs-id-2: 32AAAUJAIAABAAAQAAEAABAAAQAAEAABCScDjcXgZ7oMYSVnZnk4+HrClVwLVPTi
x-forward-status: 0x40020000000001
x-dae-api-type: REST.POST.OBJECT
```

5.4.3 Copying an Object

Functions

You can perform this operation to create a copy of an existing object in OBS.

Users can determine whether to copy the metadata of the source object to the target object (by default) or replace the metadata of the target object with the metadata contained in the request. The ACL of the source object is not copied to the target object. By default, the ACL of the target object is private. You can set an ACL for the target object by sending an API request.

The request for copying an object needs to carry the information about the bucket and object to be copied in the header field. The message body cannot be carried.

This operation supports server-side encryption.

An object copy can be up to 5 GB in size. If the source object size exceeds 5 GB, you can only **copy part of the object**.

NOTE

You cannot determine whether a request is executed successfully only using **status_code** in the header returned by HTTP. If 200 in **status_code** is returned, the server has received the request and starts to process the request. The body in the response shows whether the copy succeeds. If the body contains ETag, the copy succeeds. Otherwise, the copy failed.

Versioning

By default, **x-obs-copy-source** specifies the latest version of the source object. If the latest version of the source object is a delete marker, the object is considered deleted. You can add **versionId** to request header **x-obs-copy-source** to copy an object with the specified version ID.

If a bucket has versioning enabled, the system automatically generates a unique version ID for the requested object in this bucket and returns the version ID in response header **x-obs-version-id**. If versioning is suspended for the bucket, the object version ID is **null**.

NOTICE

When the bucket versioning status is disabled, if you make a copy of object_A and save it as object_B, and an object named as object_B already exists, the new object_B will overwrite the existing one. After the copying is executed successfully, only new object_B can be downloaded because old object_B has been deleted. Therefore, before copying an object, ensure that there is no object with the same name as the object copy to prevent data from being deleted mistakenly. During the copying, object_A has no changes.

Cold Objects

If source objects are in the Cold storage class, ensure that these objects have been restored before you copy them. If a source object is not restored or is being restored, its copy will fail and error **403 Forbidden** will be returned. The fault is described as follows:

ErrorCode: InvalidObjectState

ErrorMessage: Operation is not valid for the source object's storage class

Request Syntax

```
PUT /destinationObjectName HTTP/1.1
Host: bucketname.obs.region.example.com
x-obs-copy-source: /sourceBucket/sourceObject
x-obs-metadata-directive: metadata_directive
x-obs-copy-source-if-match: etag
x-obs-copy-source-if-none-match: etag
x-obs-copy-source-if-unmodified-since: time_stamp
x-obs-copy-source-if-modified-since: time_stamp
Authorization: signature
Date: date
```


Request Parameters

This request contains no parameters.

Request Headers

You can add optional headers to specify the object to be copied. **Table 3-3** describes the optional headers.

Table 5-60 Request headers

Header	Description	Mandatory
x-obs-acl	When copying an object, you can add this header to configure the object ACL using the predefined common policies, including **private**, **public-read**, and **public-read-write**. Type: string Example: **x-obs-acl: acl**	No
x-obs-grant-read	When creating an object, you can use this header to grant all users in an account the permissions to read the object and obtain the object metadata. Type: string	No
x-obs-grant-read-acp	When creating an object, you can use this header to grant all users in an account the permission to obtain the object ACL. Type: string	No
x-obs-grant-write-acp	When creating an object, you can use this header to grant all users in an account the permission to write the object ACL. Type: string	No
x-obs-grant-full-control	When creating an object, you can use this header to grant all users in an account the permissions to read the object, obtain the object metadata and ACL, and write the object ACL. Type: string	No
x-obs-copy-source	Indicates names of the source bucket and the source object. If the source object has multiple versions, the versionId parameter can be used to specify the desired version. Type: string Constraint: URL encoding is required for handling full-width characters and %. Example: **x-obs-copy-source: /source_bucket/sourceObject**	Yes

Header	Description	Mandatory
x-obs-metadata-directive	Indicates whether the metadata of the target object is copied from the source object or replaced with the metadata contained in the request. Type: string Valid values: COPY and REPLACE Default value: COPY Example: **x-obs-metadata-directive: metadata_directive** Constraints: Values other than **COPY** or **REPLACE** result in an immediate 400-based error response. If you need to modify the metadata (the same for both the source and target objects), this parameter must be set to **REPLACE**, otherwise, the request is invalid and the server returns a 400 HTTP status code error. This parameter cannot be used to change an encrypted object to a non-encrypted object (the same for both the source and target objects). If you use this parameter to change the encrypted object, the system returns 400.	No
x-obs-copy-source-if-match	Indicates that the source object is copied only if its ETag matches the one specified in this header. Otherwise, a 412 status code (failed precondition) is returned. Type: string Example: **x-obs-copy-source-if-match: etag** Constraint: This header can be used with **x-obs-copy-source-if-unmodified-since** but not other conditional copy headers.	No
x-obs-copy-source-if-none-match	Indicates that the source object is copied only if its ETag does not match the one specified in this header. Otherwise, a 412 status code (failed precondition) is returned. Type: string Example: **x-obs-copy-source-if-none-match: etag** Constraint: This parameter can be used with **x-obs-copy-source-if-modified-since** but not other conditional copy parameters.	No

Header	Description	Mandatory
x-obs-copy-source-if-unmodified-since	Indicates that the source object is copied only if it has not been modified since the time specified by this header. Otherwise, error code 412 (failed precondition) is returned. This header can be used with **x-obs-copy-source-if-match**, but cannot be used with other conditional copy headers. Type: string Format: HTTP time string complying with the format specified at **http://www.ietf.org/rfc/rfc2616.txt**, which can be any of the following: 1. **EEE, dd MMM yyyy HH:mm:ss z** 2. **EEEE, dd-MMM-yy HH:mm:ss z** 3. **EEE MMM dd HH:mm:ss yyyy** Examples: 1. **x-obs-copy-source-if-unmodified-since: Sun, 06 Nov 1994 08:49:37 GMT** 2. **x-obs-copy-source-if-unmodified-since: Sunday, 06-Nov-94 08:49:37 GMT** 3. **x-obs-copy-source-if-unmodified-since: Sun Nov 6 08:49:37 1994** Constraint: The time specified by this header cannot be later than the current server time (GMT time), or this header does not take effect.	No

Header	Description	Mandatory
x-obs-copy-source-if-modified-since	Indicates that the source object is copied only if it has been modified since the time specified by this header. Otherwise, error code 412 (failed precondition) is returned. This header can be used with **x-obs-copy-source-if-none-match**, but cannot be used with other conditional copy headers. Type: string Format: HTTP time string complying with the format specified at **http://www.ietf.org/rfc/rfc2616.txt**, which can be any of the following: 1. **EEE, dd MMM yyyy HH:mm:ss z** 2. **EEEE, dd-MMM-yy HH:mm:ss z** 3. **EEE MMM dd HH:mm:ss yyyy** Examples: 1. **x-obs-copy-source-if-unmodified-since: Sun, 06 Nov 1994 08:49:37 GMT** 2. **x-obs-copy-source-if-unmodified-since: Sunday, 06-Nov-94 08:49:37 GMT** 3. **x-obs-copy-source-if-unmodified-since: Sun Nov 6 08:49:37 1994** Constraint: The time specified by this header cannot be later than the current server time (GMT time), or this header does not take effect.	No
x-obs-storage-class	When copying an object, you can use this header to specify the storage class for the object. If you do not use this header, the object storage class is the default storage class of the destination bucket where the object is copied to. Type: string Storage class options: **STANDARD** (Standard), **WARM** (Warm), **COLD** (Cold). These values are case sensitive. Example: **x-obs-storage-class: STANDARD**	No

Header	Description	Mandatory
x-obs-website-redirect-location	If a bucket is configured with the static website hosting function, it will redirect requests for this object to another object in the same bucket or to an external URL. OBS stores the value of this header in the object metadata. Type: string Default value: none Constraint: The value must be prefixed by a slash (/), **http://**, or **https://**. The length of the value cannot exceed 2 KB.	No
x-obs-server-side-encryption	Indicates that SSE-KMS is used. Objects are encrypted using SSE-KMS. Type: string Example: **x-obs-server-side-encryption: kms**	No. This header is required when SSE-KMS is used.
x-obs-server-side-encryption-kms-key-id	Indicates the master key for encrypting the object copy when SSE-KMS is used. If this header is not provided, the default master key will be used. If there is no such a default master key, OBS will create one and use it by default. Type: string The following two formats are supported: - *regionID*:*domainID*:**key/***key_id* 2. *key_id* *regionID* indicates the ID of the region where the key belongs. *domainID* indicates the ID of the tenant where the key belongs. *key_id* indicates the ID of the key created in KMS. Example: - **x-obs-server-side-encryption-kms-key-id: *region*:domainiddomainiddomainiddo-ma0001:key/4f1cd4de-ab64-4807-920a-47fc42e7f0d0** - **x-obs-server-side-encryption-kms-key-id: 4f1cd4de-ab64-4807-920a-47fc42e7f0d0**	No

Header	Description	Mandatory
x-obs-server-side-encryption-customer-algorithm	Indicates the encryption algorithm for the object copy when SSE-C is used. Type: string Example: **x-obs-server-side-encryption-customer-algorithm: AES256** Constraint: This header must be used together with **x-obs-server-side-encryption-customer-key** and **x-obs-server-side-encryption-customer-key-MD5**.	No. This header is required when SSE-C is used.
x-obs-server-side-encryption-customer-key	Indicates the key for encrypting the object copy when SSE-C is used. Type: string Example: **x-obs-server-side-encryption-customer-key:K7QkYpBkM5+hca27fsNkUnNVaobncnLht/rCB2o/9Cw=** Constraint: This header is a Base64-encoded 256-bit key and must be used together with **x-obs-server-side-encryption-customer-algorithm** and **x-obs-server-side-encryption-customer-key-MD5**.	No. This header is required when SSE-C is used.
x-obs-server-side-encryption-customer-key-MD5	Indicates the MD5 value of the key for encrypting the object copy when SSE-C is used. The MD5 value is used to check whether any error occurs during the transmission of the key. Type: string Example: **x-obs-server-side-encryption-customer-key-MD5:4XvB3tbNTN+tIEVa0/fGaQ==** Constraint: This header is a Base64-encoded 128-bit MD5 value and must be used together with **x-obs-server-side-encryption-customer-algorithm** and **x-obs-server-side-encryption-customer-key**.	No. This header is required when SSE-C is used.
x-obs-copy-source-server-side-encryption-customer-algorithm	Indicates the algorithm for decrypting the source object when SSE-C is used. Type: string Example: x-obs-copy-source-server-side-encryption-customer-algorithm: AES256 Constraint: This header must be used together with **x-obs-copy-source-server-side-encryption-customer-key** and **x-obs-copy-source-server-side-encryption-customer-key-MD5**.	No. This header is required when SSE-C is used to copy a source object.

Header	Description	Mandatory
x-obs-copy-source-server-side-encryption-customer-key	Indicates the key for decrypting the source object when SSE-C is used. Type: string Example: **x-obs-copy-source-server-side-encryption-customer-key: K7QkYpBkM5+hca27fsNkUnNVaobncnLht/rCB2o/9Cw=** Constraint: This header is a Base64-encoded 256-bit key and must be used together with **x-obs-copy-source-server-side-encryption-customer-algorithm** and **x-obs-copy-source-server-side-encryption-customer-key-MD5**.	No. This header is required when SSE-C is used to copy a source object.
x-obs-copy-source-server-side-encryption-customer-key-MD5	Indicates the MD5 value of the key for decrypting the source object when SSE-C is used. The MD5 value is used to check whether any error occurs during the transmission of the key. Type: string Example: **x-obs-copy-source-server-side-encryption-customer-key-MD5:4XvB3tbNTN+tIEVa0/fGaQ==** Constraint: This header is a Base64-encoded 128-bit MD5 value and must be used together with **x-obs-copy-source-server-side-encryption-customer-algorithm** and **x-obs-copy-source-server-side-encryption-customer-key**.	No. This header is required when SSE-C is used to copy a source object.
success_action_redirect	Indicates the address (URL) to which a successfully responded request is redirected. • If the value is valid and the request is successful, OBS returns status code 303. **Location** contains **success_action_redirect** as well as the bucket name, object name, and object ETag. • If this parameter value is invalid, OBS ignores this parameter. In such case, the **Location** header is the object address, and OBS returns the response code based on whether the operation succeeds or fails. Type: string	No

For details about other headers, see **Table 3-3**.

Request Elements

This request contains no elements.

Response Syntax

```
HTTP/1.1 status_code
Content-Type: application/xml
Date: date
Content-Length: length

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<CopyObjectResult xmlns="http://obs.region.example.com/doc/2015-06-30/">
   <LastModified>modifiedDate</LastModified>
   <ETag>etagValue</ETag>
</CopyObjectResult>
```

Response Headers

The response to the request uses common headers. For details, see **Table 3-19**.

In addition to the common response headers, the headers listed in **Table 5-61** may be used.

Table 5-61 Additional response headers

Header	Description
x-obs-copy-source-version-id	Version ID of the source object Type: string
x-obs-version-id	Version ID of the target object Type: string
x-obs-server-side-encryption	This header is included in a response if SSE-KMS is used. Type: string Example: **x-obs-server-side-encryption: kms**
x-obs-server-side-encryption-kms-key-id	Indicates the master key ID. This header is included in a response when SSE-KMS is used. Type: string Format: *regionID*:*domainID*:**key/***key_id* *regionID* indicates the ID of the region where the key belongs. *domainID* indicates the ID of the tenant where the key belongs. *key_id* indicates the key ID used in this encryption. Example: x-obs-server-side-encryption-kms-key-id: *region*:domainiddomainiddomainiddo-ma0001:key/4f1cd4de-ab64-4807-920a-47fc42e7f0d0

Header	Description
x-obs-server-side-encryption-customer-algorithm	Indicates the encryption algorithm. This header is included in a response when SSE-C is used. Type: string Example: **x-obs-server-side-encryption-customer-algorithm: AES256**
x-obs-server-side-encryption-customer-key-MD5	Indicates the MD5 value of the key for encrypting objects. This header is included in a response when SSE-C is used. Type: string Example: **x-obs-server-side-encryption-customer-key-MD5:4XvB3tbNTN+tIEVa0/fGaQ==**
x-obs-storage-class	This header is returned when the storage class of an object is not Standard. The value can be **WARM** or **COLD**. Type: string

Response Elements

This response contains elements of a copy result. **Table 5-62** describes the elements.

Table 5-62 Response elements

Element	Description
CopyObjectResult	Container for the copy result Type: XML
LastModified	Latest time when the object was modified Type: string
ETag	128-bit MD5 digest of the Base64 code of a new object. ETag is the unique identifier of the object content. It can be used to determine whether the object content is changed. For example, if the ETag value is **A** when an object is uploaded, but this value has changed to **B** when the object is downloaded, it indicates that the object content has been changed. Type: string

Error Responses

No special error responses are returned. For details about error responses, see **Table 6-2**.

Sample Request: Copying an Object

Copy the object **srcobject** in bucket **bucket** to the **destobject** object in bucket **examplebucket**.

```
PUT /destobject HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
Date: WED, 01 Jul 2015 04:19:21 GMT
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:2rZR+iaH8xUewvUKuicLhLHpNoU=
x-obs-copy-source: /bucket/srcobject
```

Sample Response: Copying an Object

```
HTTP/1.1 200 OK
Server: OBS
x-obs-request-id: 001B21A61C6C00000134031BE8005293
x-obs-id-2: MDAxQjIxQTYxQzZDMDAwMDAxMzQwMzFCRTgwMDUyOTNBQUFBQUFBQWJiYmJiYmJi
Date: WED, 01 Jul 2015 04:19:21 GMT
Content-Length: 249

<?xml version="1.0" encoding="utf-8"?>
<CopyObjectResult xmlns="http://obs.region.example.com/doc/2015-06-30/">
  <LastModified>2015-07-01T00:48:07.706Z</LastModified>
  <ETag>"507e3fff69b69bf57d303e807448560b"</ETag>
</CopyObjectResult>
```

Sample Request: Copying an Object Version

Copy a multi-version object and copy the object **srcobject** whose version number is **AAABQ4uBLdLc0vycq3gAAAAEVURTRkha** in bucket **bucket** to the **destobject** object in bucket **examplebucket**.

```
PUT /destobject HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
Date: WED, 01 Jul 2015 04:20:29 GMT
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:4BLYv+1UxfRSHBMvrhVLDszxvcY=
x-obs-copy-source: /bucket/srcobject?versionId=AAABQ4uBLdLc0vycq3gAAAAEVURTRkha
```

Sample Response: Copying an Object Version

```
HTTP/1.1 200 OK
Server: OBS
x-obs-request-id: DCD2FC9CAB78000001438B8A9C898B79
x-obs-id-2: DB/qBZmbN6AIoX9mrrSNYdLxwvbO0tLR/l6/XKTT4NmZspzharwp5Z74ybAYVOgr
Content-Type: application/xml
x-obs-version-id: AAABQ4uKnOrc0vycq3gAAAAFVURTRkha
x-obs-copy-source-version-id: AAABQ4uBLdLc0vycq3gAAAAEVURTRkha
Date: WED, 01 Jul 2015 04:20:29 GMT
Transfer-Encoding: chunked

<?xml version="1.0" encoding="utf-8"?>
<CopyObjectResult xmlns="http://obs.region.example.com/doc/2015-06-30/">
  <LastModified>2015-07-01T01:48:07.706Z</LastModified>
  <ETag>"507e3fff69b69bf57d303e807448560b"</ETag>
</CopyObjectResult>
```


5.4.4 Downloading an Object

Functions

This operation downloads an object from OBS. Before using this GET operation, check that you have the read permission for the target object. If the object owner has granted anonymous users the read permission for the object, anonymous users can access this object without using the authentication header field.

Server-Side Encryption

If the object uploaded to the server is encrypted on the server using the encryption key provided by the client, downloading the object requires including the encryption key in the message.

Versioning

By default, the GET operation returns the current version of an object. If the current version of the object is a delete marker, OBS returns a code meaning that the object does not exist. To obtain an object of a specified version, the **versionId** parameter can be used to specify the desired version.

Cold Objects

If the object you want to download is in the Cold storage class, ensure that this object has been restored before you download it. The response varies depending on the object's restore state. If an object has been restored, the **x-obs-restore** header (indicating the expiry date of the object) is returned when the object is successfully downloaded. If you send a request to download Cold objects that are not restored or are being restored, a **403 Forbidden** error will be returned.

Request Syntax

```
GET /ObjectName HTTP/1.1
Host: bucketname.obs.region.example.com
Date: date
Authorization: authorization
Range:bytes=byte_range
<Optional Additional Header>
```

NOTE

The field is optional. If it does not exist, you can obtain the whole content.

Request Parameters

In a **GET** request, you can override values for a set of message headers using the request parameters. Message headers that you can override are **Content-Type**, **Content-Language**, **Expires**, **Cache-Control**, **Content-Disposition**, and **Content-Encoding**. If the target object has multiple versions, use the **versionId** parameter to specify the version to be downloaded. For details, see **Table 5-63**.

NOTE

OBS does not process Accept-Encoding carried in a request or compress or decompress the uploaded data. The client determines whether to compress or decompress the data. Some HTTP clients may decompress data based on the Content-Encoding returned by the server. The client program needs to determine whether to decompress and how to decompress the data. To decompress the data, it can modify Content-Encoding (the object metadata stored in OBS) or rewrite Content-Encoding the object is downloaded. If an object download request specifies the rewrite header, the standard HTTP message header returned by OBS is subject to the rewrite content specified in the request.

Table 5-63 Request parameters

Parameter	Description	Mandatory
response-content-type	Rewrites the **Content-Type** header in the response. Type: string	No
response-content-language	Rewrites the **Content-Language** header in the response. Type: string	No
response-expires	Rewrites the **Expires** header in the response. Type: string	No
response-cache-control	Rewrites the **Cache-Control** header in the response. Type: string	No
response-content-disposition	Rewrites the **Content-Disposition** header in the response. Type: string Example: response-content-disposition=attachment; filename*=utf-8''name1 In this example, the downloaded object is renamed **name1**. If the new name contains full-width characters, it must be URL-encoded.	No
response-content-encoding	Rewrites the **Content-Encoding** header in the response. Type: string	No
versionId	Indicates the version ID of the object whose content is obtained. Type: string	No

Parameter	Description	Mandatory
attname	Rewrites the **Content-Disposition** header in the response. Type: string Example: attname=name1 Rename the downloaded object as **name1**.	No

Request Headers

This request uses common headers. In addition, you can add additional headers to this request. **Table 5-64** describes the additional headers.

Table 5-64 Request headers

Header	Description	Mandatory
Range	Obtains the object content within the scope defined by **Range**. If the parameter value is invalid, the entire object is obtained. **Range** value starts from 0, and the maximum value equals the object length minus 1. The start value of **Range** is mandatory. If only the start value is specified, the system obtains the object content from the start value to default maximum value. After the **Range** header field is carried, the value of ETag in the response message is the ETag of the object instead of the ETag of the object in the **Range** field. Type: string bytes=byte_range Example 1: **bytes=0-4** Example 2: **bytes=1024** Example 3: **bytes=10-20, 30-40** (multiple ranges)	No

Header	Description	Mandatory
If-Modified-Since	Returns the object only if it has been modified since the time specified by this header. Otherwise, **304 Not Modified** is returned. Type: HTTP time character string complying with the format specified at **http://www.ietf.org/rfc/rfc2616.txt**	No
If-Unmodified-Since	Returns the object only if it has not been modified since the time specified by this header. Otherwise, **412 Precondition Failed** is returned. Type: HTTP time character string complying with the format specified at **http://www.ietf.org/rfc/rfc2616.txt**	No
If-Match	Returns the object only if its ETag is the same as the one specified by this header. Otherwise, **412 Precondition Failed** is returned. Type: string ETag example: **0f64741bf7cb1089e988e4585d0d3434**	No
If-None-Match	Returns the object only if its ETag is different from the one specified by this header. Otherwise, **304 Not Modified** is returned. Type: string ETag example: **0f64741bf7cb1089e988e4585d0d3434**	No
x-obs-server-side-encryption-customer-algorithm	Indicates the encryption algorithm when SSE-C is used. Type: string Example: **x-obs-server-side-encryption-customer-algorithm:AES256** Constraint: This header must be used together with **x-obs-server-side-encryption-customer-key** and **x-obs-server-side-encryption-customer-key-MD5**.	No. This header is required when SSE-C is used.

Header	Description	Mandatory
x-obs-server-side-encryption-customer-key	Indicates the key for decrypting objects when SSE-C is used. Type: string Example: **x-obs-server-side-encryption-customer-key:K7QkYpBkM5+hca27fsNkUnNVaobncnLht/rCB2o/9Cw=** Constraint: This header is a Base64-encoded 256-bit key and must be used together with **x-obs-server-side-encryption-customer-algorithm** and **x-obs-server-side-encryption-customer-key-MD5**.	No. This header is required when SSE-C is used.
x-obs-server-side-encryption-customer-key-MD5	Indicates the MD5 value of the encryption key when SSE-C is used. The MD5 value is used to check whether any error occurs during the transmission of the key. Type: string Example: **x-obs-server-side-encryption-customer-key-MD5:4XvB3tbNTN+tIEVa0/fGaQ==** Constraint: This header is a Base64-encoded 128-bit MD5 value and must be used together with **x-obs-server-side-encryption-customer-algorithm** and **x-obs-server-side-encryption-customer-key**.	No. This header is required when SSE-C is used.

Request Elements

This request involves no elements.

Response Syntax

```
HTTP/1.1 status_code
Content-Type: type
Date: date
Content-Length: length
Etag: etag
Last-Modified: time

<Object Content>
```

Response Headers

The response to the request uses common headers. For details, see **Table 3-19**.

In addition to the common response headers, the headers listed in **Table 5-65** may be used.

Table 5-65 Additional response headers

Header	Description
x-obs-expiration	When an object has its lifecycle rule, the object expiration time is subject to its lifecycle rule. This header field is use **expiry-date** to describe the object expiration date. If the lifecycle rule is configured only for the entire bucket not individual objects, the object expiration time is subject to the bucket lifecycle rule. This header field uses the **expiry-date** and **rule-id** to describe the detailed expiration information of objects. If no lifecycle rule is configured, this header field is not contained in the response. Type: string
x-obs-website-redirect-location	Indicates the redirected-to location. If the bucket is configured with website information, this parameter can be set for the object metadata so that the website endpoint will evaluate the request for the object as a 301 redirect to another object in the same bucket or an external URL. Type: string
x-obs-delete-marker	Indicates whether an object is a delete marker. If the object is not marked as deleted, the response does not contain this header. Type: boolean Value options: **true**, **false** The default value is **false**.
x-obs-version-id	Object version ID. If the object has no version number specified, the response does not contain this header. Valid value: string Default value: none
x-obs-server-side-encryption	This header is included in a response if SSE-KMS is used. Type: string Example: **x-obs-server-side-encryption:kms**

Header	Description
x-obs-server-side-encryption-kms-key-id	Indicates the master key ID. This header is included in a response when SSE-KMS is used. Type: string Format: *regionID*:*domainID*:**key/***key_id* *regionID* indicates the ID of the region where the key belongs. *domainID* indicates the ID of the tenant where the key belongs. *key_id* indicates the key ID used in this encryption. Example: **x-obs-server-side-encryption-kms-key-id:*region*:domainiddomainiddomainid-doma0001:key/4f1cd4de-ab64-4807-920a-47fc42e7f0d0**
x-obs-server-side-encryption-customer-algorithm	Indicates a decryption algorithm. This header is included in a response if SSE-C is used. Type: string Example: **x-obs-server-side-encryption-customer-algorithm:AES256**
x-obs-server-side-encryption-customer-key-MD5	Indicates the MD5 value of a key used to decrypt objects. This header is included in a response if SSE-C is used. Type: string Example: **x-obs-server-side-encryption-customer-key-MD5:4XvB3tbNTN+tIEVa0/fGaQ==**
x-obs-object-type	If the object is not a normal one, this header field is returned. The value can be **Appendable**. Type: string
x-obs-next-append-position	This header field is returned when the object is an appendable object. Type: integer

Response Elements

This response contains no elements.

Error Responses

No special error responses are returned. For details about error responses, see **Table 6-2**.

Sample Request: Downloading an Object

```
GET /object01 HTTP/1.1
User-Agent: curl/7.29.0
```



```
Host: examplebucket.obs.region.example.com
Accept: */*
Date: WED, 01 Jul 2015 04:24:33 GMT
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:NxtSMS0jaVxlLnxlO9awaMTn47s=
```

Sample Response: Downloading an Object

```
HTTP/1.1 200 OK
Server: OBS
x-obs-request-id: 8DF400000163D3F2A89604C49ABEE55E
Accept-Ranges: bytes
ETag: "3b46eaf02d3b6b1206078bb86a7b7013"
Last-Modified: WED, 01 Jul 2015 01:20:29 GMT
Content-Type: binary/octet-stream
x-obs-id-2: 32AAAQAAEAABAAAQAAEAABAAAQAAEAABCSQwxJ2I1VvxD/Xgwuw2G2RQax30gdXU
Date: WED, 01 Jul 2015 04:24:33 GMT
Content-Length: 4572

[4572 Bytes object content]
```

Sample Request: Downloading a Specified Range of an Object

Download the specified range of an object (download a range of an object).

