Object Storage Service

Console User Guide

MORE THAN JUST CLOUD | Alibaba Cloud

Console User Guide

The Alibaba Cloud OSS console provides an intuitive operation interface for you to perform most OSS tasks. Before you log on to the OSS console, ensure that you have registered an Alibaba Cloud account. If you do not have an Alibaba Cloud account, the system will prompt you to register an account when you activate OSS.

Operation procedure

Log on to the Alibaba Cloud official website.

On the OSS product detail page, click **Buy now**.

After OSS is activated, click **Console** to access the OSS console.