```
GET /object01 HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
Date: Mon, 14 Sep 2020 09:59:04 GMT
Range:bytes=20-30
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:mNPLWQMDWg30PTkAWiqJaLl3ALg=
```

Download the specified range of an object (download multiple ranges of an object).

```
GET /object01 HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
Date: Mon, 14 Sep 2020 10:02:43 GMT
Range:bytes=20-30,40-50
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:ZwM7Vk2d7sD9o8zRsRKehgKQDkk=
```

Sample Response: Downloading a Specified Range of an Object

Download the specified range of an object (download a range of an object).

```
HTTP/1.1 206 Partial Content
Server: OBS
x-obs-request-id: 000001748C0DBC35802E360C9E869F31
Accept-Ranges: bytes
ETag: "2200446c2082f27ed2a569601ca4e360"
Last-Modified: Mon, 14 Sep 2020 01:16:20 GMT
Content-Range: bytes 20-30/4583
Content-Type: binary/octet-stream
x-obs-id-2: 32AAAQAAEAABAAAQAAEAABAAAQAAEAABCSn2JHu4okx9NBRNZAvBGawa3lt3g31g
Date: Mon, 14 Sep 2020 09:59:04 GMT
Content-Length: 11

[ 11 Bytes object content]
```

Download the specified range of an object (download multiple ranges of an object).

```
HTTP/1.1 206 Partial Content
Server: OBS
```



```
x-obs-request-id: 8DF400000163D3F2A89604C49ABEE55E
Accept-Ranges: bytes
ETag: "2200446c2082f27ed2a569601ca4e360"
Last-Modified: Mon, 14 Sep 2020 01:16:20 GMT
Content-Type: multipart/byteranges;boundary=35bcf444-e65f-4c76-9430-7e4a68dd3d26
x-obs-id-2: 32AAAQAAEAABAAAQAAEAABAAAQAAEAABCSIBWFOVW8eeWujkqSnoIANC2mNR1cdF
Date: Mon, 14 Sep 2020 10:02:43 GMT
Content-Length: 288

--35bcf444-e65f-4c76-9430-7e4a68dd3d26
Content-type: binary/octet-stream
Content-range: bytes 20-30/4583
[ 11 Bytes object content]
--35bcf444-e65f-4c76-9430-7e4a68dd3d26
Content-type: binary/octet-stream
Content-range: bytes 40-50/4583
[ 11 Bytes object content]
--35bcf444-e65f-4c76-9430-7e4a68dd3d26
```

Sample Request: Checking the ETag Value of an Object

Download an object if its ETag value is matched.

```
GET /object01 HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
Date: WED, 01 Jul 2015 04:24:33 GMT
If-Match: 682e760adb130c60c120da3e333a8b09
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:NxtSMS0jaVxlLnxlO9awaMTn47s=
```

Sample Response: Checking the ETag Value of an Object (ETag Mismatch)

If the object's ETag value is not **682e760adb130c60c120da3e333a8b09**, the system displays a download failure message.

```
HTTP/1.1 412 Precondition Failed
Server: OBS
x-obs-request-id: 8DF400000163D3F2A89604C49ABEE55E
Content-Type: application/xml
x-obs-id-2: 32AAAQAAEAABAAAQAAEAABAAAQAAEAABCSQwxJ2I1VvxD/Xgwuw2G2RQax30gdXU
Date: WED, 01 Jul 2015 04:20:51 GMT

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Error>
  <Code>PreconditionFailed</Code>
  <Message>At least one of the pre-conditions you specified did not hold</Message>
  <RequestId>8DF400000163D3F2A89604C49ABEE55E</RequestId>
  <HostId>ha0ZGaSKVm+uLOrCXXtx4Qn1aLzvoeblctVXRAqA7pty10mzUUW/yOzFue04lBqu</HostId>
  <Condition>If-Match</Condition>
</Error>
```

Sample Response: Checking the ETag Value of an Object (ETag Matched)

If the object's ETag value is **682e760adb130c60c120da3e333a8b09**, the download is successful.

```
HTTP/1.1 200 OK
Server: OBS
x-obs-request-id: 5DEB00000164A21E1FC826C58F6BA001
Accept-Ranges: bytes
ETag: "682e760adb130c60c120da3e333a8b09"
Last-Modified: Mon, 16 Jul 2015 08:03:34 GMT
Content-Type: application/octet-stream
x-obs-id-2: 32AAAQAAEAABAAAQAAEAABAAAQAAEAABCSbkdml1sLSvKnoHaRcOwRl+6+ustDwk
Date: Mon, 16 Jul 2015 08:04:00 GMT
```



```
Content-Length: 8

[ 8 Bytes object content]
```

Sample Request: Downloading an Object Using a Signed URL

```
GET /object02?
AccessKeyId=H4IPJX0TQTHTHEBQQCEC&Expires=1532688887&Signature=EQmDuOhaLUrzrzRNZxwS72CXeXM%3D HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
Date: Fri, 27 Jul 2018 10:52:31 GMT
```

Sample Response: Downloading an Object Using a Signed URL

```
HTTP/1.1 200 OK
Server: OBS
x-obs-request-id: 804F00000164DB5E5B7FB908D3BA8E00
ETag: "682e760adb130c60c120da3e333a8b09"
Last-Modified: Mon, 16 Jul 2015 08:03:34 GMT
Content-Type: application/octet-stream
x-obs-id-2: 32AAAUJAIAABAAAQAAEAABAAAQAAEAABCTlpxILjhVK/heKOWIP8Wn2IWmQoerfw
Date: Fri, 27 Jul 2018 10:52:31 GMT
Content-Length: 8

[ 8 Bytes object content]
```

Sample Request: Downloading an Object and Renaming It (with response-content-disposition Used)

Use the response-content-disposition parameter to download and rename an object.

```
GET /object01?response-content-disposition=attachment; filename*=utf-8''name1 HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
Date: WED, 01 Jul 2015 04:24:33 GMT
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:NxtSMS0jaVxlLnxlO9awaMTn47s=
```

Sample Response: Downloading an Object and Renaming It (with response-content-disposition Used)

```
HTTP/1.1 200 OK
Server: OBS
x-obs-request-id: 804F00000164DB5E5B7FB908D3BA8E00
ETag: "682e760adb130c60c120da3e333a8b09"
Last-Modified: Mon, 16 Jul 2015 08:03:34 GMT
Content-Type: application/octet-stream
x-obs-id-2: 32AAAUJAIAABAAAQAAEAABAAAQAAEAABCTlpxILjhVK/heKOWIP8Wn2IWmQoerfw
Date: Fri, 27 Jul 2018 10:52:31 GMT
Content-Length: 8
Content-Disposition: attachment; filename*=utf-8''name1

[ 8 Bytes object content]
```

Sample Request: Downloading an Object and Renaming It (with attname Used)

Use the attname parameter to download and rename an object.

```
GET /object01?attname=name1 HTTP/1.1
User-Agent: curl/7.29.0
```



```
Host: examplebucket.obs.region.example.com
Accept: */*
Date: WED, 01 Jul 2015 04:24:33 GMT
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:NxtSMS0jaVxlLnxlO9awaMTn47s=
```

Sample Response: Downloading an Object and Renaming It (with attname Used)

```
HTTP/1.1 200 OK
Server: OBS
x-obs-request-id: 804F00000164DB5E5B7FB908D3BA8E00
ETag: "682e760adb130c60c120da3e333a8b09"
Last-Modified: Mon, 16 Jul 2015 08:03:34 GMT
Content-Type: application/octet-stream
x-obs-id-2: 32AAAUJAIAABAAAQAAEAABAAAQAAEAABCTlpxILjhVK/heKOWIP8Wn2IWmQoerfw
Date: Fri, 27 Jul 2018 10:52:31 GMT
Content-Length: 8
Content-Disposition: attachment; filename*=utf-8''name1

[ 8 Bytes object content]
```

5.4.5 Querying Object Metadata

Functions

Users with the read permission on objects can perform the HeadObject operation to obtain metadata of objects. The object metadata is included in the response.

This operation supports server-side encryption.

Versioning

By default, this operation returns the latest metadata of an object. If the object has a delete marker, status code 404 is returned. To obtain the object metadata of a specified version, the **versionId** parameter can be used to specify the desired version.

Request Syntax

```
HEAD /ObjectName HTTP/1.1
Host: bucketname.obs.region.example.com
Date: date
Authorization: authorization
```

Request Parameters

Table 5-66 describes the request parameters.

Table 5-66 Request parameters

Parameter	Description	Mandatory
versionId	Object version ID Type: string	No

Request Headers

This request uses common headers. For details, see **Table 3-3**.

In addition, the request can use additional headers, as shown in **Table 5-67**.

Table 5-67 Request headers

Header	Description	Mandatory
Origin	Origin of the cross-domain request specified by the pre-request. Generally, it is a domain name. Type: string	No
Access-Control-Request-Headers	Indicates the HTTP headers of a request. The request can use multiple HTTP headers. Type: string	No
x-obs-server-side-encryption-customer-algorithm	Indicates the decryption algorithm when SSE-C is used. Type: string Example: **x-obs-server-side-encryption-customer-algorithm:AES256** Constraint: This header must be used together with **x-obs-server-side-encryption-customer-key** and **x-obs-server-side-encryption-customer-key-MD5**.	No. This header is required when SSE-C is used.
x-obs-server-side-encryption-customer-key	Indicates the decryption key when SSE-C is used. Type: string Example: **x-obs-server-side-encryption-customer-key:K7QkYpBkM5+hca27fsNkUnNVaobncnLht/rCB2o/9Cw=** Constraint: This header is a Base64-encoded 256-bit key and must be used together with **x-obs-server-side-encryption-customer-algorithm** and **x-obs-server-side-encryption-customer-key-MD5**.	No. This header is required when SSE-C is used.

Header	Description	Mandatory
x-obs-server-side-encryption-customer-key-MD5	Indicates the MD5 value of the decryption key when SSE-C is used. The MD5 value is used to check whether any error occurs during the transmission of the key. Type: string Example: **x-obs-server-side-encryption-customer-key-MD5:4XvB3tbNTN+tIEVa0/fGaQ==** Constraint: This header is a Base64-encoded 128-bit MD5 value and must be used together with **x-obs-server-side-encryption-customer-algorithm** and **x-obs-server-side-encryption-customer-key**.	No. This header is required when SSE-C is used.

Request Elements

This request involves no elements.

Response Syntax

```
HTTP/1.1 status_code
Content-Type: type
Date: date
Content-Length: length
Etag: etag
Last-Modified: time
```

Response Headers

The response to the request uses common headers. For details, see **Table 3-19**.

In addition to the common response headers, the headers listed in **Table 5-68** may be used.

Table 5-68 Additional response headers

Header	Description
x-obs-expiration	When an object has its lifecycle rule, the object expiration time is subject to its lifecycle rule. This header field is use **expiry-date** to describe the object expiration date. If the lifecycle rule is configured only for the entire bucket not individual objects, the object expiration time is subject to the bucket lifecycle rule. This header field uses the **expiry-date** and **rule-id** to describe the detailed expiration information of objects. If no lifecycle rule is configured, this header field is not contained in the response. Type: string

Header	Description
x-obs-website-redirect-location	Indicates the redirected-to location. If the bucket is configured with website information, this parameter can be set for the object metadata so that the website endpoint will evaluate the request for the object as a 301 redirect to another object in the same bucket or an external URL. Type: string
x-obs-version-id	Object version ID. If the object has no version number specified, the response does not contain this header. Type: string Default value: none
Access-Control-Allow-Origin	Indicates that the origin is included in the response if the origin in the request meets the CORS configuration requirements when CORS is configured for buckets. Type: string
Access-Control-Allow-Headers	Indicates that the headers are included in the response if headers in the request meet the CORS configuration requirements when CORS is configured for buckets. Type: string
Access-Control-Max-Age	Value of **MaxAgeSeconds** in the CORS configuration of the server when CORS is configured for buckets. Type: integer
Access-Control-Allow-Methods	Indicates that methods in the rule are included in the response if Access-Control-Request-Method in the request meets the CORS configuration requirements when CORS is configured for buckets. Type: string Value options: **GET**, **PUT**, **HEAD**, **POST**, **DELETE**
Access-Control-Expose-Headers	Value of **ExposeHeader** in the CORS configuration of a server when CORS is configured for buckets. Type: string

Header	Description
x-obs-server-side-encryption	This header is included in a response if SSE-KMS is used. Type: string Example: **x-obs-server-side-encryption:kms**
x-obs-server-side-encryption-kms-key-id	Indicates the master key ID. This header is included in a response when SSE-KMS is used. Type: string Format: *regionID*:*domainID*:**key/***key_id* *regionID* indicates the ID of the region where the key belongs. *domainID* indicates the ID of the tenant where the key belongs. *key_id* indicates the key ID used in this encryption. Example: **x-obs-server-side-encryption-kms-key-id:*region*:domainiddomainiddomainid-doma0001:key/4f1cd4de-ab64-4807-920a-47fc42e7f0d0**
x-obs-server-side-encryption-customer-algorithm	Indicates a decryption algorithm. This header is included in a response if SSE-C is used. Type: string Example: **x-obs-server-side-encryption-customer-algorithm:AES256**
x-obs-server-side-encryption-customer-key-MD5	Indicates the MD5 value of a key used to decrypt objects. This header is included in a response if SSE-C is used. Type: string Example: **x-obs-server-side-encryption-customer-key-MD5:4XvB3tbNTN+tIEVa0/fGaQ==**
x-obs-storage-class	This header is returned when the storage class of an object is not Standard. The value can be **WARM** or **COLD**. Type: string
x-obs-restore	This header is returned when a Cold object is being restored or has been restored. It represents the object's restore status, which can be **ongoing-request="true"** (the object is being restored) or **ongoing-request="false", expiry-date="Wed, 7 Nov 2012 00:00:00 GMT"** (the object has been restored). In these statuses, **expiry-date** indicates when the restored object will expire. Type: string

Header	Description
x-obs-object-type	If the object is not a normal one, this header field is returned. The value can be **Appendable** Type: string
x-obs-next-append-position	This header field is returned when the object is an appendable object. Type: integer
x-obs-uploadId	This header is returned if the object is a combination of multiple parts. The header value indicates the ID of the corresponding multipart upload task. Type: string

Response Elements

This response contains no elements.

Error Responses

No special error responses are returned. For details about error responses, see **Table 6-2**.

Sample Request

```
HEAD /object1 HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
Date: WED, 01 Jul 2015 04:19:25 GMT
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:/cARjk81l2iExMfQqn6iT3qEZ74=
```

Sample Response

```
HTTP/1.1 200 OK
Server: OBS
x-obs-request-id: 8DF400000163D3E4BB5905C41B6E65B6
Accept-Ranges: bytes
ETag: "3b46eaf02d3b6b1206078bb86a7b7013"
Last-Modified: WED, 01 Jul 2015 01:19:21 GMT
Content-Type: binary/octet-stream
x-obs-id-2: 32AAAQAAEAABAAAQAAEAABAAAQAAEAABCSD3nAiTaBoeyt9oHp9vTYtXnLDmwV6D
Date: WED, 01 Jul 2015 04:19:21 GMT
Content-Length: 4572
```

5.4.6 Deleting an Object

Functions

You can perform this operation to delete an object. If you try to delete an object that does not exist, OBS will return a success message.

Versioning

When versioning is enabled for a bucket, a delete request that does not specify a version ID cannot permanently delete the object. Instead, OBS creates a delete marker with a unique version ID. When versioning is suspended for a bucket, a delete request that does not specify a version ID deletes the object whose version ID is **null** and creates a delete marker with a version ID of **null**.

To delete an object of a specified version, the **versionId** parameter can be used to specify the desired version.

Request Syntax

```
DELETE /ObjectName HTTP/1.1
Host: bucketname.obs.region.example.com
Date: date
Authorization: authorization
```

Request Parameters

Table 5-69 describes the request parameters.

NOTICE

For deleting an object, only parameters listed in **Table 5-69** are supported. If the request contains parameters that cannot be identified by OBS, the server returns the 400 error code.

Table 5-69 Request parameters

Parameter	Description	Mandatory
versionId	Object version ID Type: string	No

Request Headers

This request uses common headers. For details, see **Table 3-3**.

Request Elements

This request involves no elements.

Response Syntax

```
HTTP/1.1 status_code
Date: date
```

Response Headers

The response to the request uses common headers. For details, see **Table 3-19**.

If versioning is enabled for the bucket, the headers listed in **Table 5-70** may also be used.

Table 5-70 Additional response headers

Header	Description
x-obs-delete-marker	Indicates whether an object is deleted. If the object is not marked as deleted, the response does not contain this header. Type: boolean Value options: **true**, **false** The default value is **false**.
x-obs-version-id	Object version ID. If the object has no version number specified, the response does not contain this header. Valid value: string Default value: none

Response Elements

This response contains no elements.

Error Responses

No special error responses are returned. For details about error responses, see **Table 6-2**.

Sample Request

```
DELETE /object2 HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
Date: WED, 01 Jul 2015 04:19:21 GMT
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:MfK9JCnSFHCrJmjv7iRkRrrce2s=
```

Sample Response

```
HTTP/1.1 204 No Content
Server: OBS
x-obs-request-id: 8DF400000163D3F51DEA05AC9CA066F1
x-obs-id-2: 32AAAUgAIAABAAAQAAEAABAAAQAAEAABCSgkM4Dij80gAeFY8pAZIwx72QhDeBZ5
Date: WED, 01 Jul 2015 04:19:21 GMT
```

5.4.7 Deleting Objects

Functions

This operation can be used to batch delete some objects in a bucket. The deletion cannot be undone. After the operation is implemented, the returned information contains the implementation result of each object in the specified bucket. OBS

deletes the objects synchronously. The deletion result of each object is returned to the request user.

Objects in batches can be deleted in **verbose** or **quiet** mode. With **verbose** mode, OBS returns results of successful and failed deletion in an XML response; with **quiet** mode, OBS only returns results of failed deletion in an XML response. OBS uses the **verbose** mode by default and you can specify the **quiet** mode in the request body.

For batch deletion, the request header must contain **Content-MD5** and **Content-Length**, so that the message body can be identified if network transmission error is detected at the server side.

Request Syntax

```
POST /?delete HTTP/1.1
Host: bucketname.obs.region.example.com
Date: date
Authorization: authorization
Content-MD5: MD5
Content-Length: length

<?xml version="1.0" encoding="UTF-8"?>
<Delete>
   <Quiet>true</Quiet>
   <Object>
      <Key>Key</Key>
      <VersionId>VersionId</VersionId>
   </Object>
   <Object>
      <Key>Key</Key>
   </Object>
</Delete>
```

Request Parameters

This request involves no parameters.

Request Headers

This request uses common headers. For details, see **Table 3-3**.

Request Elements

This request uses elements to specify the list of objects to be deleted in a batch. **Table 5-71** describes the elements.

Table 5-71 Request elements

Element	Description	Mandatory
Quiet	Specifies the **quiet** mode. With the **quiet** mode, OBS only returns the list of objects that failed to be deleted. This element is valid when set to **true**. Otherwise, OBS ignores it. Type: boolean	No

Element	Description	Mandatory
Delete	List of objects to be deleted Type: XML	Yes
Object	Names of objects to be deleted Type: XML	Yes
Key	Key of the object to be deleted. Type: string	Yes
VersionId	Version ID of the object to be deleted Type: string	No

A maximum of 1,000 objects can be deleted at a time. If you send a request for deleting more than 1,000 objects, OBS returns an error message.

After concurrent tasks are assigned, OBS may encounter an internal error during cyclic deletion of multiple objects. In that case, the metadata still exists when the object index data is deleted, which means data inconsistency.

Response Syntax

```
HTTP/1.1 status_code
Date: date
Content-Type: application/xml
Content-Length: length

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<DeleteResult xmlns="http://obs.region.example.com/doc/2015-06-30/">
<Deleted>
   <Key>Key</Key>
</Deleted>
<Error>
   <Key>Key</Key>
   <Code>ErrorCode</Code>
   <Message>Message</Message>
</Error>
</DeleteResult>
```

Response Headers

The response to the request uses common headers. For details, see **Table 3-19**.

Response Elements

This response uses elements to return results of deleted objects in a batch. **Table 5-72** describes the elements.

Table 5-72 Response elements

Element	Description
DeleteResult	Root node of batch deletion responses Type: container
Deleted	Container for results of successful deletion Type: container
Error	Container for results of failed deletion Type: container
Key	Object names in a deletion result Type: string
Code	Error code of a deletion failure Type: string
Message	Error message of a deletion failure Type: string
VersionId	Version IDs of objects to be deleted Type: string
DeleteMarker	If this element is specified, **true** will be returned when you create or delete a delete marker in a bucket with versioning enabled. Type: boolean
DeleteMarkerVersionId	Indicates the version ID of the delete marker deleted or created by the request. If you create or delete a delete marker in a bucket with versioning enabled, OBS returns this element in the response. This element will be returned in either of the following cases: • You send a request that has only the object name but not the version ID specified. In this case, OBS creates a delete marker and returns its version ID in the response. • You send a request that has both the object key and version ID (that identifies a delete marker) specified. In this case, OBS deletes the delete marker and returns its version ID in the response. Type: boolean

Error Responses

1. If the resolution result of an XML request contains more than 1000 objects, OBS returns **400 Bad Request**.

2. If the object key in an XML request is invalid (for example, containing more than 1024 characters), OBS returns **400 Bad Request**.

3. If the request header does not contain Content-MD5, OBS returns **400 Bad Request**.

Other errors are included in **Table 6-2**.

Sample Request

```
POST /test333?delete HTTP/1.1
User-Agent: curl/7.29.0
Host: 127.0.0.1
Accept: */*
Date: WED, 01 Jul 2015 04:34:21 GMT
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:8sjZWJlWmYmYnK5JqXaFFQ+vHEg=
Content-MD5: ZPzz8L+hdRJ6qCqYbU/pCw==
Content-Length: 188

<?xml version="1.0" encoding="utf-8"?>
<Delete>
  <Quiet>true</Quiet>
  <Object>
    <Key>obja02</Key>
  </Object>
  <Object>
    <Key>obja02</Key>
  </Object>
</Delete>
```

Sample Response

```
HTTP/1.1 200 OK
Server: OBS
x-obs-request-id: 8DF400000163D3FE4CE80340D30B0542
x-obs-id-2: 32AAAQAAEAABAAAQAAEAABAAAQAAEAABCRhY0FBWRm6qjOE1ACBZwS+0KYlPBq0f
Content-Type: application/xml
Date: WED, 01 Jul 2015 04:34:21 GMT
Content-Length: 120

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<DeleteResult xmlns="http://obs.example.com/doc/2015-06-30/"/>
```

5.4.8 Restoring Cold Objects

Functions

To obtain the content of an object in the Cold storage class, you need to restore the object first and then you can download it. After an object is restored, a copy of the object is saved in the Standard storage class. By doing so, the object in the Cold storage class and its copy in the Standard storage class co-exist in the bucket. The copy will be automatically deleted once its retention period expires.

Versioning

By default, this operation returns the latest version of an object. If the object has a delete marker, status code 404 is returned. To restore an object of a specified version, the **versionId** parameter can be used to specify the desired version.

Request Syntax

```
POST /ObjectName?restore&versionId=VersionID HTTP/1.1
Host: bucketname.obs.region.example.com
```



```
Date: date
Authorization: authorization string
Content-MD5: MD5

<RestoreRequest>
  <Days>NumberOfDays</Days>
  <RestoreJob>
    <Tier>RetrievalOption</Tier>
  </RestoreJob>
</RestoreRequest>
```

Request Parameters

Parameter	Description	Mandatory
versionId	Version ID of the Cold object to be restored Type: string	No

Request Headers

This request uses common headers. For details, see **Table 3-3**.

Request Elements

Table 5-73 Request elements

Element	Description	Mandatory
RestoreRequest	Container for the restore information Type: container	Yes
Days	Indicates the storage duration of the restored object. The minimum value is 1 and the maximum value is 30. Type: integer	Yes
RestoreJob	Container for the restore options Type: container	No

Element	Description	Mandatory
Tier	Restore options: **Expedited** | **Standard** **Expedited** indicates that objects can be quickly restored from Archive storage within 1 to 5 minutes. **Standard** indicates that objects can be restored from Archive storage within 3 to 5 hours. The default value is **Standard**. Type: string	No

Response Syntax

```
HTTP/1.1 status_code
Date: date
```

Response Headers

The response to the request uses common headers. For details, see **Table 3-19**.

Response Elements

This response contains no elements.

Error Responses

Table 5-74 List of OBS access error codes

Error Code	Description	HTTP Status Code
RestoreAlreadyIn-Progress	The object is being restored. The request conflicts with another. ErrorMessage: Object restore is already in progress	409 Conflict
ObjectHasAlready Restored	The objects have been restored and the retention period of the objects cannot be shortened. ErrorMessage: After restoring an archived object, you cannot shorten the restoration period of the archived object	409 Conflict

Error Code	Description	HTTP Status Code
MalformedXML	Invalid value for the **Days** field (not an integer) ErrorMessage: The XML you provided was not well-formed or did not validate against our published schema	400 Bad Request
InvalidArgument	The value of the **Days** field is not within the range of 1 to 30. ErrorMessage: restoration days should be at least 1 and at most 30	400 Bad Request
MalformedXML	Invalid value for the **Tier** field. ErrorMessage: The XML you provided was not well-formed or did not validate against our published schema	400 Bad Request
InvalidObjectState	The restored object is not in the Cold storage. ErrorMessage: Restore is not allowed, as object's storage class is not COLD	403 Forbidden

Sample Request

```
POST /object?restore HTTP/1.1
Host: examplebucket.obs.region.example.com
Accept: */*
Date: WED, 01 Jul 2015 04:39:46 GMT
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:kaEwOixnSVuS6If3Q0Lnd6kxm5A=
Content-Length: 183

<RestoreRequest>
  <Days>2</Days>
  <RestoreJob>
    <Tier>Expedited</Tier>
  </RestoreJob>
</RestoreRequest>
```

Sample Response

```
HTTP/1.1 202 Accepted
Server: OBS
x-obs-request-id: A2F500000163F374CCBB2063F834C6C4
x-obs-id-2: 32AAAUgAIAABAAAQAAEAABAAAQAAEAABCSLbWIs23RR95NVpkbWlJdlm8Dq+wQBw
Date: WED, 01 Jul 2015 04:39:46 GMT
Content-Length: 0
```

5.4.9 Appending an Object

Functions

The AppendObject operation adds data to the end of an object in a specified bucket. If there is no namesake object in the bucket, a new object is created.

The object created using the **AppendObject** operation is an appendable object, and the object uploaded using the **PUT** operation is a normal object.

NOTE

Uploaded objects must be stored in buckets. Only the users who have the write permission to a bucket can upload objects to the bucket. The name of each object in the same bucket must be unique.

To ensure that data is not damaged during transmission, you can add the **Content-MD5** parameter to the request header. After receiving the data, OBS performs MD5 verification for the data. If the data is inconsistent, OBS returns an error message.

This operation allows you to specify the **x-obs-acl** parameter when creating an appendable object and set the permission control policy for the object.

This operation supports server-side encryption.

Relationship with Other Operations

1. If you perform the PUT operation on an existing appendable object, the appendable object is overwritten by the newly uploaded object and the object type changes to normal. If you perform the other way around, an error occurs.
2. An appendable object will be changed to a normal object after being copied. An appendable object cannot be copied and saved as an appendable object.

Constraints

1. The last modification time of the object is updated each time an appending upload is performed.
2. If the SSE-C encryption mode is used on the server side, the appending upload is the same as the initialization segment. In this case, the request headers such as **x-obs-server-side-encryption** must be carried.
3. For the server-side encryption (SSE-KMS), the request header such as **x-obs-server-side-encryption** is specified only when the file is uploaded for the first time and no object with the same name exists in the bucket.
4. The length of each appended upload cannot exceed the upper limit (5 GB) of the object length.
5. The maximum number of append-only writes for each appendable object is 10,000.
6. If the object storage class is **COLD** (Cold), this API cannot be called.
7. Object appending is not available for parallel file systems.

Request Syntax

```
POST /ObjectName?append&position=Position HTTP/1.1
Host: bucketname.obs.region.example.com
Content-Type: application/xml
Content-Length: length
Authorization: authorization
Date: date
<Optional Additional Header>
<object Content>
```


Request Parameters

The request needs to specify parameters in the message, indicating that the request is for appending upload and the upload location must be specified. For details about the parameters, see **Table 5-75**.

Table 5-75 Request parameters

Parameter	Description	Mandatory
append	Indicates that the file is uploaded in appending mode. Type: string	Yes
position	Location for the appending upload For an object to be appended, the value of **position** must be set to **0** when the object is uploaded for the first time. The value of **position** will be carried in the **x-obs-next-append-position** header of the response returned by the server when the object is successfully uploaded next time. Type: integer	Yes

Request Headers

This request uses common headers. For details, see **Table 3-3**.

Table 5-76 describes the additional message headers that a request can use when the **position=0** parameter is requested.

This request can use the server-side encryption request header. For details, see **Table 5-77**.

Table 5-76 Request headers

Header	Description	Mandatory
x-obs-acl	For the first appending, the message header can be added to set the permission control policy of the object. The predefined common policies are used, including: **private**, **public-read**, **public-read-write**. Type: string Note: This header is a predefined policy expressed in a character string.	No

Header	Description	Mandatory
x-obs-grant-read	For the first write, you can use this header to grant all users in an account the permissions to read the object and obtain the object metadata. Type: string	No
x-obs-grant-read-acp	For the first write, you can use this header to grant all users in an account the permission to obtain object ACL information. Type: string	No
x-obs-grant-write-acp	For the first write, you can use this header to grant all users in an account the permission to write the object ACL. Type: string	No
x-obs-grant-full-control	For the first write, you can use this header to grant all users in an account the permissions to read the object, obtain the object metadata, obtain the object ACL information, and write the object ACL. Type: string	No
x-obs-storage-class	For the first write, you can use this header field to configure the object storage class. If you do not use this header, the object storage class is the default storage class of the bucket. Type: string Because Cold (**COLD**) objects do not support append upload, the configurable values are as follows: **STANDARD** (Standard), **WARM** (Warm), which are case sensitive. Example: **x-obs-storage-class:STANDARD**	No
x-obs-meta-*	For the first write, you can use a header starting with **x-obs-meta-** to define object metadata in an HTTP request. Custom metadata will be returned in the response header when you retrieve or query the metadata of the object. The size of the HTTP request excluding the request body must be equal to or smaller than 8 KB. Type: string Example: **x-obs-meta-test:test metadata**	No

Header	Description	Mandatory
x-obs-website-redirect-location	If a bucket is configured with the static website hosting function, it will redirect requests for this object to another object in the same bucket or to an external URL. OBS stores the value of this header in the object metadata. Type: string Default value: none Constraint: The value must be prefixed by a slash (/), **http://**, or **https://**. The length of the value cannot exceed 2 KB.	No
x-obs-expires	Specifies when an object expires. It is measured in days. Once the object expires, it is automatically deleted. (The calculation starts from when the object was last modified). Type: integer Example: **x-obs-expires:3**	No

Table 5-77 Server encryption request headers

Header	Description	Mandatory
x-obs-server-side-encryption	Indicates that SSE-KMS is used. Type: string Example: **x-obs-server-side-encryption:kms**	No. This header is required when SSE-KMS is used.

Header	Description	Mandatory
x-obs-server-side-encryption-kms-key-id	Indicates the master key when SSE-KMS is used. If this header is not provided, the default master key will be used. If there is no such a default master key, OBS will create one and use it by default. Type: string The following two formats are supported: - *regionID*:*domainID*:**key/***key_id* - *key_id* *regionID* indicates the ID of the region where the key belongs. *domainID* indicates the ID of the tenant where the key belongs. *key_id* indicates the ID of the key created in KMS. Examples: - **x-obs-server-side-encryption-kms-key-id:***region*:**domainiddomainiddomainiddo-ma0001:key/4f1cd4de-ab64-4807-920a-47fc42e7f0d0** - **x-obs-server-side-encryption-kms-key-id:4f1cd4de-ab64-4807-920a-47fc42e7f0d0**	No
x-obs-server-side-encryption-customer-algorithm	Indicates the encryption algorithm when SSE-C is used. Type: string Example: **x-obs-server-side-encryption-customer-algorithm:AES256** Constraint: This header must be used together with **x-obs-server-side-encryption-customer-key** and **x-obs-server-side-encryption-customer-key-MD5**.	No. This header is required when SSE-C is used.
x-obs-server-side-encryption-customer-key	Indicates the key for encrypting objects when SSE-C is used. Type: string Example: **x-obs-server-side-encryption-customer-key:K7QkYpBkM5+hca27fsNkUnNVaobncnLht/rCB2o/9Cw=** Constraint: This header is a Base64-encoded 256-bit key and must be used together with **x-obs-server-side-encryption-customer-algorithm** and **x-obs-server-side-encryption-customer-key-MD5**.	No. This header is required when SSE-C is used.

Header	Description	Mandatory
x-obs-server-side-encryption-customer-key-MD5	Indicates the MD5 value of the encryption key when SSE-C is used. The MD5 value is used to check whether any error occurs during the transmission of the key. Type: string Example: **x-obs-server-side-encryption-customer-key-MD5:4XvB3tbNTN+tIEVa0/fGaQ==** Constraint: This header is a Base64-encoded 128-bit MD5 value and must be used together with **x-obs-server-side-encryption-customer-algorithm** and **x-obs-server-side-encryption-customer-key**.	No. This header is required when SSE-C is used.

Request Elements

This request involves no elements.

Response Syntax

```
HTTP/1.1 status_code
Date: date
ETag: etag
Content-Length: length
```

Response Headers

The response to the request uses common headers. For details, see **Table 3-19**.

NOTE

The ETag returns the hash value of the data to be uploaded, not the hash value of the entire object.

Table 5-78 Additional response headers

Header	Description
x-obs-version-id	Object version ID. If versioning is enabled for the bucket, the object version ID will be returned. Type: string
x-obs-server-side-encryption	This header is included in a response if SSE-KMS is used. Type: string Example: **x-obs-server-side-encryption:kms**

Header	Description
x-obs-server-side-encryption-kms-key-id	Indicates the master key ID. This header is included in a response when SSE-KMS is used. Type: string Format: *regionID*:*domainID*:**key/***key_id* *regionID* indicates the ID of the region where the key belongs. *domainID* indicates the ID of the tenant where the key belongs. *key_id* indicates the key ID used in this encryption. Example: **x-obs-server-side-encryption-kms-key-id:***region***:domainiddomainiddomai-niddoma0001:key/4f1cd4de-ab64-4807-920a-47fc42e7f0d0**
x-obs-server-side-encryption-customer-algorithm	Indicates the encryption algorithm. This header is included in a response when SSE-C is used. Type: string Example: **x-obs-server-side-encryption-customer-algorithm:AES256**
x-obs-server-side-encryption-customer-key-MD5	Indicates the MD5 value of the key for encrypting objects. This header is included in a response when SSE-C is used. Type: string Example: **x-obs-server-side-encryption-customer-key-MD5:4XvB3tbNTN+tIEVa0/fGaQ==**
x-obs-next-append-position	Indicates the position to be provided for the next request. Type: integer

Response Elements

This response contains no elements.

Error Responses

1. If the object length exceeds the limit due to the appending upload, OBS returns **400 Bad Request** and the error code is **AppendTooLarge**.

2. If the value of position is different from the original length of the current object, OBS returns **409 Conflict** and the error code is **PositionNotEqualToLength**.
3. If an object with the same object name exists in a bucket and the object type is not Appendable, OBS returns **409 Conflict** and the error code is **ObjectNotAppendable**.
4. If the number of write times of an object exceeds 10000, OBS returns **409 Conflict** and the error code is **ObjectNotAppendable**.
5. If the object storage class is **COLD** (Cold), this API cannot be called. If you still call this API, OBS returns **409 Conflict** with the error code of **ObjectNotAppendable**.

Other errors are included in **Table 6-2**.

Sample Request: Append Upload

```
POST /object?append&position=0 HTTP/1.1
Host: examplebucket.obs.region.example.com
Expires: Wed, 27 Jun 2015 13:45:50 GMT
Date: Wed, 08 Jul 2015 06:57:01 GMT
Content-Type: image/jpg
Content-Length: 1458
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:kZoYNv66bsmc10+dcGKw5x2PRrk=

[1458 bytes of object data]
```

Sample Response: Append Upload

```
HTTP/1.1 200 OK
Date: Wed, 27 Jun 2015 13:45:50 GMT
ETag: "d41d8cd98f00b204e9800998ecf8427e"
Content-Length: 0
Server: OBS
x-obs-request-id: 8DF400000163D3F0FD2A03D2D30B0542
x-obs-id-2: 32AAAUgAIAABAAAQAAEAABAAAQAAEAABCTjCqTmsA1XRpIrmrJdvcEWvZyjbztdd
x-obs-next-append-position: 1458
```

Sample Request: Append Upload (with redirect and a User-Defined Header Used)

The bucket **examplebucket** exists but the object **obj001** does not exist. Create an object by making the API call for the append operation. Set the redirection header field as follows: **"x-obs-website-redirect-location":"http://www.example.com/"**, and set the user-defined header field to: **"x-obs-meta-redirect":"redirect"**. The request is as follows:

```
POST /obj001?append&position=0 HTTP/1.1
Host: examplebucket.obs.region.example.com
Expires: Wed, 27 Jun 2015 13:45:50 GMT
Date: Wed, 08 Jul 2015 06:57:01 GMT
x-obs-website-redirect-location: http://www.example.com/
x-obs-meta-redirect: redirect
Content-Length: 6
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:kZoYNv66bsmc10+dcGKw5x2PRrk=

[6 bytes of object data]
```


Sample Response: Append Upload (with redirect and a User-Defined Header Used)

```
HTTP/1.1 200 OK
Date: Wed, 27 Jun 2015 13:45:50 GMT
ETag: "9516dfb15f51c7ee19a4d46b8c0dbe1d"
Content-Length: 0
Server: OBS
x-obs-request-id: 5DEB00000164A3150AC36F8F0C120D50
x-obs-id-2: 32AAAUgAIAABAAAQAAEAABAAAQAAEAABCSrVlTYwsA4p9GEW+LYqotSl5BYDxHfT
x-obs-next-append-position: 6
```

5.4.10 Configuring an Object ACL

Functions

OBS supports the control of access permission for objects. By default, only the object creator has the read and write permissions for the object. However, the creator can set a public access policy to assign the read permission to all other users. Even if the ACL is configured for an object encrypted in the SSE-KMS mode, the inter-tenant access is unavailable.

You can set an access control policy when uploading an object or make a call of an API operation to modify or obtain the object ACL. An object ACL supports a maximum of 100 grants.

This section explains how to modify an object ACL and change access permission on an object.

Versioning

By default, this operation modifies the ACL of the latest version of an object. To specify a specified version, the request can carry the **versionId** parameter.

Request Syntax

```
PUT /ObjectName?acl HTTP/1.1
Host: bucketname.obs.region.example.com
Date: date
Authorization: authorization

<AccessControlPolicy>
   <Owner>
      <ID>ID</ID>
   </Owner>
   <Delivered>true</Delivered>
   <AccessControlList>
      <Grant>
         <Grantee>
            <ID>ID</ID>
         </Grantee>
         <Permission>permission</Permission>
      </Grant>
   </AccessControlList>
</AccessControlPolicy>
```

Request Parameters

Table 5-79 describes the request parameters.

Table 5-79 Request parameters

Parameter	Description	Mandatory
versionId	Object version ID. Object ACL of a specified version is to be changed. Type: string	No

Request Headers

This request uses common headers. For details, see **Table 3-3**.

Request Elements

The request message carries the ACL information of the object by using message elements. For the meanings of the elements, see **Table 5-80**.

Table 5-80 Request elements

Element	Description	Mandatory
Owner	Bucket owner information, including the ID Type: XML	Yes
ID	Domain ID of a user. Type: string	Yes
Grant	Container for the grantee and the granted permissions. A single object ACL can contain no more than 100 grants. Type: XML	No
Grantee	Container for the details about the grantee. Type: XML	No
Canned	Grants permissions to all users. Value range: Everyone Type: string	No
Delivered	Indicates whether an object ACL inherits the ACL of a bucket. Type: boolean Default value: **true**	No

Element	Description	Mandatory
Permission	Authorized permission. Value options: **READ**, **READ_ACP**, **WRITE_ACP**, **FULL_CONTROL** Type: string	No
AccessControlList	Indicates an ACL, which consists of three elements: **Grant**, **Grantee**, and **Permission**. Type: XML	Yes

Response Syntax

```
HTTP/1.1 status_code
Content-Length: length
Content-Type: application/xml
```

Response Headers

The response to the request uses common headers. For details, see **Table 3-19**.

In addition to the common response headers, the headers listed in **Table 5-81** may be used.

Table 5-81 Additional response headers

Header	Description
x-obs-version-id	Version number of the object whose ACL is to be modified. Type: string

Response Elements

This response contains no elements.

Error Responses

No special error responses are returned. For details about error responses, see **Table 6-2**.

Sample Request

```
PUT /obj2?acl HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
Date: WED, 01 Jul 2015 04:42:34 GMT
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:8xAODun1ofjkwHm8YhtN0QEcy9M=
Content-Length: 727
```



```
<AccessControlPolicy xmlns="http://obs.example.com/doc/2015-06-30/">
  <Owner>
    <ID>b4bf1b36d9ca43d984fbcb9491b6fce9</ID>
  </Owner>
  <Delivered>false</Delivered>
  <AccessControlList>
    <Grant>
      <Grantee>
        <ID>b4bf1b36d9ca43d984fbcb9491b6fce9</ID>
      </Grantee>
      <Permission>FULL_CONTROL</Permission>
    </Grant>
    <Grant>
      <Grantee>
        <ID>783fc6652cf246c096ea836694f71855</ID>
      </Grantee>
      <Permission>READ</Permission>
    </Grant>
    <Grant>
      <Grantee>
        <Canned>Everyone</Canned>
      </Grantee>
      <Permission>READ</Permission>
    </Grant>
  </AccessControlList>
</AccessControlPolicy>
```

Sample Response

```
HTTP/1.1 200 OK
Server: OBS
x-obs-request-id: 8DF400000163D3F0FD2A03D2D30B0542
x-obs-id-2: 32AAAUgAIAABAAAQAAEAABAAAQAAEAABCTjCqTmsA1XRpIrmrJdvcEWvZyjbztdd
Date: WED, 01 Jul 2015 04:42:34 GMT
Content-Length: 0
```

5.4.11 Obtaining Object ACL Configuration

Functions

The implementation of this operation returns the ACL configuration of an object. You can perform this operation to view the ACL of an object, as long as you have the read permission for the object ACL.

Versioning

By default, this operation obtains the ACL of the latest version of an object. If the object has a delete marker, status code 404 is returned. To obtain the ACL of a specified version, the **versionId** parameter can be used to specify the desired version.

Request Syntax

```
GET /ObjectName?acl HTTP/1.1
Host: bucketname.obs.region.example.com
Date: date
Authorization: authorization
```

Request Parameters

The request parameter specifies the object ACL to be obtained. For details about the parameters, see **Table 5-82**.

Table 5-82 Request parameters

Parameter	Description	Mandatory
versionId	Version number of an object. Type: string	No

Request Headers

This request uses common headers. For details, see **Table 3-3**.

Request Elements

This request involves no elements.

Response Syntax

```
HTTP/1.1 status_code
Date: date
Content-Length: length
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<AccessControlPolicy xmlns="http://obs.region.example.com/doc/2015-06-30/">
   <Owner>
      <ID>id</ID>
   </Owner>
   <Delivered>true</Delivered>
   <AccessControlList>
      <Grant>
         <Grantee>
            <ID>id</ID>
         </Grantee>
         <Permission>permission</Permission>
      </Grant>
   </AccessControlList>
</AccessControlPolicy>
```

Response Headers

The response to the request uses common headers. For details, see **Table 3-19**.

In addition to the common response headers, the headers listed in **Table 5-83** may be used.

Table 5-83 Additional response header

Header	Description
x-obs-version-id	Version number of an object. Valid value: string Default value: none

Response Elements

The response message of the request returns the ACL information of the object. **Table 5-84** describes the elements.

Table 5-84 Response elements

Element	Description
ID	User account ID Type: string
AccessControlList	List of users and their permissions for the bucket. Type: XML
Grant	Identifies the grantee and the permissions of the grantee. Type: XML
Grantee	Container for the details about the grantee. Type: XML
Delivered	Indicates whether an object ACL inherits the ACL of a bucket. Type: boolean
Permission	Permissions of a specified user for the bucket. Type: string

Error Responses

No special error responses are returned. For details about error responses, see **Table 6-2**.

Sample Request

```
GET /object011?acl HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
Date: WED, 01 Jul 2015 04:45:55 GMT
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:YcmvNQxItGjFeeC1K2HeUEp8MMM=
```

Sample Response

```
HTTP/1.1 200 OK
Server: OBS
x-obs-request-id: 8DF400000163D3E650F3065C2295674C
x-obs-id-2: 32AAAQAAEAABAAAQAAEAABAAAQAAEAABCS+wsHqRuA2Tx+mXUpNtBbWLPMle9CIx
Content-Type: application/xml
Date: WED, 01 Jul 2015 04:45:55 GMT
Content-Length: 769

<?xml version="1.0" encoding="utf-8"?>
<AccessControlPolicy xmlns="http://obs.region.example.com/doc/2015-06-30/">
  <Owner>
```



```
  <ID>b4bf1b36d9ca43d984fbcb9491b6fce9</ID>
 </Owner>
 <Delivered>false</Delivered>
 <AccessControlList>
  <Grant>
   <Grantee>
    <ID>b4bf1b36d9ca43d984fbcb9491b6fce9</ID>
   </Grantee>
   <Permission>FULL_CONTROL</Permission>
  </Grant>
  <Grant>
   <Grantee>
    <ID>783fc6652cf246c096ea836694f71855</ID>
   </Grantee>
   <Permission>READ</Permission>
   </Grant>
  <Grant>
   <Grantee>
    <Canned>Everyone</Canned>
   </Grantee>
   <Permission>READ_ACP</Permission>
  </Grant>
 </AccessControlList>
</AccessControlPolicy>
```

5.4.12 Modifying Object Metadata

Functions

This operation modifies, deletes, or adds metadata to uploaded objects in a bucket.

Request Syntax

```
PUT /ObjectName?metadata HTTP/1.1
Host: bucketname.obs.region.example.com
Content-Type: application/xml
Content-Length: length
Authorization: authorization
Date: date
<Optional Additional Header>
<object Content>
```

Request Parameters

Table 5-85 Request parameters

Parameter	Description	Mandatory
versionId	Object version ID Type: string	No

Request Headers

NOTE

OBS supports the six HTTP request headers: Cache-Control, Expires, Content-Encoding, Content-Disposition, Content-Type, and Content-Language. It saves these header values in the metadata of the object. When the object is downloaded or queried, the saved values are set for corresponding HTTP headers and returned to the client.

Table 5-86 Request headers

Header	Description	Mandatory
x-obs-metadata-directive	Metadata operation indicator. The value can be **REPLACE_NEW** or **REPLACE**. **REPLACE_NEW**: The metadata that has an existing value is replaced. A value is assigned to the metadata that does not have a value. The metadata that is not specified remains unchanged. (Note: a header with custom metadata is replaced.) **REPLACE**: Use the header field carried in the current request to replace the original metadata. The metadata that is not specified (except **x-obs-storage-class**) will be deleted. Type: string	Yes
Cache-Control	Specifies the cache behavior of the web page when the object is downloaded. Type: string	No
Content-Disposition	Specifies the name of the object when it is downloaded. Type: string	No
Content-Encoding	Specifies the content encoding format when an object is being downloaded. Type: string	No
Content-Language	Specifies the content language format when an object is downloaded. Type: string	No
Content-Type	Object file type. Type: string	No
Expires	Specifies the cache expiration time of the web page when the object is downloaded. Type: string	No

Header	Description	Mandatory
x-obs-website-redirect-location	When the bucket is configured with the website redirection, the request for obtaining the object can be redirected to another object or an external URL in the bucket. In the following example, the request header sets the redirection to an object (**anotherPage.html**) in the same bucket: x-obs-website-redirect-location:/anotherPage.html In the following example, the request header sets the object redirection to an external URL: x-obs-website-redirect-location:http://www.example.com/ Type: string Constraint: The value must be prefixed by a slash (/), **http://**, or **https://**. The length of the value cannot exceed 2 KB.	No
x-obs-storage-class	Specifies the storage class of an object. Type: string Storage class options: **STANDARD** (Standard), **WARM** (Warm), **COLD** (Cold). These values are case sensitive. Example: **x-obs-storage-class: STANDARD**	No
x-obs-meta-*	A message header starting with **x-obs-meta-** can be added to a request to add custom metadata for object management. Custom metadata will be returned in the response header when you retrieve or query the metadata of the object. Type: string Example: **x-obs-meta-test: test metadata**	No

Request Elements

This request involves no elements.

Response Syntax

```
HTTP/1.1 status_code
Date: date
Content-Length: length
Etag: etag
Last-Modified: time
```


Response Headers

Table 5-87 Additional response headers

Header	Description
x-obs-metadata-directive	Metadata operation indicator. The value can be **REPLACE_NEW** or **REPLACE**. Type: string
Cache-Control	Specifies the cache behavior of the web page when the object is downloaded. If a request carries this header field, the response message must contain this header field. Type: string
Content-Disposition	Specifies the name of the object when it is downloaded. If a request carries this header field, the response message must contain this header field. Type: string
Content-Encoding	Specifies the content encoding format when an object is being downloaded. If a request carries this header field, the response message must contain this header field. Type: string
Content-Language	Specifies the content language format when an object is downloaded. If a request carries this header field, the response message must contain this header field. Type: string
Expires	Specifies the cache expiration time of the web page when the object is downloaded. If a request carries this header field, the response message must contain this header field. Type: string
x-obs-website-redirect-location	When the bucket is configured with the website redirection, the request for obtaining the object can be redirected to another object or an external URL in the bucket. If a request carries this header field, the response message must contain this header field. Type: string
x-obs-storage-class	Specifies the storage class of an object. If a request carries this header field, the response message must contain this header field. Type: string
x-obs-meta-*	Custom metadata is used to manage objects in a customized manner. If a request carries this header field, the response message must contain this header field. Type: string

Response Elements

This response contains no elements.

Error Responses

No special error responses are returned. For details about error responses, see **Table 6-2**.

Sample Request: Adding Metadata for an Object

Add the following metadata to the object: **Content-Type:application/zip** and **x-obs-meta-test:meta**.

```
PUT /object?metadata HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
Date: WED, 01 Jul 2015 14:24:33 GMT
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:NxtSMS0jaVxlLnxlO9awaMTn47s=
x-obs-metadata-directive:REPLACE_NEW
Content-Type:application/zip
x-obs-meta-test:meta
```

Sample Response: Adding Metadata for an Object

```
HTTP/1.1 200 OK
Server: OBS
x-obs-request-id: 8DF400000163D3E4BB5905C41B6E65B6
Accept-Ranges: bytes
x-obs-id-2: 32AAAQAAEAABAAAQAAEAABAAAQAAEAABCSD3nAiTaBoeyt9oHp9vTYtXnLDmwV6D
Date: WED, 01 Jul 2015 04:19:21 GMT
Content-Length: 0
x-obs-metadata-directive:REPLACE_NEW
x-obs-meta-test:meta
```

Sample Request: Editing Metadata of an Object

If metadata **x-obs-meta-test:testmeta** exists in the object and the value of **x-obs-storage-class** is **WARM**, change the metadata **x-obs-meta-test** of the object to **newmeta** and change **x-obs-storage-class** to **COLD**.

```
PUT /object?metadata HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
Date: WED, 01 Jul 2015 14:24:33 GMT
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:NxtSMS0jaVxlLnxlO9awaMTn47s=
x-obs-metadata-directive:REPLACE_NEW
x-obs-meta-test:newmeta
x-obs-storage-class:COLD
```

Sample Response: Editing Metadata of an Object

```
HTTP/1.1 200 OK
Server: OBS
x-obs-request-id: 8DF400000163D3E4BB5905C41B6E65B6
Accept-Ranges: bytes
x-obs-id-2: 32AAAQAAEAABAAAQAAEAABAAAQAAEAABCSD3nAiTaBoeyt9oHp9vTYtXnLDmwV6D
Date: WED, 01 Jul 2015 04:19:21 GMT
Content-Length: 0
x-obs-metadata-directive:REPLACE_NEW
x-obs-meta-test:newmeta
x-obs-storage-class:COLD
```


Sample Request: Deleting Metadata of an Object

Metadata **x-obs-meta-test:newmeta** and **Content-Type:application/zip** exist in the object, and delete **x-obs-meta-test**.

```
PUT /object?metadata HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
Date: WED, 01 Jul 2015 14:24:33 GMT
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:NxtSMS0jaVxlLnxlO9awaMTn47s=
x-obs-metadata-directive:REPLACE
Content-Type:application/zip
```

Sample Response: Deleting Metadata of an Object

```
HTTP/1.1 200 OK
Server: OBS
x-obs-request-id: 8DF400000163D3E4BB5905C41B6E65B6
Accept-Ranges: bytes
x-obs-id-2: 32AAAQAAEAABAAAQAAEAABAAAQAAEAABCSD3nAiTaBoeyt9oHp9vTYtXnLDmwV6D
Date: WED, 01 Jul 2015 04:19:21 GMT
Content-Length: 0
x-obs-metadata-directive:REPLACE
```

5.4.13 Modifying an Object

Functions

This operation can modify an object from a specified position.

NOTE

This API is supported only by parallel file systems. For details about how to create a parallel file system, see **Sample Request: Creating a Parallel File System**.

Request Syntax

```
PUT /ObjectName?modify&position=Position HTTP/1.1
Host: bucketname.obs.region.example.com
Content-Type: type
Content-Length: length
Authorization: authorization
Date: date
<object Content>
```

Request Parameters

The request needs to specify parameters in the message, indicating that the upload is for modification, and specifying the position in the object to be modified. **Table 5-88** describes the parameters.

Table 5-88 Request parameters

Parameter	Description	Mandatory
modify	Indicates that the file is uploaded for modification. Type: string	Yes
position	Position in the object where the modification starts Type: integer	Yes

Request headers

This request uses common request headers. For details, see **Table 3-3**.

Request Elements

This request involves no elements.

Response Syntax

```
HTTP/1.1 status_code
Date: Date
ETag: etag
Content-Length: length
Server: OBS
x-obs-request-id: request-id
x-obs-id-2: id
```

Response Headers

The response to the request uses common headers. For details, see **Table 3-19**.

Response Elements

This response contains no elements.

Error Responses

No special error responses are returned. For details about error responses, see **Table 6-2**.

Sample Request

```
PUT /ObjectName?modify&position=Position HTTP/1.1
Host: examplebucket.obs.region.example.com
Date: Wed, 08 Jul 2015 06:57:01 GMT
Content-Type: image/jpg
Content-Length: 1458
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:kZoYNv66bsmc10+dcGKw5x2PRrk=

[1458 bytes of object data]
```


Sample Response

```
HTTP/1.1 200
Date: Wed, 08 Jul 2015 06:57:02 GMT
ETag: "d41d8cd98f00b204e9800998ecf8427e"
Content-Length: 0
Server: OBS
x-obs-request-id: 8DF400000163D3F0FD2A03D2D30B0542
x-obs-id-2: 32AAAUgAIAABAAAQAAEAABAAAQAAEAABCTjCqTmsA1XRpIrmrJdvcEWvZyjbztd
```

5.4.14 Truncating an Object

Functions

This operation can truncate an object to a specified size.

NOTE

This API is supported only by parallel file systems. For details about how to create a parallel file system, see **Sample Request: Creating a Parallel File System**.

Request Syntax

```
PUT /ObjectName?truncate&length=Length HTTP/1.1
Host: bucketname.obs.region.example.com
Authorization: authorization
Content-Length: length
Date: date
```

Request Parameters

The request needs to specify parameters in the message, indicating that this is to truncate an object to a specified size. **Table 5-89** describes the parameters.

Table 5-89 Request parameters

Parameter	Description	Mandatory
truncate	Indicates that the upload is for truncation. Type: string	Yes
length	Size of the object after the truncation Type: integer	Yes

Request headers

This request uses common request headers. For details, see **Table 3-3**.

Request Elements

This request involves no elements.

Response Syntax

```
HTTP/1.1 204 status_code
Server: OBS
```



```
x-obs-request-id: request-id
x-obs-id-2: id
Date: Date
```

Response Headers

The response to the request uses common headers. For details, see **Table 3-19**.

Response Elements

This response contains no elements.

Error Responses

No special error responses are returned. For details about error responses, see **Table 6-2**.

Sample Request

```
PUT /ObjectName?truncate&length=1000 HTTP/1.1
Host: examplebucket.obs.region.example.com
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:75/Y4Ng1izvzc1nTGxpMXTE6ynw=
Content-Length: 1
Date: WED, 01 Jul 2015 04:19:20 GMT
```

Sample Response

```
HTTP/1.1 204 No Content
Server: OBS
x-obs-request-id: 8DF400000163D3F51DEA05AC9CA066F1
x-obs-id-2: 32AAAUgAIAABAAAQAAEAABAAAQAAEAABCSgkM4Dij80gAeFY8pAZIwx72QhDeBZ5
Date: WED, 01 Jul 2015 04:19:21 GMT
```

5.4.15 Renaming an Object

Functions

This operation can rename an object.

NOTE

This API is supported only by parallel file systems. For details about how to create a parallel file system, see **Sample Request: Creating a Parallel File System**. Renaming an object is a non-idempotent operation.

Request Syntax

```
POST /ObjectName?name=Name&rename HTTP/1.1
Host: bucketname.obs.region.example.com
Authorization: authorization
Date: date
```

Request Parameters

The request needs to specify parameters in the message, indicating that this is a renaming operation, specifying the new name. **Table 5-90** describes the parameters.

Table 5-90 Request parameters

Parameter	Description	Mandatory
name	New name for the object. Use the absolute path. Type: string	Yes
rename	Indicates that this is a renaming operation. Type: string	Yes

Request Headers

This request uses common request headers. For details, see **Table 3-3**.

Request Elements

This request involves no elements.

Response Syntax

```
HTTP/1.1 204 status_code
Server: OBS
x-obs-request-id: request-id
x-obs-id-2: id
Date: Date
```

Response Headers

The response to the request uses common headers. For details, see **Table 3-19**.

Response Elements

This response contains no elements.

Error Responses

No special error responses are returned. For details about error responses, see **Table 6-2**.

Sample Request

```
POST /ObjectName?name=file2&rename HTTP/1.1
Host: examplebucket.obs.region.example.com
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:75/Y4Ng1izvzc1nTGxpMXTE6ynw=
Date: WED, 01 Jul 2015 04:19:20 GMT
```

Sample Response

```
HTTP/1.1 204 No Content
Server: OBS
x-obs-request-id: 8DF400000163D3F51DEA05AC9CA066F1
x-obs-id-2: 32AAAUgAIAABAAAQAAEAABAAAQAAEAABCSgkM4Dij80gAeFY8pAZIwx72QhDeBZ5
Date: WED, 01 Jul 2015 04:19:21 GMT
```


5.5 Operations on Multipart Upload

5.5.1 Listing Initiated Multipart Uploads in a Bucket

Functions

This operation queries all the multipart upload tasks that are initialized but have not been merged or canceled in a bucket.

Request Syntax

```
GET /?uploads&max-uploads=max HTTP/1.1
Host: bucketname.obs.region.example.com
Date: date
Authorization: authorization
```

Request Parameters

This request uses parameters to specify the query range for multipart uploads. Table 5-91 describes the parameters.

Table 5-91 Request parameters

Parameter	Description	Mandatory
delimiter	For a multipart upload that contains delimiters, the string between the first character and the first delimiter in the object name (excluding the prefix specified in the request, if any) are returned as **CommonPrefix**. Multipart uploads with objects that contain **CommonPrefix** are considered as a group and returned as one record. The record contains no information about the tasks, only informing the user that the group involves multipart uploads. Type: string	No
prefix	If a prefix is specified, the response only contains tasks whose names start with the prefix value. Type: string	No
max-uploads	Maximum number of multipart upload tasks returned. The value ranges from 1 to 1000. If the value has exceeded this range, 1000 tasks are returned by default. Type: integer	No

Parameter	Description	Mandatory
key-marker	Lists multipart uploads that follow the value of **key-marker**. Type: string	No
upload-id-marker	Lists multipart tasks that follow the value of **upload-id-marker** in **key-marker**. This parameter only functions together with **key-marker**. Type: string	No

Request Headers

This request uses common headers. For details, see **Table 3-3**.

Request Elements

This request involves no elements.

Response Syntax

```
HTTP/1.1 status_code
Date: date
Content-Length: length

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ListMultipartUploadsResult xmlns="http://obs.region.example.com/doc/2015-06-30/">
   <Bucket>bucketname</Bucket>
   <KeyMarker/>
   <UploadIdMarker/>
   <NextKeyMarker>nextMarker</NextKeyMarker>
   <NextUploadIdMarker>idMarker</NextUploadIdMarker>
   <MaxUploads>maxUploads</MaxUploads>
   <IsTruncated>true</IsTruncated>
   <Upload>
      <Key>key</Key>
      <UploadId>uploadID</UploadId>
      <Initiator>
         <ID>domainID/domainID:userID/userID</ID>
      </Initiator>
      <Owner>
         <ID>ownerID</ID>
      </Owner>
      <StorageClass>storageclass</StorageClass>
      <Initiated>initiatedDate</Initiated>
   </Upload>
</ListMultipartUploadsResult>
```

Response Headers

The response to the request uses common headers. For details, see **Table 3-19**.

Response Elements

This response contains elements of information about the multipart uploads. **Table 5-92** describes the elements.

Table 5-92 Response elements

Element	Description
ListMultipartUploadsResult	Container for responses of requests. Type: container Child: Bucket, KeyMarker, UploadIdMarker, NextKeyMarker, NextUploadIdMarker, MaxUploads, Delimiter, Prefix, Upload, CommonPrefixes, and IsTruncated Parent: none
Bucket	Name of the bucket to which the multipart upload was initiated Type: string Parent: ListMultipartUploadsResult
KeyMarker	Object keys at or after which the multipart upload listing begins Type: string Parent: ListMultipartUploadsResult
UploadIdMarker	Upload ID after which the multipart upload listing begins Type: string Parent: ListMultipartUploadsResult
NextKeyMarker	Value of **KeyMarker** in a subsequent request after a multipart upload list is truncated Type: string Parent: ListMultipartUploadsResult
NextUploadIdMarker	Value of UploadMarker in a subsequent request when a multipart upload list is truncated. Type: string Parent: ListMultipartUploadsResult
MaxUploads	Maximum of multipart uploads to be returned in the response Type: integer Parent: ListMultipartUploadsResult
IsTruncated	Indicates whether the returned list of multipart uploads is truncated. The value **true** indicates that the list was truncated and **false** indicates that the list was not truncated. Type: boolean Parent: ListMultipartUploadsResult

Element	Description
Upload	Container for elements related to a specific multipart upload Type: container Child: Key, UploadId, InitiatorOwner, StorageClass, and Initiated Parent: ListMultipartUploadsResult
Key	Indicates the name of the object for which a multipart upload is initiated. Type: string Parent: Upload
UploadId	ID of the multipart upload Type: string Parent: Upload
Initiator	Container element that identifies who initiated the multipart upload Child: ID Type: container Parent: Upload
ID	ID of the account to which the owner belongs. Type: string Parent: Initiator or Owner
Owner	Owner of the part. Type: container Child: ID Parent: Upload
StorageClass	Indicates the storage class that will be used for storing an object when the multipart is uploaded. Type: string Parent: Upload
Initiated	Date and time when the multipart upload was initiated Type: date Parent: Upload
ListMultipartUploadsResult.Prefix	Specified prefix in a request. Type: string Parent: ListMultipartUploadsResult

Element	Description
Delimiter	Delimiter in a request. Type: string Parent: ListMultipartUploadsResult
CommonPrefixes	Indicates group information. If you specify a delimiter in the request, the response contains group information in **CommonPrefixes**. Type: container Parent: ListMultipartUploadsResult
CommonPrefixes. Prefix	Indicates a different prefix in the group information in **CommonPrefixes**. Type: string Parent: CommonPrefixes

Error Responses

If the value of **maxUploads** is a non-integer or smaller than 0, OBS returns **400 Bad Request**.

Other errors are included in **Table 6-2**.

Sample Request: Listing Initiated Multipart Uploads

```
GET /?uploads HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
Date: WED, 01 Jul 2015 04:51:21 GMT
Authorization: OBS UDSIAMSTUBTEST000008:XdmZgYQ+ZVy1rjxJ9/KpKq+wrU0=
```

Sample Response: Listing Initiated Multipart Uploads

```
HTTP/1.1 200 OK
Server: OBS
x-obs-request-id: 8DF400000163D405534D046A2295674C
x-obs-id-2: 32AAAQAAEAABAAAQAAEAABAAAQAAEAABCSDaHP+a+Bp0RI6Mm9XvCOrf7q3qvBQW
Content-Type: application/xml
Date: WED, 01 Jul 2015 04:51:21 GMT
Content-Length: 681

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ListMultipartUploadsResult xmlns="http://obs.example.com/doc/2015-06-30/">
  <Bucket>examplebucket</Bucket>
  <KeyMarker/>
  <UploadIdMarker/>
  <Delimiter/>
  <Prefix/>
  <MaxUploads>1000</MaxUploads>
  <IsTruncated>false</IsTruncated>
  <Upload>
    <Key>obj2</Key>
    <UploadId>00000163D40171ED8DF4050919BD02B8</UploadId>
    <Initiator>
      <ID>domainID/b4bf1b36d9ca43d984fbcb9491b6fce9:userID/71f390117351534r88115ea2c26d1999</ID>
    </Initiator>
```



```
  <Owner>
    <ID>b4bf1b36d9ca43d984fbcb9491b6fce9</ID>
  </Owner>
  <StorageClass>STANDARD</StorageClass>
  <Initiated>2015-07-01T02:30:54.582Z</Initiated>
 </Upload>
</ListMultipartUploadsResult>
```

Sample Request: Listing Initiated Multipart Uploads (with a Prefix and Delimiter Specified)

The following example describes how to list two initiated multipart uploads (with objects **multipart-object001** and **part2-key02** in bucket **examplebucket**. In this listing operation, **prefix** is set to **multipart** and **object001** is set to **delimiter**.

```
GET /?uploads&delimiter=object001&prefix=multipart HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
Date: WED, 01 Jul 2015 04:51:21 GMT
Authorization: OBS UDSIAMSTUBTEST000008:XdmZgYQ+ZVy1rjxJ9/KpKq+wrU0=
```

Sample Response: Listing Initiated Multipart Uploads (with a Prefix and Delimiter Specified)

```
HTTP/1.1 200 OK
Server: OBS
x-obs-request-id: 5DEB00000164A27A1610B8250790D703
x-obs-id-2: 32AAAQAAEAABAAAQAAEAABAAAQAAEAABCSq3ls2ZtLDD6pQLcJq1yGITXgspSvBR
Content-Type: application/xml
Date: WED, 01 Jul 2015 04:51:21 GMT
Content-Length: 681
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ListMultipartUploadsResult xmlns="http://obs.example.com/doc/2015-06-30/">
  <Bucket>newbucket0001</Bucket>
  <KeyMarker></KeyMarker>
  <UploadIdMarker>
  </UploadIdMarker>
  <Delimiter>object</Delimiter>
  <Prefix>multipart</Prefix>
  <MaxUploads>1000</MaxUploads>
  <IsTruncated>false</IsTruncated>
  <CommonPrefixes>
    <Prefix>multipart-object001</Prefix>
  </CommonPrefixes>
</ListMultipartUploadsResult>
```

5.5.2 Initiating a Multipart Upload

Functions

Before using this operation, make an API operation call to create a multipart upload task. The system will return a globally unique upload ID as the multipart upload identifier. This identifier can be used in subsequent requests including UploadPart, CompleteMultipartUpload, and ListParts. Create a multipart upload task does not affect the object that has the same name as object to be uploaded in multiple parts. You can create more than one multipart upload tasks for an object. This operation request can contain headers **x-obs-acl**, **x-obs-meta-***, **Content-Type**, and **Content-Encoding**. The headers are recorded in the multipart upload metadata.

This operation supports server-side encryption.

Request Syntax

```
POST /ObjectName?uploads  HTTP/1.1
Host: bucketname.obs.region.example.com
Date: date
Authorization: authorization
```

Request Parameters

This request uses parameters to specify a multipart upload. **Table 5-93** describes the parameters.

Table 5-93 Request parameters

Parameter	Description	Mandatory
uploads	Indicates a multipart upload. Type: string **NOTE** • This parameter is an empty string. • If this parameter is not contained in a request, the request performs a common upload using POST.	Yes

Request Headers

The request can use additional headers, as shown in **Table 5-94**.

Table 5-94 Request headers

Header	Description	Mandatory
x-obs-acl	When initiating a multipart upload, you can add this message header to set the permission control policy for the object. The predefined common policies are as follows: **private**, **public-read**, and **public-read-write**. Type: string Note: This header is a predefined policy expressed in a character string. Example: **x-obs-acl: public-read-write**	No

Header	Description	Mandatory
x-obs-grant-read	When initiating a multipart upload, you can use this header to grant all users in an account the permissions to read the object and obtain the object metadata. Type: string Example: **x-obs-grant-read: ID=domainID** If multiple accounts are authorized, separate them with commas (,).	No
x-obs-grant-read-acp	When initiating a multipart upload, you can use this header to grant all users in an account the permission to obtain the object ACL. Type: string Example: **x-obs-grant-read-acp: ID=domainID** If multiple accounts are authorized, separate them with commas (,).	No
x-obs-grant-write-acp	When initiating a multipart upload, you can use this header to grant all users in an account the permission to write the object ACL. Type: string Example: **x-obs-grant-write-acp: ID=domainID** If multiple accounts are authorized, separate them with commas (,).	No
x-obs-grant-full-control	When initiating a multipart upload, you can use this header to grant all users in an account the permissions to read the object, obtain the object metadata and ACL, and write the object ACL. Type: string Example: **x-obs-grant-full-control: ID=domainID** If multiple accounts are authorized, separate them with commas (,).	No
x-obs-storage-class	When initiating a multipart upload, you can add this header to specify the storage class for the object. If you do not use this header, the object storage class is the default storage class of the bucket. Type: string Storage class options: **STANDARD** (Standard), **WARM** (Warm), **COLD** (Cold). These values are case sensitive. Example: **x-obs-storage-class: STANDARD**	No

Header	Description	Mandatory
x-obs-website-redirect-location	If a bucket is configured with the static website hosting function, it will redirect requests for this object to another object in the same bucket or to an external URL. OBS stores the value of this header in the object metadata. Type: string Default value: none Constraint: The value must be prefixed by a slash (/), **http://**, or **https://**. The length of the value cannot exceed 2 KB.	No
x-obs-server-side-encryption	Indicates that SSE-KMS is used. Type: string Example: **x-obs-server-side-encryption:kms**	No. This header is required when SSE-KMS is used.
x-obs-server-side-encryption-kms-key-id	Indicates the master key when SSE-KMS is used. If this header is not provided, the default master key will be used. If there is no such a default master key, OBS will create one and use it by default. Type: string The following two formats are supported: - *regionID*:*domainID*:**key/***key_id* - *key_id* *regionID* indicates the ID of the region where the key belongs. *domainID* indicates the ID of the tenant where the key belongs. *key_id* indicates the ID of the key created in KMS. Examples: - **x-obs-server-side-encryption-kms-key-id:***region*:**domainiddomainiddomainiddo-ma0001:key/4f1cd4de-ab64-4807-920a-47fc42e7f0d0** - **x-obs-server-side-encryption-kms-key-id:4f1cd4de-ab64-4807-920a-47fc42e7f0d0**	No

Header	Description	Mandatory
x-obs-server-side-encryption-customer-algorithm	Indicates the encryption algorithm when SSE-C is used. Type: string Example: **x-obs-server-side-encryption-customer-algorithm:AES256** Constraint: This header must be used together with **x-obs-server-side-encryption-customer-key** and **x-obs-server-side-encryption-customer-key-MD5**.	No. This header is required when SSE-C is used.
x-obs-server-side-encryption-customer-key	Indicates the key for encrypting objects when SSE-C is used. Type: string Example: **x-obs-server-side-encryption-customer-key:K7QkYpBkM5+hca27fsNkUnNVaobncnLht/rCB2o/9Cw=** Constraint: This header is a Base64-encoded 256-bit key and must be used together with **x-obs-server-side-encryption-customer-algorithm** and **x-obs-server-side-encryption-customer-key-MD5**.	No. This header is required when SSE-C is used.
x-obs-server-side-encryption-customer-key-MD5	Indicates the MD5 value of the encryption key when SSE-C is used. The MD5 value is used to check whether any error occurs during the transmission of the key. Type: string Example: **x-obs-server-side-encryption-customer-key-MD5:4XvB3tbNTN+tIEVa0/fGaQ==** Constraint: This header is a Base64-encoded 128-bit MD5 value and must be used together with **x-obs-server-side-encryption-customer-algorithm** and **x-obs-server-side-encryption-customer-key**.	No. This header is required when SSE-C is used.
x-obs-expires	Specifies when an object expires. It is measured in days. Once the object expires, it is automatically deleted. (The calculation starts from when the object was last modified). Type: integer Example: **x-obs-expires:3**	No

Header	Description	Mandatory
x-obs-meta-*	When initiating a multipart upload, you can use a header starting with **x-obs-meta-** in the HTTP request to define object metadata for easy management. The user-defined metadata will be returned in the response when you retrieve the object or query the object metadata. Type: string Example: **x-obs-meta-test: test metadata**	No

For details about other common message headers, see **Table 3-3**.

Request Elements

This request involves no elements.

Response Syntax

```
HTTP/1.1 status_code
Date: date
Content-Length: length
Connection: status

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<InitiateMultipartUploadResult xmlns="http://obs.region.example.com/doc/2015-06-30/">
   <Bucket>BucketName</Bucket>
   <Key>ObjectName</Key>
   <UploadId>uploadID</UploadId>
</InitiateMultipartUploadResult>
```

Response Headers

The response to the request uses common headers. For details, see **Table 3-19**.

Table 5-95 Additional response headers

Header	Description
x-obs-server-side-encryption	This header is included in a response if SSE-KMS is used. Type: string Example: **x-obs-server-side-encryption:kms**

Header	Description
x-obs-server-side-encryption-kms-key-id	Indicates the master key ID. This header is included in a response when SSE-KMS is used. Type: string Format: *regionID*:*domainID*:**key/***key_id* *regionID* indicates the ID of the region where the key belongs. *domainID* indicates the ID of the tenant where the key belongs. *key_id* indicates the key ID used in this encryption. Example: **x-obs-server-side-encryption-kms-key-id:***region*:**domainiddomainiddomai-niddoma0001:key/4f1cd4de-ab64-4807-920a-47fc42e7f0d0**
x-obs-server-side-encryption-customer-algorithm	Indicates the encryption algorithm. This header is included in a response when SSE-C is used. Type: string Example: **x-obs-server-side-encryption-customer-algorithm:AES256**
x-obs-server-side-encryption-customer-key-MD5	Indicates the MD5 value of a key used to encrypt objects. This header is included in a response if SSE-C is used. Type: string Example: **x-obs-server-side-encryption-customer-key-MD5:4XvB3tbNTN+tIEVa0/fGaQ==**

Response Elements

This response contains elements to indicate the upload ID and the key (name) of the object (bucket) for which the multipart upload was initiated. The returned information is used in the subsequent operations. **Table 5-96** describes the elements.

Table 5-96 Response elements

Element	Description
InitiateMultipartUploadResult	Container of a multipart upload task. Type: XML

Element	Description
Bucket	Indicates the name of the bucket to which the multipart upload was initiated. Type: string
Key	Indicates the object key in a multipart upload. Type: string
UploadId	Indicates the ID for the initiated multipart upload. This ID is used for the subsequent operation. Type: string

Error Responses

1. If the AK or signature is invalid, OBS returns **403 Forbidden** and the error code is **AccessDenied**.

2. If the bucket is not found, OBS returns **404 Not Found** and the error code is **NoSuchBucket**.

3. Check whether the user has the write permission for the specified bucket. If not, OBS returns **403 Forbidden** and the error code is **AccessDenied**.

Other errors are included in **Table 6-2**.

Sample Request: Initiating a Multipart Upload

```
POST /objectkey?uploads  HTTP/1.1
Host: examplebucket.obs.region.example.com
Date: WED, 01 Jul 2015 05:14:52 GMT
Authorization: OBS AKIAIOSFODNN7EXAMPLE:VGhpcyBtZXNzYWdlIHNpZ25lZGGieSRlbHZpbmc=
```

Sample Response: Initiating a Multipart Upload

```
HTTP/1.1 200 OK
Server: OBS
x-obs-id-2: Weag1LuByRx9e6j5Onimru9pO4ZVKnJ2Qz7/C1NPcfTWAtRPfTaOFg==
x-obs-request-id: 996c76696e6727732072657175657374
Date: WED, 01 Jul 2015 05:14:52 GMT
Content-Length: 303

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<InitiateMultipartUploadResult xmlns="http://obs.region.example.com/doc/2015-06-30/">
  <Bucket>bucketname</Bucket>
  <Key>objectkey</Key>
  <UploadId>DCD2FC98B4F70000013DF578ACA318E7</UploadId>
</InitiateMultipartUploadResult>
```

Sample Request: Initiating a Multipart Upload (with the ACL Configured)

```
POST /objectkey?uploads  HTTP/1.1
Host: examplebucket.obs.region.example.com
Date: WED, 01 Jul 2015 05:15:43 GMT
x-obs-grant-write-acp:ID=52f24s3593as5730ea4f722483579ai7,ID=a93fcas852f24s3596ea8366794f7224
Authorization: OBS AKIAIOSFODNN7EXAMPLE:VGhpcyBtZXNzYWdlIHNpZ25lZGGieSRlbHZpbmc=
```


Sample Response: Initiating a Multipart Upload (with the ACL Configured)

```
HTTP/1.1 200 OK
Server: OBS
x-obs-id-2: 32AAAQAAEAABAAAQAAEAABAAAQAAEAABCTnv+daB51p+IVhAvWN7s5rSKhcWqDFs
x-obs-request-id: BB78000001648457112DF37FDFADD7AD
Date: WED, 01 Jul 2015 05:15:43 GMT
Content-Length: 303

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<InitiateMultipartUploadResult xmlns="http://obs.region.example.com/doc/2015-06-30/">
  <Bucket>bucketname</Bucket>
  <Key>objectkey</Key>
  <UploadId>000001648453845DBB78F2340DD460D8</UploadId>
</InitiateMultipartUploadResult>
```

5.5.3 Uploading Parts

Functions

After initiating a multipart upload, you can use this operation to upload parts for the multipart upload using its task ID. When parts are uploaded in a multipart upload of an object, the upload sequence does not affect part merging, namely, multiple parts can be uploaded concurrently.

Part sizes range from 100 KB to 5 GB. However, when parts are being merged, the size of the last uploaded part ranges from 0 to 5 GB. The upload part ID ranges from 1 to 10,000.

This operation supports server-side encryption.

NOTICE

The value of **partNumber** in a multipart task is unique. If you upload a part of the same **partNumber** repeatedly, the last part uploaded will overwrite the previous one. When multiple concurrent uploading of the same **partNumber** part of the same object is performed, the Last Write Win policy is applied. The time of **Last Write** is defined as the time when the metadata of the part is created. To ensure data accuracy, the client must be locked to ensure concurrent upload of the same part of the same object. Concurrent upload of different parts of the same object does not need to be locked.

Request Syntax

```
PUT /ObjectName?partNumber=partNum&uploadId=uploadID  HTTP/1.1
Host: bucketname.obs.region.example.com
Date: date
Content-Length: length
Authorization: authorization
Content-MD5:md5
<object Content>
```

Request Parameters

This request uses parameters to specify the upload task ID and part number. **Table 5-97** describes the parameters.

Table 5-97 Request parameters

Parameter	Description	Mandatory
partNumber	Indicates the ID of a part to be uploaded. The value is an integer from 1 to 10000. Type: integer	Yes
uploadId	Indicates a multipart upload ID. Type: string	Yes

Request Headers

This request uses common headers. For details, see **Table 3-3**.

Table 5-98 Server encryption request headers

Header	Description	Mandatory
x-obs-server-side-encryption-customer-algorithm	Indicates the encryption algorithm when SSE-C is used. Type: string Example: **x-obs-server-side-encryption-customer-algorithm:AES256** Constraint: This header must be used together with **x-obs-server-side-encryption-customer-key** and **x-obs-server-side-encryption-customer-key-MD5**.	No. This header is required when SSE-C is used. The encryption algorithm must be the same as that used to initiate multipart upload tasks.

Header	Description	Mandatory
x-obs-server-side-encryption-customer-key	Indicates the key for encrypting objects when SSE-C is used. Type: string Example: **x-obs-server-side-encryption-customer-key:K7QkYpBkM5+hca27fsNkUnNVaobncnLht/rCB2o/9Cw=** Constraint: This header is a Base64-encoded 256-bit key and must be used together with **x-obs-server-side-encryption-customer-algorithm** and **x-obs-server-side-encryption-customer-key-MD5**.	No. This header is required when SSE-C is used. The key must be the same as that used to initiate multipart upload tasks.
x-obs-server-side-encryption-customer-key-MD5	Indicates the MD5 value of the encryption key when SSE-C is used. The MD5 value is used to check whether any error occurs during the transmission of the key. Type: string Example: **x-obs-server-side-encryption-customer-key-MD5:4XvB3tbNTN+tIEVa0/fGaQ==** Constraint: This header is a Base64-encoded 128-bit MD5 value and must be used together with **x-obs-server-side-encryption-customer-algorithm** and **x-obs-server-side-encryption-customer-key**.	No. This header is required when SSE-C is used. The MD5 value must be the same as that used to initiate multipart upload tasks.

Request Elements

This request involves no elements.

Response Syntax

```
HTTP/1.1 status_code
Date: date
ETag: etag
Content-Length: length
```

Response Headers

The response to the request uses common headers. For details, see **Table 3-19**.

Table 5-99 Additional response headers

Header	Description
x-obs-server-side-encryption	This header is included in a response if SSE-KMS is used. Type: string Example: **x-obs-server-side-encryption:kms**
x-obs-server-side-encryption-kms-key-id	Indicates the master key ID. This header is included in a response when SSE-KMS is used. Type: string Format: *regionID*:*domainID*:**key/***key_id* *regionID* indicates the ID of the region where the key belongs. *domainID* indicates the ID of the tenant where the key belongs. *key_id* indicates the key ID used in this encryption. Example: **x-obs-server-side-encryption-kms-key-id:*region*:domainiddomainiddomai-niddoma0001:key/4f1cd4de-ab64-4807-920a-47fc42e7f0d0**
x-obs-server-side-encryption-customer-algorithm	Indicates the encryption algorithm. This header is included in a response when SSE-C is used. Type: string Example: **x-obs-server-side-encryption-customer-algorithm:AES256**

Header	Description
x-obs-server-side-encryption-customer-key-MD5	Indicates the MD5 value of the key for encrypting objects. This header is included in a response when SSE-C is used. Type: string Example: **x-obs-server-side-encryption-customer-key-MD5:4XvB3tbNTN+tIEVa0/fGaQ==**

Response Elements

This response contains no elements.

Error Responses

1. If a part number is not within the range from 1 to 10000, OBS returns **400 Bad Request**.
2. If a part size has exceeded 5 GB, the error code **400 Bad Request** is returned.
3. If the AK or signature is invalid, OBS returns **403 Forbidden** and the error code is **AccessDenied**.
4. Check whether the bucket exists. If the bucket is not found, OBS returns **404 Not Found** and the error code is **NoSuchBucket**.
5. View the bucket ACL to check whether the user has the read permission for the requested bucket. If the user does not have the read permission, OBS returns **403 AccessDenied**.
6. Check whether the multipart upload task exists. If the task does not exist, OBS returns **404 Not Found** and the error code is **NoSuchUpload**.
7. Check whether the request user is the initiator of the multipart upload task. If not, OBS returns **403 Forbidden** and the error code is **AccessDenied**.

Other errors are included in **Table 6-2**.

Sample Request

```
PUT /object02?partNumber=1&uploadId=00000163D40171ED8DF4050919BD02B8 HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
Date: WED, 01 Jul 2015 05:15:55 GMT
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:ZB0hFwaHubi1aKHv7dSZjJts40g=
Content-Length: 102015348

[102015348 Byte part content]
```

Sample Response

```
HTTP/1.1 200 OK
Server: OBS
x-obs-request-id: 8DF400000163D40956A703289CA066F1
ETag: "b026324c6904b2a9cb4b88d6d61c81d1"
x-obs-id-2: 32AAAQAAEAABAAAQAAEAABAAAQAAEAABCUQu/EOEVSMa04GXVwy0z9WI+BsDKvfh
```



```
Date: WED, 01 Jul 2015 05:15:55 GMT
Content-Length: 0
```

5.5.4 Copying Parts

Functions

After creating a multipart upload job, you can specify its upload ID and upload a part to the job in OBS. Alternatively, you can make an API call to add a part (part of an object or the whole object).

This operation supports server-side encryption.

NOTICE

You cannot determine whether a request is successful only based on the **status_code** in the returned HTTP header. If **200** is returned for **status_code**, the server has received the request and started to process the request. The copy is successful only when the body in the response contains ETag.

Copy the source object and save it as **part1**. If a **part1** already exists before the copying, the original **part1** will be overwritten by the newly copied **part1**. After the copy is successful, only the latest **part1** is displayed. The old **part1** data will be deleted. Therefore, ensure that the target part does not exist or has no value when using the part copy operation. Otherwise, data may be deleted by mistake. The source object in the copy process does not change.

Cold Objects

If source objects are in the Cold storage class, ensure that these objects have been restored before you copy them. If the source object is not restored or is being restored, the copy fails and error **403 Forbidden** is returned. The fault is described as follows:

ErrorCode: InvalidObjectState

ErrorMessage: Operation is not valid for the source object's storage class

Request Syntax

```
PUT /ObjectName?partNumber=partNum&uploadId=UploadID HTTP/1.1
Host: bucketname.obs.region.example.com
Date: date
x-obs-copy-source: sourceobject
x-obs-copy-source-range:bytes=start-end
Authorization: authorization
Content-Length: length
```

Request Parameters

To copy a part, you need to specify the part number of the target part and the multipart upload task number. **Table 5-100** describes the parameters.

Table 5-100 Request parameters

Parameter	Description	Mandatory
partNumber	Indicates the ID of a part to be uploaded. Type: integer	Yes
uploadId	Indicates a multipart upload ID. Type: string	Yes

Request Headers

In addition the common message headers, the request uses two extended headers. **Table 3-3** describes the common message header.

Table 5-101 Request headers

Header	Description	Mandatory
x-obs-copy-source	Indicates the source object to be copied. Type: string	Yes
x-obs-copy-source-range	Indicates the range of bytes (start - end) to be copied from the source object. **start** indicates the start byte of the part to be copied and **end** indicates the end byte. Type: integer	No
x-obs-server-side-encryption-customer-algorithm	Indicates the encryption algorithm for the part copy when SSE-C is used. Type: string Example: **x-obs-server-side-encryption-customer-algorithm:AES256** Constraint: This header must be used together with **x-obs-server-side-encryption-customer-key** and **x-obs-server-side-encryption-customer-key-MD5**.	No. This header is required when SSE-C is used. The encryption algorithm must be the same as that used to initiate multipart upload tasks.

Header	Description	Mandatory
x-obs-server-side-encryption-customer-key	Indicates the key for encrypting the part copy when SSE-C is used. Type: string Example: **x-obs-server-side-encryption-customer-key:K7QkYpBkM5+hca27fsNkUnNVaobncnLht/rCB2o/9Cw=** Constraint: This header is a Base64-encoded 256-bit key and must be used together with **x-obs-server-side-encryption-customer-algorithm** and **x-obs-server-side-encryption-customer-key-MD5**.	No. This header is required when SSE-C is used. The key must be the same as that used to initiate multipart upload tasks.
x-obs-server-side-encryption-customer-key-MD5	Indicates the MD5 value of the key for encrypting the part copy when SSE-C is used. The MD5 value is used to check whether any error occurs during the transmission of the key. Type: string Example: **x-obs-server-side-encryption-customer-key-MD5:4XvB3tbNTN+tIEVa0/fGaQ==** Constraint: This header is a Base64-encoded 128-bit MD5 value and must be used together with **x-obs-server-side-encryption-customer-algorithm** and **x-obs-server-side-encryption-customer-key**.	No. This header is required when SSE-C is used. The MD5 value must be the same as that used to initiate multipart upload tasks.

Header	Description	Mandatory
x-obs-copy-source-server-side-encryption-customer-algorithm	Indicates the algorithm for the source object when SSE-C is used. Type: string Example: **x-obs-copy-source-server-side-encryption-customer-algorithm:AES256** Constraint: This header must be used together with **x-obs-copy-source-server-side-encryption-customer-key** and **x-obs-copy-source-server-side-encryption-customer-key-MD5**.	No. This header is required when SSE-C is used to copy a source object.
x-obs-copy-source-server-side-encryption-customer-key	Indicates the key for decrypting the source object when SSE-C is used. Type: string Example: **x-obs-copy-source-server-side-encryption-customer-key:K7QkYpBkM5+hca27fsNkUnNVaobncnLht/rCB2o/9Cw=** Constraint: This header is a Base64-encoded 256-bit key and must be used together with **x-obs-copy-source-server-side-encryption-customer-algorithm** and **x-obs-copy-source-server-side-encryption-customer-key-MD5**.	No. This header is required when SSE-C is used to copy a source object.

Header	Description	Mandatory
x-obs-copy-source-server-side-encryption-customer-key-MD5	Indicates the MD5 value of the key for the source object when SSE-C is used. The MD5 value is used to check whether any error occurs during the transmission of the key. Type: string Example: **x-obs-copy-source-server-side-encryption-customer-key-MD5:4XvB3tbNTN+tIEVa0/fGaQ==** Constraint: This header is a Base64-encoded 128-bit MD5 value and must be used together with **x-obs-copy-source-server-side-encryption-customer-algorithm** and **x-obs-copy-source-server-side-encryption-customer-key**.	No. This header is required when SSE-C is used to copy a source object.
x-obs-copy-source-if-match	Indicates that the source object is copied only if its ETag matches the one specified in this header. Otherwise, a 412 status code (failed precondition) is returned. Type: string Example: **x-obs-copy-source-if-match: etag** Constraint: This header can be used with **x-obs-copy-source-if-unmodified-since** but not other conditional copy headers.	No

Header	Description	Mandatory
x-obs-copy-source-if-none-match	Indicates that the source object is copied only if its ETag does not match the one specified in this header. Otherwise, a 412 status code (failed precondition) is returned. Type: string Example: **x-obs-copy-source-if-none-match: etag** Constraint: This header can be used with **x-obs-copy-source-if-modified-since** but not other conditional copy headers.	No

Header	Description	Mandatory
x-obs-copy-source-if-unmodified-since	Indicates that the source object is copied only if it has not been modified since the time specified by this header. Otherwise, a 412 status code (failed precondition) is returned. This header can be used with **x-obs-copy-source-if-match** but not other conditional copy headers. Type: string Format: HTTP time string complying with the format specified at **http://www.ietf.org/rfc/rfc2616.txt**, which can be any of the following: 1. **EEE, dd MMM yyyy HH:mm:ss z** 2. **EEEE, dd-MMM-yy HH:mm:ss z** 3. **EEE MMM dd HH:mm:ss yyyy** Examples: 1. **x-obs-copy-source-if-unmodified-since: Sun, 06 Nov 1994 08:49:37 GMT** 2. **x-obs-copy-source-if-unmodified-since: Sunday, 06-Nov-94 08:49:37 GMT** 3. **x-obs-copy-source-if-unmodified-since: Sun Nov 6 08:49:37 1994** Constraint: The time specified by this header cannot be later than the current server time (GMT time), or this header does not take effect.	No

Header	Description	Mandatory
x-obs-copy-source-if-modified-since	Indicates that the source object is copied only if it has been modified since the time specified by this header. Otherwise, a 412 status code (failed precondition) is returned. This header can be used with **x-obs-copy-source-if-none-match** but not other conditional copy headers. Type: string Format: HTTP time string complying with the format specified at **http://www.ietf.org/rfc/rfc2616.txt**, which can be any of the following: 1. **EEE, dd MMM yyyy HH:mm:ss z** 2. **EEEE, dd-MMM-yy HH:mm:ss z** 3. **EEE MMM dd HH:mm:ss yyyy** Examples: 1. **x-obs-copy-source-if-unmodified-since: Sun, 06 Nov 1994 08:49:37 GMT** 2. **x-obs-copy-source-if-unmodified-since: Sunday, 06-Nov-94 08:49:37 GMT** 3. **x-obs-copy-source-if-unmodified-since: Sun Nov 6 08:49:37 1994** Constraint: The time specified by this header cannot be later than the current server time (GMT time), or this header does not take effect.	No

Request Elements

This request involves no elements.

Response Syntax

```
HTTP/1.1 status_code
Date: date

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<CopyPartResult xmlns="http://obs.region.example.com/doc/2015-06-30/">
   <LastModified>modifiedDate</LastModified>
   <ETag>etag</ETag>
</CopyPartResult>
```

Response Headers

The response to the request uses common headers. For details, see **Table 3-19**.

Table 5-102 Additional response headers

Header	Description
x-obs-server-side-encryption	This header is included in a response if SSE-KMS is used. Type: string Example: **x-obs-server-side-encryption:kms**
x-obs-server-side-encryption-kms-key-id	Indicates the master key ID. This header is included in a response when SSE-KMS is used. Type: string Format: *regionID*:*domainID*:**key/***key_id* *regionID* indicates the ID of the region where the key belongs. *domainID* indicates the ID of the tenant where the key belongs. *key_id* indicates the key ID used in this encryption. Example: **x-obs-server-side-encryption-kms-key-id:*region*:domainiddomainiddomai-niddoma0001:key/4f1cd4de-ab64-4807-920a-47fc42e7f0d0**
x-obs-server-side-encryption-customer-algorithm	Indicates the encryption algorithm. This header is included in a response when SSE-C is used. Type: string Example: **x-obs-server-side-encryption-customer-algorithm:AES256**

Header	Description
x-obs-server-side-encryption-customer-key-MD5	Indicates the MD5 value of the key for encrypting objects. This header is included in a response when SSE-C is used. Type: string Example: **x-obs-server-side-encryption-customer-key-MD5:4XvB3tbNTN+tIEVa0/fGaQ==**

Response Elements

This response contains elements of a part copy result. **Table 5-103** describes the elements.

Table 5-103 Response elements

Element	Description
LastModified	Indicates the latest time an object was modified. Type: string
ETag	ETag value of the target part. It is the unique identifier of the part content and is used to verify data consistency when merging parts. Type: string

Error Responses

1. If the AK or signature is invalid, OBS returns **403 Forbidden** and the error code is **AccessDenied**.
2. Check whether the source bucket or destination bucket exists. If the source bucket or destination bucket does not exist, OBS returns **404 Not Found** and the error code is **NoSuchBucket**.
3. If the source object does not exist, OBS returns **404 Not Found** and the error code is **NoSuchKey**.
4. If the user does not have the read permission for the specified object, OBS returns **403 Forbidden** and the error code is **AccessDenied**.
5. If the user does not have the write permission for the destination bucket, OBS returns **403 Forbidden** and the error code is **AccessDenied**.
6. If the specified task does not exist, OBS returns **404 Not Found** and the error code is **NoSuchUpload**.
7. If the user is not the initiator of the multipart upload task, OBS returns **403 Forbidden** and the error code is **AccessDenied**.
8. When the size of a copied part has exceeded 5 GB, OBS returns **400 Bad Request**.

9. If a part number is not within the range from 1 to 10000, OBS returns error code **400 Bad Request**.

Other errors are included in **Table 6-2**.

Sample Request

```
PUT /tobject02?partNumber=2&uploadId=00000163D40171ED8DF4050919BD02B8 HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
Date: WED, 01 Jul 2015 05:16:32 GMT
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:dSnpnNpawDSsLg/xXxaqFzrAmMw=
x-obs-copy-source: /destbucket/object01
```

Sample Response

```
HTTP/1.1 200 OK
Server: OBS
x-obs-request-id: 8DF400000163D40ABBD20405D30B0542
x-obs-id-2: 32AAAQAAEAABAAAQAAEAABAAAQAAEAABCTIJpD2efLy5o8sTTComwBb2He0j11Ne
Content-Type: application/xml
Date: WED, 01 Jul 2015 05:16:32 GMT
Transfer-Encoding: chunked

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<CopyPartResult xmlns="http://obs.example.com/doc/2015-06-30/">
  <LastModified>2015-07-01T05:16:32.344Z</LastModified>
  <ETag>"3b46eaf02d3b6b1206078bb86a7b7013"</ETag>
</CopyPartResult>
```

5.5.5 Listing Uploaded Parts

Functions

You can perform this operation to query all parts associated to a multipart upload. The size of each part listed by this API is the same as the size of the part uploaded.

Request Syntax

```
GET /ObjectName?uploadId=uploadid&max-parts=max&part-number-marker=marker HTTP/1.1
Host: bucketname.obs.region.example.com
Date: date
Authorization: auth
```

Request Parameters

This request uses parameters to specify which parts in a multipart upload will be listed. **Table 5-104** describes the parameters.

Table 5-104 Request parameters

Parameter	Description	Mandatory
uploadId	ID of the multipart upload Type: string Default value: none	Yes

Parameter	Description	Mandatory
max-parts	Maximum number of parts that can be listed Type: integer Default value: **1,000**	No
part-number -marker	Part after which the part listing begins. OBS lists only parts with greater numbers than that specified by this parameter. Type: integer Default value: none	No

Request Headers

This request uses common headers. For details, see **Table 3-3**.

Request Elements

This request involves no elements.

Response Syntax

```
HTTP/1.1 status_code
Date: date
Content-Length: length

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ListPartsResult xmlns="http://obs.region.example.com/doc/2015-06-30/">
   <Bucket>BucketName</Bucket>
   <Key>object</Key>
   <UploadId>uploadid</UploadId>
   <Initiator>
      <ID>id</ID>
   </Initiator>
   <Owner>
      <ID>ownerid</ID>
   </Owner>
   <StorageClass>storageclass</StorageClass>
   <PartNumberMarker>partNmebermarker</PartNumberMarker>
   <NextPartNumberMarker>nextPartnumberMarker</NextPartNumberMarker>
   <MaxParts>maxParts</MaxParts>
   <IsTruncated>true</IsTruncated>
   <Part>
      <PartNumber>partNumber</PartNumber>
      <LastModified>modifiedDate</LastModified>
      <ETag>etag</ETag>
      <Size>size</Size>
   </Part>
</ListPartsResult>
```

Response Headers

The response to the request uses common headers. For details, see **Table 3-19**.

Response Elements

This response uses elements to return information about uploaded parts. **Table 5-105** describes the elements.

Table 5-105 Response elements

Element	Description
ListPartsResult	Container for responses to part listing requests Type: container Child: Bucket, Key, UploadId, PartNumberMarker, NextPartNumberMarker, MaxParts, IsTruncated, and Part Parent: none
Bucket	Name of the bucket Type: string Parent: ListPartsResult
Key	Object name Type: string Parent: ListPartsResult
UploadId	ID of the multipart upload Type: string Parent: ListPartsResult
Initiator	Initiator of the multipart upload Type: container Child: ID Parent: ListPartsResult
Owner	The value of this parameter is the same as that of **Initiator**. Type: container Child: ID Parent: ListPartsResult
ID	ID of the domain where the owner belongs Type: string Parent: Initiator or Owner
StorageClass	Storage class Type: string Value options: **STANDARD**, **WARM**, **COLD** Parent: ListPartsResult

Element	Description
PartNumberMarker	Part number after which listing parts begins Type: integer Parent: ListPartsResult
NextPartNumberMarker	Value of **PartNumberMarker** in the next request when the returned result is incomplete Type: integer Parent: ListPartsResult
MaxParts	Maximum number of parts returned in a response Type: integer Parent: ListPartsResult
IsTruncated	Whether the returned part list is truncated. The value **true** indicates that the list was truncated and **false** indicates that the list was not truncated. Type: boolean Parent: ListPartsResult
Part	Container for elements related to a particular part. Type: string Child: PartNumber, LastModified, ETag, and Size Parent: ListPartsResult **PartNumber** identifies a part.
PartNumber	Number of an uploaded part Type: integer Parent: ListPartsResult.Part
LastModified	When a part was uploaded Type: date Parent: ListPartsResult.Part
ETag	ETag value of the uploaded parts. It is the unique identifier of the part content and is used to verify data consistency during the combination of parts. Type: string Parent: ListPartsResult.Part
Size	Size of an uploaded part Type: integer Parent: ListPartsResult.Part

Error Responses

1. If the AK or signature is invalid, OBS returns **403 Forbidden** and the error code is **AccessDenied**.
2. If the requested bucket is not found, OBS returns **404 Not Found** and the error code is **NoSuchBucket**.
3. If the requested multipart upload task does not exist, OBS returns **404 Not Found** and the error code is **NoSuchUpload**.
4. OBS determines whether the use's domain ID has the read permission for the specified bucket. If the user does not have the permission, OBS returns **403 Forbidden** and the error code is **AccessDenied**.

Other errors are included in **Table 6-2**.

Sample Request

```
GET /object02?uploadId=00000163D40171ED8DF4050919BD02B8 HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
Date: WED, 01 Jul 2015 05:20:35 GMT
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:xkABdSrBPrz5yqzuZdJnK5oL/yU=
```

Sample Response

```
HTTP/1.1 200 OK
Server: OBS
x-obs-request-id: 8DF400000163D40C099A04EF4DD1BDD9
x-obs-id-2: 32AAAQAAEAABAAAQAAEAABAAAQAAEAABCSK71fr+hDnzB0JBvQC1B9+S12AWxC41
Content-Type: application/xml
Date: WED, 01 Jul 2015 05:20:35 GMT
Content-Length: 888

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ListPartsResult xmlns="http://obs.example.com/doc/2015-06-30/">
  <Bucket>test333</Bucket>
  <Key>obj2</Key>
  <UploadId>00000163D40171ED8DF4050919BD02B8</UploadId>
  <Initiator>
    <ID>domainID/domainiddomainiddomainiddo000008:userID/useriduseriduseriduseridus000008</ID>
  </Initiator>
  <Owner>
    <ID>domainiddomainiddomainiddo000008</ID>
  </Owner>
  <StorageClass>STANDARD</StorageClass>
  <PartNumberMarker>0</PartNumberMarker>
  <NextPartNumberMarker>2</NextPartNumberMarker>
  <MaxParts>1000</MaxParts>
  <IsTruncated>false</IsTruncated>
  <Part>
    <PartNumber>1</PartNumber>
    <LastModified>2018-06-06T07:39:32.522Z</LastModified>
    <ETag>"b026324c6904b2a9cb4b88d6d61c81d1"</ETag>
    <Size>2058462721</Size>
  </Part>
  <Part>
    <PartNumber>2</PartNumber>
    <LastModified>2018-06-06T07:41:03.344Z</LastModified>
    <ETag>"3b46eaf02d3b6b1206078bb86a7b7013"</ETag>
    <Size>4572</Size>
  </Part>
</ListPartsResult>
```


5.5.6 Completing a Multipart Upload

Functions

After uploading all parts for a multipart upload, you can use this operation to complete the multipart upload. Before performing this operation, you cannot download the uploaded data. When merging parts, you need to copy the additional message header information recorded during the initialization of the multipart upload task to the object metadata. The processing process is the same as that of the common upload object with these message headers. In the case of merging parts concurrently, the Last Write Win policy must be followed but the time for initiating Last Write is specified as the time when a part multipart upload is initiated.

If a multipart upload has not been aborted, the uploaded parts occupy your storage quota. After all parts in the multipart upload are merged to an object, only the object occupies your storage quota. If a part uploaded in a multipart upload is not used in any merging parts multipart uploads, the part will be deleted to release storage quota.

You can send a request for downloading all or some data of the generated multipart by specifying a range.

You can send a request for deleting all parts uploaded in a multipart upload. Deleted data cannot be restored.

The merged parts do not use the MD5 value of entire object as the ETag. Their ETag is calculated as follows: $MD5(M_1M_2...M_N)$-*N*, where M_n is the MD5 value of part *n* (*N* is the total number of parts). As described in the **Sample Request**, there are three parts and each part has an MD5 value. The MD5 values of the three parts are recalculated to obtain a new MD5 value. Then -*N* is added to the right of the MD5 value to get the ETag of the combined parts. In this example, -*N* is **-3**.

If the response to an object merge request times out and error 500 or 503 is returned, you can first obtain the object metadata of the multipart upload task. Then, check whether the value of header **x-obs-uploadId** in the response is the same as the ID of this multipart upload task. If they are the same, object parts have been successfully merged on the server and you do not need to try again. For details, see **Consistency of Concurrent Operations**.

Versioning

If a bucket has versioning enabled, a unique version ID is generated for an object created from a multipart upload in this bucket and the version ID is returned in response header **x-obs-version-id**. If versioning is suspended for a bucket, the object version obtained after the merge is **null**. For details about the versioning statuses of a bucket, see **Configuring Versioning for a Bucket**.

NOTICE

If 10 parts are uploaded but only nine parts are selected for merge, the parts that are not merged will be automatically deleted by the system. The parts that are not merged cannot be restored after being deleted. Before combining the parts, adopt the interface used to list the parts that have been uploaded to check all parts to ensure that no part is missed.

Request Syntax

```
POST /ObjectName?uploadId=uploadID HTTP/1.1
Host: bucketname.obs.region.example.com
Date: date
Content-Length: length
Authorization: authorization
<CompleteMultipartUpload>
   <Part>
      <PartNumber>partNum</PartNumber>
      <ETag>etag</ETag>
   </Part>
   <Part>
      <PartNumber>partNum</PartNumber>
      <ETag>etag</ETag>
   </Part>
   <Part>
      <PartNumber>partNum</PartNumber>
      <ETag>etag</ETag>
   </Part>
</CompleteMultipartUpload>
```

Request Parameters

This request uses parameters to specify the ID of a multipart upload whose parts will be merged. **Table 5-106** describes the parameters.

Table 5-106 Request parameters

Parameter	Description	Mandatory
uploadId	Indicates a multipart upload. Type: string	Yes

Request Headers

This request uses common headers. For details, see **Table 3-3**.

Request Elements

This request uses elements to specify the list of parts to be merged. **Table 5-107** describes the elements.

Table 5-107 Request Elements

Element	Description	Mandatory
CompleteMultipartUpload	List of parts to be combined Type: XML	Yes
PartNumber	Part number Type: integer	Yes
ETag	ETag value returned upon successful upload of a part. It is the unique identifier of the part content. This parameter is used to verify data consistency when parts are merged. Type: string	Yes

Response Syntax

```
HTTP/1.1 status_code
Date: date
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<CompleteMultipartUploadResult xmlns="http://obs.region.example.com/doc/2015-06-30/">
   <Location>http://example-Bucket.obs.region.example.com/example-Object</Location>
   <Bucket>bucketname</Bucket>
   <Key>ObjectName</Key>
   <ETag>ETag</ETag>
</CompleteMultipartUploadResult>
```

Response Headers

The response to the request uses common headers. For details, see **Table 3-19**.

In addition to the common response headers, the message headers listed in **Table 5-108** may be used.

Table 5-108 Additional response headers

Header	Description
x-obs-version-id	Version of the object after parts being merged. Type: string
x-obs-server-side-encryption	This header is included in a response if SSE-KMS is used. Type: string Example: **x-obs-server-side-encryption:kms**

Header	Description
x-obs-server-side-encryption-kms-key-id	Indicates the master key ID. This header is included in a response if SSE-KMS is used. Type: string Format: *regionID*:*domainID*:**key/***key_id* *regionID* indicates the ID of the region where the key belongs. *domainID* indicates the ID of the tenant where the key belongs. *key_id* indicates the key ID used in this encryption. Example: **x-obs-server-side-encryption-kms-key-id:*region*:domainiddomainiddomainid-doma0001:key/4f1cd4de-ab64-4807-920a-47fc42e7f0d0**
x-obs-server-side-encryption-customer-algorithm	Indicates an encryption algorithm. This header is included in a response if SSE-C is used. Type: string Example: **x-obs-server-side-encryption-customer-algorithm:AES256**

Response Elements

This response uses elements to return the result of merging parts. **Table 5-109** describes the elements.

Table 5-109 Response elements

Element	Description
Location	Path of the object after parts have been merged. Type: string
Bucket	Bucket in which parts are merged. Type: string
Key	Indicates the key of the generated object. Type: string
ETag	The result calculated based on the ETag of each part is the unique identifier of the object content. Type: string

Error Responses

1. If no message body exists, OBS returns **400 Bad Request**.
2. If the message body format is incorrect, OBS returns **400 Bad Request**.

3. If the part information in the message body is not sorted by part sequence number, OBS returns **400 Bad Request** and the error code is **InvalidPartOrder**.
4. If the AK or signature is invalid, OBS returns **403 Forbidden** and the error code is **AccessDenied**.
5. If the requested bucket is not found, OBS returns **404 Not Found** and the error code is **NoSuchBucket**.
6. If the requested multipart upload does not exist, OBS returns **404 Not Found** and error code **NoSuchUpload**.
7. If the user is not the initiator of the task, OBS returns **403 Forbidden** and the error code is **AccessDenied**.
8. If the request part list contains a part that does not exist, OBS returns **400 Bad Request** and the error code is **InvalidPart**.
9. If the part's ETag contained in the request list is incorrect, OBS returns **400 Bad Request** with an error code of **InvalidPart**.
10. If the size of a part other than the last part is smaller than 100 KB, OBS returns **400 Bad Request**.
11. If the size of the object is greater than 48.8 TB after parts being merged, OBS returns status code **400 Bad Request**.

Other errors are included in **Table 6-2**.

Sample Request

```
POST /object02?uploadId=00000163D46218698DF407362295674C HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
Date: WED, 01 Jul 2015 05:23:46 GMT
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:dOfK9iILcKxo58tRp3fWeDoYzKA=
Content-Length: 422

<?xml version="1.0" encoding="utf-8"?>
<CompleteMultipartUpload>
  <Part>
    <PartNumber>1</PartNumber>
    <ETag>a54357aff0632cce46d942af68356b38</ETag>
  </Part>
  <Part>
    <PartNumber>2</PartNumber>
    <ETag>0c78aef83f66abc1fa1e8477f296d394</ETag>
  </Part>
  <Part>
    <PartNumber>3</PartNumber>
    <ETag>acbd18db4cc2f85cedef654fccc4a4d8</ETag>
  </Part>
</CompleteMultipartUpload>
```

Sample Response

```
HTTP/1.1 200 OK
Server: OBS
x-obs-request-id: 8DF400000163D4625BE3075019BD02B8
x-obs-id-2: 32AAAQAAEAABAAAQAAEAABAAAQAAEAABCSN8D1AfQcIvyGBZ9+Ee+jU6zv1iYdO4
Content-Type: application/xml
Date: WED, 01 Jul 2015 05:23:46 GMT
Content-Length: 326

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
```



```
<CompleteMultipartUploadResult xmlns="http://obs.example.com/doc/2015-06-30/">
  <Location>/examplebucket/object02</Location>
  <Bucket>examplebucket</Bucket>
  <Key>object02</Key>
  <ETag>"03f814825e5a691489b947a2e120b2d3-3"</ETag>
</CompleteMultipartUploadResult>
```

5.5.7 Canceling a Multipart Upload Task

Functions

You can perform this operation to abort a multipart upload. You cannot upload or list parts after operations to merge parts or abort a multipart upload are performed.

Request Syntax

```
DELETE /ObjectName?uploadId=uplaodID HTTP/1.1
Host: bucketname.obs.region.example.com
Date: date
Authorization: auth
```

Request Parameters

This request uses message parameters to specify the multipart upload task number of the segment task. **Table 5-110** describes the parameters.

Table 5-110 Request parameters

Parameter	Description	Mandatory
uploadId	Indicates a multipart upload. Type: string	Yes

Request Headers

This request uses common headers. For details, see **Table 3-3**.

Request Elements

This request involves no elements.

Response Syntax

```
HTTP/1.1 status_code
Date: date
```

Response Headers

The response to the request uses common headers. For details, see **Table 3-19**.

Response Elements

This response contains no elements.

Error Responses

1. If the AK or signature is invalid, OBS returns **403 Forbidden** and the error code is **AccessDenied**.
2. If the requested bucket is not found, OBS returns **404 Not Found** and the error code is **NoSuchBucket**.
3. If you are neither the initiator of a multipart upload nor the bucket owner, OBS returns **403 Forbidden**.
4. If the operation is successful, OBS returns **204 No Content** to the user.

Other errors are included in **Table 6-2**.

Sample Request

```
DELETE /object02?uploadId=00000163D46218698DF407362295674C HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
Date: WED, 01 Jul 2015 05:28:27 GMT
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:QmM2d1DBXZ/b8drqtEv1QJHPbM0=
```

Sample Response

```
HTTP/1.1 204 No Content
Server: OBS
x-obs-request-id: 8DF400000163D463E02A07EC2295674C
x-obs-id-2: 32AAAQAAEAABAAAQAAEAABAAAQAAEAABCTp5YDlzn0UgqG3laRfkHLGyz7RpR9ON
Date: WED, 01 Jul 2015 05:28:27 GMT
```

5.6 Server-Side Encryption

5.6.1 Server-Side Encryption Overview

You can configure server-side encryption for objects, so that they will be encrypted or decrypted when you upload them to or download them from a bucket.

The encryption and decryption happen on the server side.

The encryption methods provided include SSE-KMS and SSE-C. All of them use the AES-256 algorithm.

With SSE-KMS, OBS uses the keys provided by KMS for server-side encryption. You can create custom keys on KMS to encrypt your objects.

With SSE-C, OBS uses the keys and MD5 values provided by customers for server-side encryption.

When server-side encryption is used, the returned ETag value is not the object's MD5 value.

5.6.2 SSE-KMS

Functions

With SSE-KMS, OBS uses the keys provided by Key Management Service (KMS) for server-side encryption. You can create custom keys on KMS to encrypt your

objects. If you do not specify a key, OBS creates a default key the first time you upload an object to the bucket. Custom keys or default keys are used to encrypt and decrypt data encryption keys (DEKs).

NOTE

When a custom KMS key in a non-default IAM project is used to encrypt objects, only the key owner can upload or download the encrypted objects.

When the default KMS key in a region is used to encrypt an object, this default key belongs to the object owner. Only the key owner (also the object owner) can upload or download this object.

Newly Added Headers

Two headers are added for SSE-KMS. You can configure the headers listed in **Table 5-111** to enable SSE-KMS.

You can also configure the default encryption for a bucket to encrypt objects you upload to the bucket. After default encryption is enabled for a bucket, any object upload request without encryption header included will inherit the bucket's encryption settings. For details, see **Configuring Bucket Encryption**.

Table 5-111 Header fields used in SSE-KMS mode

Element	Description
x-obs-server-side-encryption	Indicates that SSE-KMS is used for encrypting objects. Type: string Example: **x-obs-server-side-encryption:kms**

Element	Description
x-obs-server-side-encryption-kms-key-id	Indicates the master key for encrypting the object when SSE-KMS is used. If this header is not provided, the default master key will be used. If there is no such a default master key, OBS will create one and use it by default. Type: string The following two formats are supported: - *regionID*:*domainID*:**key/***key_id* - *key_id* *regionID* indicates the ID of the region where the key belongs. *domainID* indicates the ID of the tenant where the key belongs. *key_id* indicates the ID of the key created in KMS. Examples: - **x-obs-server-side-encryption-kms-key-id:***region***:domainiddomainiddo-mainiddoma0001:key/4f1cd4de-ab64-4807-920a-47fc42e7f0d0** - **x-obs-server-side-encryption-kms-key-id:4f1cd4de-ab64-4807-920a-47fc42e7f0d0**

APIs Where SSE-KMS Headers Apply

You can configure headers about SSE-KMS in the APIs below:

- **Uploading Objects - PUT**
- **Uploading Objects - POST**: **x-obs-server-side-encryption** and **x-obs-server-side-encryption-kms-key-id** need to be placed in the form instead of headers.
- **Copying Objects** (The newly added headers apply to object copies.)
- **Initiating a Multipart Upload**

You can configure a bucket policy to restrict the request headers for a specified bucket. For example, if you require that object upload requests do not contain header **x-obs-server-side-encryption:"kms"**, you can use the following bucket policy:

```
{
   "Statement": [
      {
         "Sid": "DenyUnEncryptedObjectUploads",
         "Effect": "Deny",
         "Principal": "*",
         "Action": "PutObject",
         "Resource": "YourBucket/*",
```



```
        "Condition": {
            "StringNotEquals": {
                "x-obs-server-side-encryption": "kms"
            }
        }
    }
  ]
}
```

Sample Request: Using the Default Key to Encrypt an Object

```
PUT /encryp1 HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
Date: Wed, 06 Jun 2018 09:08:21 GMT
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:f3/7eS6MFbW3JO4+7I5AtyAQENU=
x-obs-server-side-encryption:kms
Content-Length: 5242
Expect: 100-continue

[5242 Byte object contents]
```

Sample Response: Using the Default Key to Encrypt an Object

```
HTTP/1.1 200 OK
Server: OBS
x-obs-request-id: 8DF400000163D45AA81D038B6AE4C482
ETag: "d8bffdfbab5345d91ac05141789d2477"
x-obs-server-side-encryption: kms
x-obs-server-side-encryption-kms-key-id: region:783fc6652cf246c096ea836694f71855:key/
522d6070-5ad3-4765-9737-9312ddc72cdb
x-obs-id-2: 32AAAUJAIAABAAAQAAEAABAAAQAAEAABCTv7cHmAnGfBAGXUHeibUsiETTNqlCqC
Date: Wed, 06 Jun 2018 09:08:21 GMT
Content-Length: 0
```

Sample Request: Using a Custom Key to Encrypt an Object

```
PUT /encryp1 HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
Date: Wed, 06 Jun 2018 09:08:50 GMT
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:f3/PWjkXYTYGs5lPOctTNEI2QENU=
x-obs-server-side-encryption:kms
x-obs-server-side-encryption-kms-key-id: 522d6070-5ad3-4765-43a7-a7d1-ab21f498482d
Content-Length: 5242
Expect: 100-continue

[5242 Byte object contents]
```

Sample Response: Using a Custom Key to Encrypt an Object

```
HTTP/1.1 200 OK
Server: OBS
x-obs-request-id: 8DF400000163D45AA81D038B6AE4C482
ETag: "d8bffdfbab5345d91ac05141789d2477"
x-obs-server-side-encryption: kms
x-obs-server-side-encryption-kms-key-id: region:783fc6652cf246c096ea836694f71855:key/
522d6070-5ad3-4765-43a7-a7d1-ab21f498482d
x-obs-id-2: 32AAAUJAIAABAdiAEAABA09AEAABCTv7cHmAn12BAG83ibUsiET5eqlCqg
Date: Wed, 06 Jun 2018 09:08:50 GMT
Content-Length: 0
```

Sample Request: Using a Key to Encrypt an Object Copy

```
PUT /destobject HTTP/1.1
User-Agent: curl/7.29.0
```



```
Host: examplebucket.obs.region.example.com
x-obs-server-side-encryption:kms
x-obs-server-side-encryption-kms-key-id: region:783fc6652cf246c096ea836694f71855:key/
522d6070-5ad3-4765-9737-9312ddc72cdb
Accept: */*
Date: Wed, 06 Jun 2018 09:10:29 GMT
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:SH3uTrElaGWarVI1uTq325kTVCI=
x-obs-copy-source: /bucket/srcobject1
```

Sample Response: Using a Key to Encrypt an Object Copy

```
HTTP/1.1 200 OK
Server: OBS
x-obs-request-id: BB78000001648480AF3900CED7F15155
ETag: "d8bffdfbab5345d91ac05141789d2477"
x-obs-server-side-encryption: kms
x-obs-server-side-encryption-kms-key-id: region:783fc6652cf246c096ea836694f71855:key/
522d6070-5ad3-4765-9737-9312ddc72cdb
x-obs-id-2: oRAXhgwdaLc9wKVHqTLSmQB7I35D+32AAAUJAIAABAAAQAAEAABAAAQAAEAABCS
Date: Wed, 06 Jun 2018 09:10:29 GMT
Content-Length: 0
```

Sample Request: Uploading an Encrypted Object Using a Signed URL

```
PUT /destobject?AccessKeyId=UI3SN1SRUQE14OYBKTZB&Expires=1534152518&x-obs-server-side-
encryption=kms&Signature=chvmG7%2FDA%2FDCQmTRJu3xngldJpg%3D HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
Date: Wed, 06 Jun 2018 09:10:29 GMT
```

Sample Response: Uploading an Encrypted Object Using a Signed URL

```
HTTP/1.1 200 OK
Server: OBS
x-obs-request-id: BB78000001648480AF3900CED7F15155
ETag: "d8bffdfbab5345d91ac05141789d2477"
x-obs-server-side-encryption: kms
x-obs-server-side-encryption-kms-key-id: region:783fc6652cf246c096ea836694f71855:key/
522d6070-5ad3-4765-9737-9312ddc72cdb
x-obs-id-2: oRAXhgwdaLc9wKVHqTLSmQB7I35D+32AAAUJAIAABAAAQAAEAABAAAQAAEAABCS
Date: Wed, 06 Jun 2018 09:10:29 GMT
Content-Length: 0
```

5.6.3 SSE-C

Functions

With SSE-C used, OBS uses the keys and MD5 values provided by customers for server-side encryption.

Newly Added Headers

OBS does not store your encryption keys. If you lost them, you lost the objects. Six headers are added to support SSE-C.

The following table lists headers that are required when you use SSE-C to encrypt objects.

Table 5-112 Header fields used for encrypting objects in SSE-C mode

Element	Description
x-obs-server-side-encryption-customer-algorithm	Indicates the encryption algorithm for the object when SSE-C is used. Example: **x-obs-server-side-encryption-customer-algorithm: AES256**
x-obs-server-side-encryption-customer-key	Indicates the key for encrypting objects when SSE-C is used. Its value is a Base64-encoded 256-bit key. Example: **x-obs-server-side-encryption-customer-key:K7QkYpBkM5+hca27fsNkUnNVaobncnLht/rCB2o/9Cw=**
x-obs-server-side-encryption-customer-key-MD5	Indicates the MD5 value of the key for encrypting objects when SSE-C is used. Its value is a Base64-encoded MD5 hash. The MD5 value is used to check whether any error occurs during the transmission of the key. Example: **x-obs-server-side-encryption-customer-key-MD5:4XvB3tbNTN+tIEVa0/fGaQ==**

APIs where the newly added headers apply:

- **Uploading an Object - PUT**
- **Uploading an Object - POST**
- **Copying an Object**: The newly added headers apply to the object copy.
- **Querying Object Metadata**
- **Downloading an Object**
- **Initiating a Multipart Upload**
- **Uploading Parts**
- **Copying Parts**: The newly added headers apply to target parts.

The following table lists three headers that are added for CopyObject and UploadPart-Copy operations to support source objects encrypted using SSE-C.

Table 5-113 Header fields for source objects encrypted by the SSE-C

Element	Description
x-obs-copy-source-server-side-encryption-customer-algorithm	Indicates the algorithm for decrypting the source object when SSE-C is used. Example: **x-obs-server-side-encryption-customer-algorithm: AES256**
x-obs-copy-source-server-side-encryption-customer-key	Indicates the key for decrypting the source object when SSE-C is used. Example: **x-obs-copy-source-server-side-encryption-customer-algorithm: K7QkYpBkM5+hca27fsNkUnNVaobncnLht/rCB2o/9Cw=**
x-obs-copy-source-server-side-encryption-customer-key-MD5	Indicates the MD5 value of the key for decrypting the source object when SSE-C is used. The MD5 value is used to check whether any error occurs during the transmission of the key. Example: **x-obs-copy-source-server-side-encryption-customer-key:4XvB3tbNTN+tIEVa0/fGaQ==**

Sample Request: Uploading an Object Encrypted with SSE-C

```
PUT /encryp2 HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
Date: Wed, 06 Jun 2018 09:12:00 GMT
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:mZSfafoM+llApk0HGOThlqeccu0=
x-obs-server-side-encryption-customer-algorithm:AES256
x-obs-server-side-encryption-customer-key:K7QkYpBkM5+hca27fsNkUnNVaobncnLht/rCB2o/9Cw=
x-obs-server-side-encryption-customer-key-MD5:4XvB3tbNTN+tIEVa0/fGaQ==
Content-Length: 5242

[5242 Byte object contents]
```

Sample Response: Uploading an Object Encrypted with SSE-C

```
HTTP/1.1 200 OK
Server: OBS
x-obs-request-id: 8DF400000163D45E0017055619BD02B8
ETag: "0f91242c7f3d86f98ae572a686d0696e"
x-obs-server-side-encryption-customer-algorithm: AES256
x-obs-server-side-encryption-customer-key-MD5: 4XvB3tbNTN+tIEVa0/fGaQ==
x-obs-id-2: 32AAAUgAIAABAAAQAAEAABAAAQAAEAABCSSAJ8bTNJV0X+Ote1PtuWecqyMh6zBJ
Date: Wed, 06 Jun 2018 09:12:00 GMT
Content-Length: 0
```

Sample Request: Copying an SSE-C Encrypted Object and Saving It as a KMS Encrypted Object

```
PUT /kmsobject HTTP/1.1
User-Agent: curl/7.29.0
```



```
Host: examplebucket.obs.region.example.com
Accept: */*
Date: Wed, 06 Jun 2018 09:20:10 GMT
Authorization: OBS H4IPJX0TQTHTHEBQQCEC:mZSfafoM+llApk0HGOThlqeccu0=
x-obs-copy-source-server-side-encryption-customer-algorithm:AES256
x-obs-copy-source-server-side-encryption-customer-key:K7QkYpBkM5+hca27fsNkUnNVaobncnLht/rCB2o/
9Cw=
x-obs-copy-source-server-side-encryption-customer-key-MD5:4XvB3tbNTN+tIEVa0/fGaQ==
x-obs-server-side-encryption: kms
x-obs-copy-source: /examplebucket/encryp2
Content-Length: 5242

[5242 Byte object contents]
```

Sample Response: Copying an SSE-C Encrypted Object and Saving It as a KMS Encrypted Object

```
HTTP/1.1 200 OK
Server: OBS
x-obs-request-id: BB7800000164848E0FC70528B9D92C41
ETag: "1072e1b96b47d7ec859710068aa70d57"
x-obs-server-side-encryption: kms
x-obs-server-side-encryption-kms-key-id: region:783fc6652cf246c096ea836694f71855:key/
522d6070-5ad3-4765-9737-9312ddc72cdb
x-obs-id-2: 32AAAUJAIAABAAAQAAEAABAAAQAAEAABCTkkRzQXs9ECzZcavVRncBqqYNkoAEsr
Date: Wed, 06 Jun 2018 09:20:10 GMT
Content-Length: 0
```

Sample Request: Uploading an SSE-C Encrypted Object Using a Signed URL

```
PUT /encrypobject?
AccessKeyId=H4IPJX0TQTHTHEBQQCEC&Expires=1532688887&Signature=EQmDuOhaLUrzrzRNZxwS72CXeX
M%3D HTTP/1.1
User-Agent: curl/7.29.0
Host: examplebucket.obs.region.example.com
Accept: */*
x-obs-server-side-encryption-customer-algorithm: AES256
x-obs-server-side-encryption-customer-key:K7QkYpBkM5+hca27fsNkUnNVaobncnLht/rCB2o/9Cw=
x-obs-server-side-encryption-customer-key-MD5:4XvB3tbNTN+tIEVa0/fGaQ==
Content-Length: 5242
Expect: 100-continue

[5242 Byte object contents]
```

Sample Response: Uploading an SSE-C Encrypted Object Using a Signed URL

```
HTTP/1.1 100 Continue
HTTP/1.1 200 OK
Server: OBS
x-obs-request-id: 804F00000164DB5E5B7FB908D3BA8E00
ETag: "1072e1b96b47d7ec859710068aa70d57"
x-obs-server-side-encryption-customer-algorithm: AES256
x-obs-server-side-encryption-customer-key-MD5: 4XvB3tbNTN+tIEVa0/fGaQ==
x-obs-id-2: 32AAAUJAIAABAAAQAAEAABAAAQAAEAABCTlpxILjhVK/heKOWIP8Wn2IWmQoerfw
Content-Length: 0
```

5.6.4 API Operations Related to Server-Side Encryption

This section lists the operations related to server-side encryption and describes HTTP protocols applicable to the operations.

The following table describes the requirements on the transmission protocols used by the API operation related to server-side encryption.

Table 5-114 Requirements for the transmission protocol used by the operations related to the SSE-C

Operation	Transfer Protocol
PutObject	HTTPS
PostObject	HTTPS
InitiateMultipartUpload	HTTPS
HeadObject	HTTPS
GetObject	HTTPS
UploadPart	HTTPS
CompleteMultipartUpload	HTTP or HTTPS

Table 5-115 Requirements for the transfer protocol used by the operations related to the SSE-KMS

Operation	Transfer Protocol
PutObject	HTTPS
PostObject	HTTPS
InitiateMultipartUpload	HTTPS
HeadObject	HTTP or HTTPS
GetObject	HTTPS
UploadPart	HTTPS
CompleteMultipartUpload	HTTP or HTTPS

Table 5-116 Requirements for transfer protocol used by the CopyObject operation

Source Object	Target Object	Transfer Protocol
Non-encrypted object	Object encrypted using SSE-KMS	HTTPS
Object encrypted using SSE-KMS	Object encrypted using SSE-KMS	HTTPS
Object encrypted using SSE-C	Object encrypted using SSE-KMS	HTTPS
Non-encrypted object	Object encrypted using SSE-C	HTTPS

Source Object	Target Object	Transfer Protocol
Object encrypted using SSE-KMS	Object encrypted using SSE-C	HTTPS
Object encrypted using SSE-C	Object encrypted using SSE-C	HTTPS
Non-encrypted object	Non-encrypted object	HTTP or HTTPS
Object encrypted using SSE-KMS	Non-encrypted object	HTTP or HTTPS
Object encrypted using SSE-C	Non-encrypted object	HTTP or HTTPS

Table 5-117 Requirements for the transfer protocol used by the UploadPart-Copy operation

Source Object	Target Part	Transfer Protocol
Non-encrypted object	Part encrypted using SSE-KMS	HTTP or HTTPS
Object encrypted using SSE-KMS	Part encrypted using SSE-KMS	HTTP or HTTPS
Object encrypted using SSE-C	Part encrypted using SSE-KMS	HTTP or HTTPS
Non-encrypted object	Part encrypted using SSE-C	HTTPS
Object encrypted using SSE-KMS	Part encrypted using SSE-C	HTTPS
Object encrypted using SSE-C	Part encrypted using SSE-C	HTTPS
Non-encrypted object	Non-encrypted part	HTTP or HTTPS
Object encrypted using SSE-KMS	Non-encrypted part	HTTP or HTTPS
Object encrypted using SSE-C	Non-encrypted part	HTTP or HTTPS

6 Error Codes

If an API call fails, no result data is returned. You can locate the cause of the error according to the error code of each API. If an API call fails, HTTP status code 3*xx*, 4*xx* or 5*xx* is returned. The response body contains the specific error code and information.

Error Response Syntax

When an error occurs, the response header information contains:

- Content-Type: application/xml
- HTTP error status code 3*xx*, 4*xx*, or 5*xx*

The response body also contains information about the error. The following is an error response example that shows common elements in the Representational State Transfer (REST) error response body.

```
<?xml version="1.0" encoding="UTF-8"?>
<Error>
<Code>NoSuchKey</Code>
<Message>The resource you requested does not exist</Message>
<Resource>/example-bucket/object</Resource>
<RequestId>001B21A61C6C0000013402C4616D5285</RequestId>
<HostId>RkRCRDJENDc5MzdGQkQ4OUY3MTI4NTQ3NDk2Mjg0M0FB
QUFBQUFBYmJiYmJiYmJD</HostId>
</Error>
```

Table 6-1 describes the meaning of each element.

Table 6-1 Error response elements

Element	Description
Error	Root element that describes the error in an XML response body
Code	HTTP return code that corresponds to the error in the XML response body. For details about error codes, see **Table 6-2**.
Message	Details the error in the XML error response body. For details about error messages, see **Table 6-2**.

Element	Description
RequestId	ID of the request whose error response is returned. The ID is used for locating the error.
HostId	ID of the server that returns an error response
Resource	Bucket or object related to an error.

NOTE

Some error responses contain more detailed information. It is recommended that all error information be logged for easier rectification of errors.

Description

If OBS encounters an error when processing a request, a response containing the error code and description is returned. Table 6-2 describes the error codes of OBS.

Table 6-2 Error codes

Status Code	Error Code	Error Message	Solution
301 Moved Permanently	PermanentRedirect	The requested bucket can be accessed only through the specified address. Send subsequent requests to the address.	Send the request to the returned redirection address.
301 Moved Permanently	WebsiteRedirect	The website request lacks **bucketName**.	Put the bucket name in the request and try again.
307 Moved Temporarily	TemporaryRedirect	Temporary redirection. If the DNS is updated, the request is redirected to the bucket.	The system automatically redirects the request or sends the request to the redirection address.
400 Bad Request	BadDigest	The specified value of **Content-MD5** does not match the value received by OBS.	Check whether the MD5 value carried in the header is the same as that calculated by the message body.
400 Bad Request	BadDomainName	The domain name is invalid.	Use a valid domain name.
400 Bad Request	BadRequest	Invalid request parameters.	Modify the parameters according to the error details in the message body.

Status Code	Error Code	Error Message	Solution
400 Bad Request	CustomDomainAreadyExist	The configured domain already exists.	It has been configured and does not need to be configured again.
400 Bad Request	CustomDomainNotExist	Delete the domain that does not exist.	It is not configured or has been deleted. You do not need to delete it.
400 Bad Request	EntityTooLarge	• The size of the file uploaded using the PUT, POST, or Append methods of SDKs or APIs exceeds 5 GB. • The part uploaded is larger than 5 GB in size. • The size of the bucket configurations exceeds 20 KB. • The file size exceeds the upper limit defined in the policy of the POST form. • The size of the file uploaded using the multipart upload of SDKs or APIs or the resumable upload of SDKs exceeds 48.8 TB.	Modify the conditions specified in the upload policy or reduce the object size.
400 Bad Request	EntityTooSmall	• The part uploaded, except the last one, is smaller than 100 KB. • The file size is smaller than the lower limit defined in the policy of the POST form.	Modify the conditions specified in the upload policy or increase the object size.

Status Code	Error Code	Error Message	Solution
400 Bad Request	IllegalLocationConstraintException	A request without **Location** is sent for creating a bucket in a non-default region.	Send the bucket creation request to the default region, or send the request with the **Location** of the non-default region.
400 Bad Request	IncompleteBody	No complete request body is received due to network or other problems.	Upload the object again.
400 Bad Request	IncorrectNumberOfFilesInPost Request	Each POST request must contain one file to be uploaded.	Carry a file to be uploaded.
400 Bad Request	InvalidArgument	Invalid parameter.	Modify the parameter according to the error details in the message body.
400 Bad Request	InvalidBucket	The bucket to be accessed does not exist.	Change the bucket name.
400 Bad Request	InvalidBucketName	The bucket name specified in the request is invalid, which may have exceeded the maximum length, or contain special characters that are not allowed.	Change the bucket name.
400 Bad Request	InvalidContentLength	Invalid Content-Length value.	Check the encapsulation header or contact technical support.
400 Bad Request	InvalidDefaultStorageClass	The default storage class is invalid.	Check which storage classes can be used.
400 Bad Request	InvalidEncryptionAlgorithmError	Incorrect encryption algorithm. The object cannot be decrypted due to incorrect encryption header carried when downloading the SSE-C encrypted object.	Carry the correct encryption header when downloading the object.

Status Code	Error Code	Error Message	Solution
400 Bad Request	InvalidLocationConstraint	The specified **Location** in the bucket creation request is invalid or does not exist.	Correct the **Location** in the bucket creation request.
400 Bad Request	InvalidPart	One or more specified parts are not found. The parts may not be uploaded or the specified entity tags (ETags) do not match the parts' ETags.	Merge the parts correctly according to the ETags.
400 Bad Request	InvalidPartOrder	Parts are not listed in ascending order by part number.	Sort the parts in ascending order and merge them again.
400 Bad Request	InvalidPolicyDocument	The content of the form does not meet the conditions specified in the policy document.	Modify the policy in the constructed form according to the error details in the message body and try again.
400 Bad Request	InvalidRedirectLocation	Invalid redirect location.	Specifies the correct IP address.
400 Bad Request	InvalidRequest	Invalid request.	Modify the parameter according to the error details in the message body.
400 Bad Request	InvalidRequestBody	The request body is invalid. The request requires a message body but no message body is uploaded.	Upload the message body in the correct format.
400 Bad Request	InvalidTargetBucketForLogging	The delivery group has no ACL permission for the target bucket.	Configure the target bucket ACL and try again.
400 Bad Request	KeyTooLongError	The provided key is too long.	Use a shorter key.
400 Bad Request	KMS.DisabledException	The customer master key (CMK) is disabled in SSE-KMS mode.	Replace the key and try again, or contact technical support.

Status Code	Error Code	Error Message	Solution
400 Bad Request	KMS.NotFoundException	The customer master key (CMK) does not exist in SSE-KMS mode.	Retry with the correct CMK.
400 Bad Request	MalformedACLError	The provided XML file is in an incorrect format or does not meet format requirements.	Use the correct XML format to retry.
400 Bad Request	MalformedError	The XML format in the request is incorrect.	Use the correct XML format to retry.
400 Bad Request	MalformedLoggingStatus	The XML format of **Logging** is incorrect.	Use the correct XML format to retry.
400 Bad Request	MalformedPolicy	The bucket policy does not pass.	Modify the bucket policy according to the error details returned in the message body.
400 Bad Request	MalformedQuotaError	The Quota XML format is incorrect.	Use the correct XML format to retry.
400 Bad Request	MalformedXML	An XML file of a configuration item is in incorrect format.	Use the correct XML format to retry.
400 Bad Request	MaxMessageLengthExceeded	Copying an object does not require a message body in the request.	Remove the message body and retry.
400 Bad Request	MetadataTooLarge	The size of the metadata header has exceeded the upper limit.	Reduce the size of the metadata header.
400 Bad Request	MissingRegion	No region contained in the request and no default region defined in the system.	Carry the region information in the request.
400 Bad Request	MissingRequestBodyError	This error code is returned after you send an empty XML file.	Provide the correct XML file.
400 Bad Request	MissingRequiredHeader	Required headers are missing in the request.	Provide required headers.

Status Code	Error Code	Error Message	Solution
400 Bad Request	MissingSecurityHeader	A required header is not provided.	Provide required headers.
400 Bad Request	MultipleContentLengths	There are multiple Content-Length headers.	Check the encapsulation header or contact technical support.
400 Bad Request	TooManyBuckets	You have attempted to create more buckets than allowed.	Delete some buckets and try again.
400 Bad Request	TooManyCustomDomains	Too many user accounts are configured.	Delete some user accounts and try again.
400 Bad Request	TooManyWrongSignature	The request is rejected due to high-frequency errors.	Replace the Access Key and try again.
400 Bad Request	UnexpectedContent	The request requires a message body which is not carried by the client, or the request does not require a message body but the client carries the message body.	Try again according to the instruction.
400 Bad Request	UserKeyMustBeSpecified	This operation is available only to specific users.	Contact technical support.
403 Forbidden	AccessDenied	Access denied, because the request does not carry a date header or the header format is incorrect.	Provide a correct date header in the request.
403 Forbidden	AccessForbidden	Insufficient permission. No CORS configuration exists for the bucket or the CORS rule does not match.	Modify the CORS configuration of the bucket or send the matched OPTIONS request based on the CORS configuration of the bucket.
403 Forbidden	AllAccessDisabled	You have no permission to perform the operation. The bucket name is forbidden.	Change the bucket name.

Status Code	Error Code	Error Message	Solution
403 Forbidden	DeregisterUserId	The user has been deregistered.	Top up or re-register.
403 Forbidden	InArrearOrInsufficientBalance	The subscriber owes fees or the account balance is insufficient, and the subscriber does not have the permission to perform an operation.	Top up.
403 Forbidden	InsufficientStorageSpace	Insufficient storage space.	If the quota is exceeded, increase quota or delete some objects.
403 Forbidden	InvalidAccessKeyId	The access key ID provided by the customer does not exist in the system.	Provide correct access key Id.
403 Forbidden	InvalidObjectState	You need to restore Cold objects first before downloading them.	Restore the object first.
403 Forbidden	NotSignedUp	Your account has not been registered with the system. Only a registered account can be used.	Register OBS.
403 Forbidden	RequestTimeTooSkewed	There was a large time offset between the OBS server time and the time when the client initiated a request. 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.	Check whether there is a large time offset between the client time and server time. If there is, adjust the client time based on your local time (UTC) and try again.

Status Code	Error Code	Error Message	Solution
403 Forbidden	SignatureDoesNotMatch	The provided signature does not match the signature calculated by OBS.	Check your secret access key and signature algorithm.
403 Forbidden	VirtualHostDomainRequired	Virtual hosting access domain name is not used.	Use the virtual hosting access domain name. For details, see **Constructing a Request**.
403 Forbidden	Unauthorized	The user has not been authenticated in real name.	Authenticate the user's real name and try again.
404 Not Found	NoSuchBucket	The specified bucket does not exist.	Create a bucket and perform the operation again.
404 Not Found	NoSuchBucketPolicy	No bucket policy exists.	Configure a bucket policy.
404 Not Found	NoSuchCORSConfiguration	No CORS configuration exists.	Configure CORS first.
404 Not Found	NoSuchCustomDomain	The requested user account does not exist.	Set a user account first.
404 Not Found	NoSuchKey	The specified key does not exist.	Upload the object first.
404 Not Found	NoSuchLifecycleConfiguration	The requested lifecycle rule does not exist.	Configure a lifecycle rule first.
404 Not Found	NoSuchUpload	The specified multipart upload does not exist. The upload ID does not exist or the multipart upload has been terminated or completed.	Use the existing part or reinitialize the part.
404 Not Found	NoSuchVersion	The specified version ID does not match any existing version.	Use a correct version ID.
404 Not Found	NoSuchWebsiteConfiguration	The requested website does not exist.	Configure the website first.

Status Code	Error Code	Error Message	Solution
405 Method Not Allowed	MethodNotAllowed	The specified method is not allowed against the requested resource. The message "Specified method is not supported." is returned.	The method is not allowed.
405 Method Not Allowed	FsNotSupport	POSIX buckets do not support this API.	The method is not allowed.
408 Request Timeout	RequestTimeout	The socket connection to the server has no read or write operations within the timeout period.	Check the network and try again, or contact technical support.
409 Conflict	BucketAlreadyExists	The requested bucket name already exists. The bucket namespace is shared by all users of OBS. Select another name and retry.	Change the bucket name.
409 Conflict	BucketAlreadyOwnedByYou	Your previous request for creating the namesake bucket succeeded and you already own it.	No more buckets need to be created.
409 Conflict	BucketNotEmpty	The bucket that you tried to delete is not empty.	Delete the objects in the bucket and then delete the bucket.
409 Conflict	InvalidBucketState	Invalid bucket status. After cross-region replication is configured, bucket versioning cannot be disabled.	Enable bucket versioning or cancel cross-region replication.
409 Conflict	OperationAborted	A conflicting operation is being performed on this resource. Retry later.	Try again later.
409 Conflict	ServiceNotSupported	The request method is not supported by the server.	Contact technical support.

Status Code	Error Code	Error Message	Solution
409 ObjectNotAppendable	ObjectNotAppendable	The object is not appendable.	Check the bucket type. Parallel file systems do not support append upload. Check the object type. Cold objects are not appendable.
411 Length Required	MissingContentLength	The HTTP header Content-Length is not provided.	Provide the Content-Length header.
412 Precondition Failed	PreconditionFailed	At least one of the specified preconditions is not met.	Modify according to the condition prompt in the returned message body.
414 URI Too Long	Request-URI Too Large	The URI used in the request was too long.	Shorten the URI length.
416 Client Requested Range Not Satisfiable	InvalidRange	The requested range cannot be obtained.	Retry with the correct range.
500 Internal Server Error	InternalError	An internal error occurs. Retry later.	Contact technical support.
501 Not Implemented	ServiceNotImplemented	The request method is not implemented by the server.	Contact technical support.
503 Service Unavailable	ServiceUnavailable	The server is overloaded or has internal errors.	Try later or contact technical support.
503 Service Unavailable	SlowDown	Too frequent requests. Reduce your request frequency.	Too frequent requests. Reduce your request frequency.

7 IAM Policies and Supported Actions

7.1 Introduction

This chapter describes fine-grained permissions management for your OBS. If your account does not require individual IAM users, skip this chapter.

By default, new IAM users do not have any permissions assigned. You need to add a user to one or more groups, and attach IAM policies to these groups. The user then inherits permissions from the groups it is a member of. This process is called authorization. After authorization, the user can perform specified operations on OBS based on the IAM policies.

For details about user policies related to OBS, see the topic of "User Permissions" in the "Service Overview" section of *OBS User Guide*. For details about the syntax structure and examples of IAM policies, see the topic of "IAM Policy" in the section "Permission Control" > "Permission Control Mechanisms" in the "Console Operation Guide" of *OBS User Guide*.

There are fine-grained policies and role-based access control (RBAC) policies. An RBAC policy consists of permissions for an entire service. Users in a group with such a policy assigned are granted all of the permissions required for that service. A fine-grained policy consists of API-based permissions for operations on specific resource types. Fine-grained policies, as the name suggests, allow for more fine-grained control than RBAC policies.

NOTE

- If you want to allow or deny the access to an API, fine-grained authorization is a good choice.
- Because of the cache, it takes about 10 to 15 minutes for the RBAC policy to take effect after being granted to users, enterprise projects, and user groups. After a fine-grained OBS policy is granted, it takes about 5 minutes for the policy to take effect.

An account has all of the permissions required to call all APIs, but IAM users must have the required permissions specifically assigned. The required permissions are determined by the actions supported by the API. Only users with the policies allowing for those actions can call the API successfully. For example, if an IAM user needs to create buckets using an API, the user must have been granted permissions that allow the **obs:bucket:CreateBucket** action.

Supported Actions

Operations supported by a fine-grained policy are specific to APIs. The following describes the headers of the actions provided in this chapter:

- Permissions: defined by actions in a custom policy
- APIs: REST APIs that can be called by a user who has been granted specific permissions
- Actions: specific operations that are allowed or denied in a custom policy
- IAM projects/Enterprise projects: the authorization scope of a custom policy. A custom policy can be applied to IAM projects or enterprise projects or both. Policies that contain actions for both IAM and enterprise projects can be used and applied for both IAM and Enterprise Management. Policies that contain actions only for IAM projects can be used and applied to IAM only.

  NOTE

  The check mark (√) indicates that an action takes effect. The cross mark (x) indicates that an action does not take effect.

OBS supports the following actions in custom policies:

- **Bucket-related actions** include actions supported by all OBS bucket-related APIs, such as the APIs for listing all buckets, creating and deleting buckets, configuring bucket policies, configuring bucket event notification, and configuring bucket logging.
- **Object-related actions** include APIs for uploading, downloading, and deleting objects.

7.2 Bucket Actions

Table 7-1 Bucket actions

Permission	API	Action	IAM Project	Enterprise Project
Listing all buckets	**Listing Buckets**	obs:bucket:ListAllMyBuckets	Supported	Supported
Creating a bucket	**Creating a Bucket**	obs:bucket:CreateBucket	Supported	Supported
Listing objects in a bucket	**Listing Objects in a Bucket**	obs:bucket:ListBucket	Supported	Supported
Listing object versions in a bucket	**Listing Objects in a Bucket**	obs:bucket:ListBucketVersions	Supported	Supported

Permission	API	Action	IAM Project	Enterprise Project
Determining whether a bucket exists and obtaining the bucket metadata	**Obtaining Bucket Metadata**	obs:bucket:HeadBucket	Supported	Supported
Obtaining the bucket location	**Obtaining Bucket Location**	obs:bucket:GetBucketLocation	Supported	Supported
Deleting a bucket	**Deleting Buckets**	obs:bucket:DeleteBucket	Supported	Supported
Configuring a bucket policy	**Configuring a Bucket Policy**	obs:bucket:PutBucketPolicy	Supported	Supported
Obtain the bucket policy configurations	**Obtaining Bucket Policy Information**	obs:bucket:GetBucketPolicy	Supported	Supported
Deleting a bucket policy	**Deleting a Bucket Policy**	obs:bucket:DeleteBucketPolicy	Supported	Supported
Configuring the bucket ACL	**Configuring a Bucket ACL**	obs:bucket:PutBucketAcl	Supported	Supported
Obtaining the bucket ACL information	**Obtaining Bucket ACL Information**	obs:bucket:GetBucketAcl	Supported	Supported
Configuring logging for a bucket	**Configuring Logging for a Bucket**	obs:bucket:PutBucketLogging	Supported	Supported
Obtaining the logging configurations of a bucket	**Obtaining a Bucket Logging Configuration**	obs:bucket:GetBucketLogging	Supported	Supported
Configuring or deleting a lifecycle rule	**Configuring Bucket Lifecycle Rules** **Deleting Lifecycle Rules**	obs:bucket:PutLifecycleConfiguration	Supported	Supported
Obtaining the lifecycle rule configurations	**Obtaining Bucket Lifecycle Configuration**	obs:bucket:GetLifecycleConfiguration	Supported	Supported
Configuring versioning for a bucket	**Configuring Versioning for a Bucket**	obs:bucket:PutBucketVersioning	Supported	Supported

Permission	API	Action	IAM Project	Enterprise Project
Obtaining the versioning configurations of a bucket	Obtaining Bucket Versioning Status	obs:bucket:GetBucketVersioning	Supported	Supported
Configuring event notifications for a bucket	Configuring Event Notification for a Bucket	obs:bucket:PutBucketNotification	Supported	Supported
Obtaining the event notification configurations of a bucket	Obtaining the Event Notification Configuration of a Bucket	obs:bucket:GetBucketNotification	Supported	Supported
Configuring storage class for a bucket	Configuring Storage Class for a Bucket	obs:bucket:PutBucketStoragePolicy	Supported	Supported
Obtaining the storage class of a bucket	Obtaining Bucket Storage Class Information	obs:bucket:GetBucketStoragePolicy	Supported	Supported
Adding tags to a bucket	Configuring Tags for a Bucket	obs:bucket:PutBucketTagging	Supported	Supported
Obtaining bucket tags	Obtaining Bucket Tags	obs:bucket:GetBucketTagging	Supported	Supported
Deleting bucket tags	Deleting Tags	obs:bucket:DeleteBucketTagging	Supported	Supported
Limiting storage capacity for a bucket	Configuring Bucket Storage Quota	obs:bucket:PutBucketQuota	Supported	Supported
Querying the storage capacity limit of a bucket	Querying Bucket Storage Quota	obs:bucket:GetBucketQuota	Supported	Supported
Querying the used capacity of a bucket	Obtaining Storage Information of a Bucket	obs:bucket:GetBucketStorage	Supported	Supported
Configuring a user-defined domain name for a bucket	Configuring a Custom Domain Name for a Bucket	obs:bucket:PutBucketCustomDomainConfiguration	Supported	Supported

Permission	API	Action	IAM Project	Enterprise Project
Obtaining the user-defined domain name of a bucket	**Obtaining the Custom Domain Name of a Bucket**	obs:bucket:GetBucketCustomDomainConfiguration	Supported	Supported
Deleting the user-defined domain name of a bucket	**Deleting the Custom Domain Name of a Bucket**	obs:bucket:DeleteBucketCustomDomainConfiguration	Supported	Supported
Configuring or deleting encryption for a bucket	**Configuring Bucket Encryption** **Deleting the Encryption Configuration of a Bucket**	obs:bucket:PutEncryptionConfigura-tion	Supported	Supported
Obtaining the encryption configurations of a bucket	**Obtaining Bucket Encryption Configuration**	obs:bucket:GetEncryptionConfigura-tion	Supported	Supported
Configuring static website hosting for a bucket	**Configuring Static Website Hosting for a Bucket**	obs:bucket:PutBucketWebsite	Supported	Supported
Obtaining the static website hosting configurations of a bucket	**Obtaining the Static Website Hosting Configuration of a Bucket**	obs:bucket:GetBucketWebsite	Supported	Supported
Deleting the static website hosting configurations of a bucket	**Deleting the Static Website Hosting Configuration of a Bucket**	obs:bucket:DeleteBucketWebsite	Supported	Supported
Configuring or deleting CORS rules for a bucket	**Configuring Bucket CORS** **Deleting the CORS Configuration of a Bucket**	obs:bucket:PutBucketCORS	Supported	Supported

Permission	API	Action	IAM Project	Enterprise Project
Obtaining the CORS configurations of a bucket	Obtaining the CORS Configuration of a Bucket	obs:bucket:GetBucketCORS	Supported	Supported
Listing initiated multipart uploads in a bucket	Listing Initiated Multipart Uploads in a Bucket	obs:bucket:ListBucketMultipartUploads	Supported	Supported

7.3 Object Actions

Table 7-2 Object actions

Permission	API	Action	IAM Project	Enterprise Project
Uploading objects with PUT or POST, copying objects, appending content to objects, initiating a multipart upload, as well as uploading, copying, and assembling parts	Uploading an Object - PUT Uploading an Object - POST Copying an Object Appending an Object Initiating a Multipart Upload Uploading Parts Completing a Multipart Upload	obs:object:PutObject	Supported	Supported
Obtaining the content and metadata of an object	Downloading an Object Querying Object Metadata	obs:object:GetObject	Supported	Supported
Obtaining the content and metadata of a specific object version	Downloading an Object Querying Object Metadata	obs:object:GetObjectVersion	Supported	Supported

Permission	API	Action	IAM Project	Enterprise Project
Deleting a single object or a batch of objects	**Deleting an Object** **Deleting Objects**	obs:object:DeleteObject	Supported	Supported
Deleting a single object version or a batch of object versions	**Deleting an Object** **Deleting Objects**	obs:object:DeleteObjectVersion	Supported	Supported
Restoring Cold objects	**Restoring Cold Objects**	obs:object:RestoreObject	Supported	Supported
Configuring the object ACL	**Configuring an Object ACL**	obs:object:PutObjectAcl	Supported	Supported
Configuring the ACL for a specific object version	**Configuring an Object ACL**	obs:object:PutObjectVersionAcl	Supported	Supported
Obtaining the object ACL information	**Obtaining Object ACL Configuration**	obs:object:GetObjectAcl	Supported	Supported
Obtaining the ACL information of a specific object version	**Obtaining Object ACL Configuration**	obs:object:GetObjectVersionAcl	Supported	Supported
Modifying object metadata	**Modifying Object Metadata**	obs:object:ModifyObjectMetaData	Supported	Supported
Listing uploaded parts	**Listing Uploaded Parts**	obs:object:ListMultipartUploadParts	Supported	Supported
Aborting a multipart upload	**Canceling a Multipart Upload Task**	obs:object:AbortMultipartUpload	Supported	Supported

8 Appendixes

8.1 Status Codes

Table 8-1 lists the status codes and prompt message returned by the server to the user.

Table 8-1 Status codes

Status Code	Description
2xx	Indicates that the server has successfully returned the requested data.
4xx	Indicates that the request sent from the client is incorrect, so the server does not create or modify data.
5xx	Indicates that an error occurs on the server, and the user does not know whether the request has been successfully sent.

NOTE

Send API requests using the HTTP/HTTPS format that complies with **https://www.ietf.org/rfc/rfc2616.txt**.

8.2 Obtaining Access Keys (AK/SK)

When you call APIs, you need to use the AK and SK for authentication. To obtain the AK and SK, perform the following steps:

To access OBS in the AP-Kuala Lumpur-OP6 region, contact the administrator to obtain the AK and SK by referring to the **access key obtaining method**.

8.3 Obtaining a Domain ID and a User ID

When making API calls, you may need to specify the domain ID (**DomainID**) and user ID (**UserID**) in some requests. To obtain them from the console, do as follows:

Step 1 Log in to the console.

Step 2 Click the username and select **My Credentials** from the drop-down list.

On the **My Credentials** page, view the domain ID and user ID.

----End

8.4 Consistency of Concurrent Operations

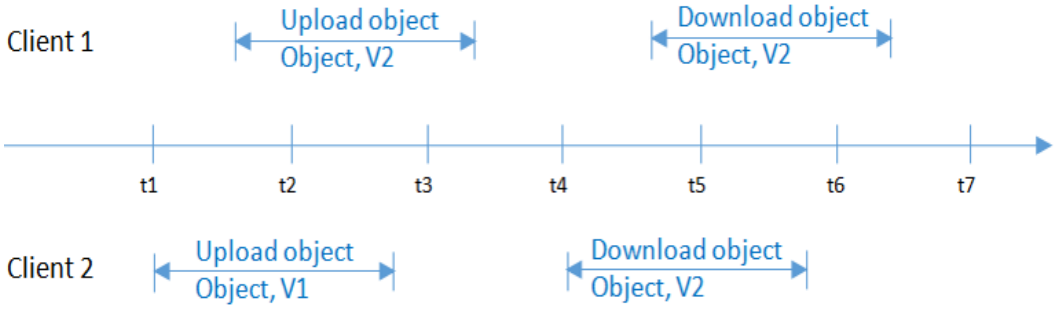
After a success message is returned in response to a client's write or deletion request, the client can obtain the latest data. If a client that initiates a write request times out in waiting for a response, or the server returns HTTP response status code **500** or **503**, the subsequent read operations may fail. If such an error occurs, query whether the data has been successfully uploaded to the server. If not, upload the data again.

If a client simultaneously uploads, queries, or deletes 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 latest upload request received by the system will replace the previous one. If you want to prevent an object from being simultaneously accessed, you must add a lock mechanism for the object in upper-layer applications.

Example of Concurrent Operations

1. When client1 is uploading an object V1, client2 is uploading an object V2 with the same name. After the successful uploads, both client1 and client2 can access the latest object data V2, as shown in **Figure 8-1**.

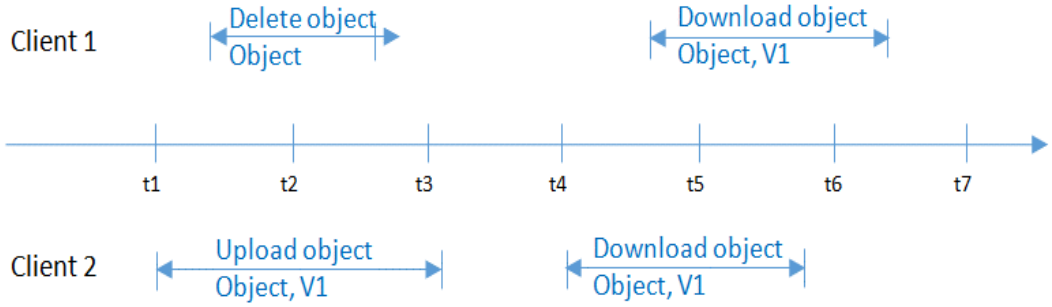
Figure 8-1 Concurrent upload of the same object



2. When client2 is uploading an object V1 and object metadata is not written yet, client1 deletes an object with the same name. In this scenario, the upload

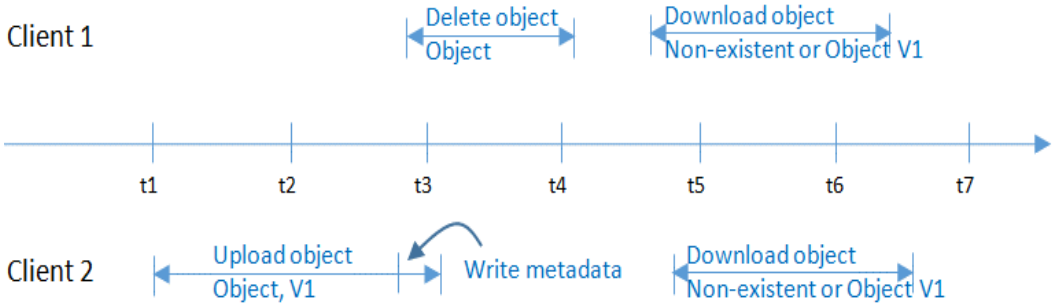
operation of client2 is still successful, and both client1 and client2 can access data object V1, as shown in **Figure 8-2**.

Figure 8-2 Concurrent upload and deletion of the same object (1)



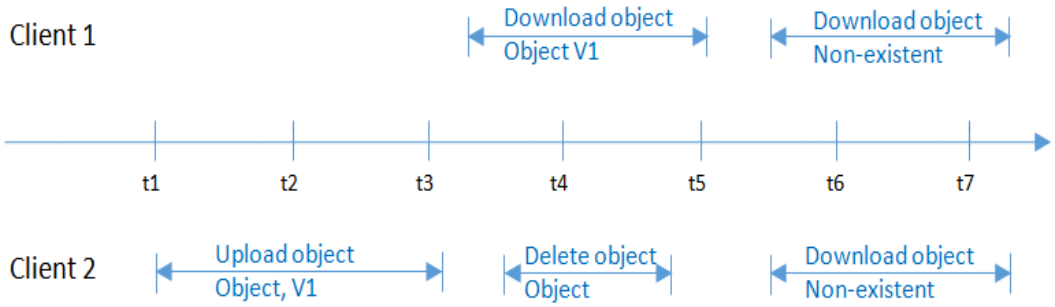
3. When client2 has successfully uploaded an object V1 and object metadata is still being written, client1 deletes an object with the same name. In this scenario, the upload operation of client2 is still successful. However, when client1 and client2 attempt to download the object, they may be able to access data object V1, or an error may be returned indicating that the object does not exist, as shown in **Figure 8-3**.

Figure 8-3 Concurrent upload and deletion of the same object (2)



4. When client1 is downloading an object, client2 deletes an object with the same name. In this scenario, client1 may have downloaded a full copy or only part of the object data. After a deletion success message is returned to client2, an attempt to download the object will fail, and an error will be returned indicating that the object does not exist, as shown in **Figure 8-4**.

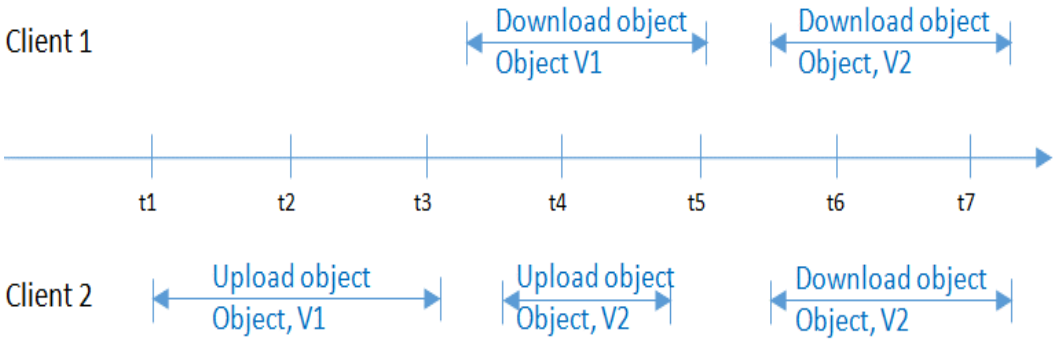
Figure 8-4 Concurrent download and deletion of the same object



5. When client1 is downloading an object, client2 is updating an object with the same name. In this scenario, client1 may have downloaded a full copy or only part

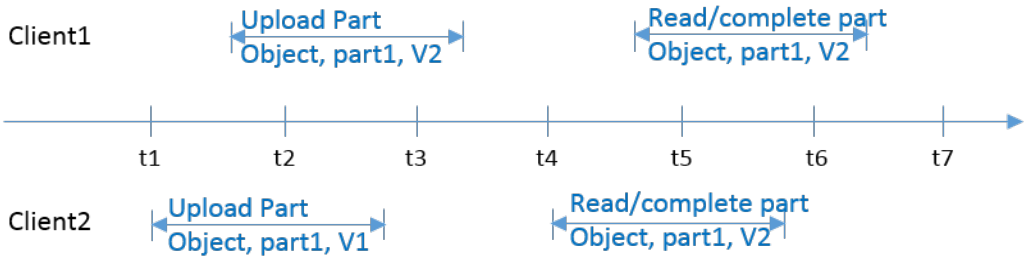
of the object data. After an update success message is returned to client 2, an attempt to download the object will succeed, and the latest data will be returned, as shown in **Figure 8-5**.

Figure 8-5 Concurrent download and update of the same object



6. When client2 is uploading part V1 of an object, client1 is uploading part V2 of the same object. After part V2 is uploaded successfully, both client1 and client2 can list the information about the multipart whose entity tag (ETag) is part V2, as shown in **Figure 8-6**.

Figure 8-6 Concurrently uploading the same part of the same object



A Change History

Date	Change History
2022-08-16	This is the first official release.

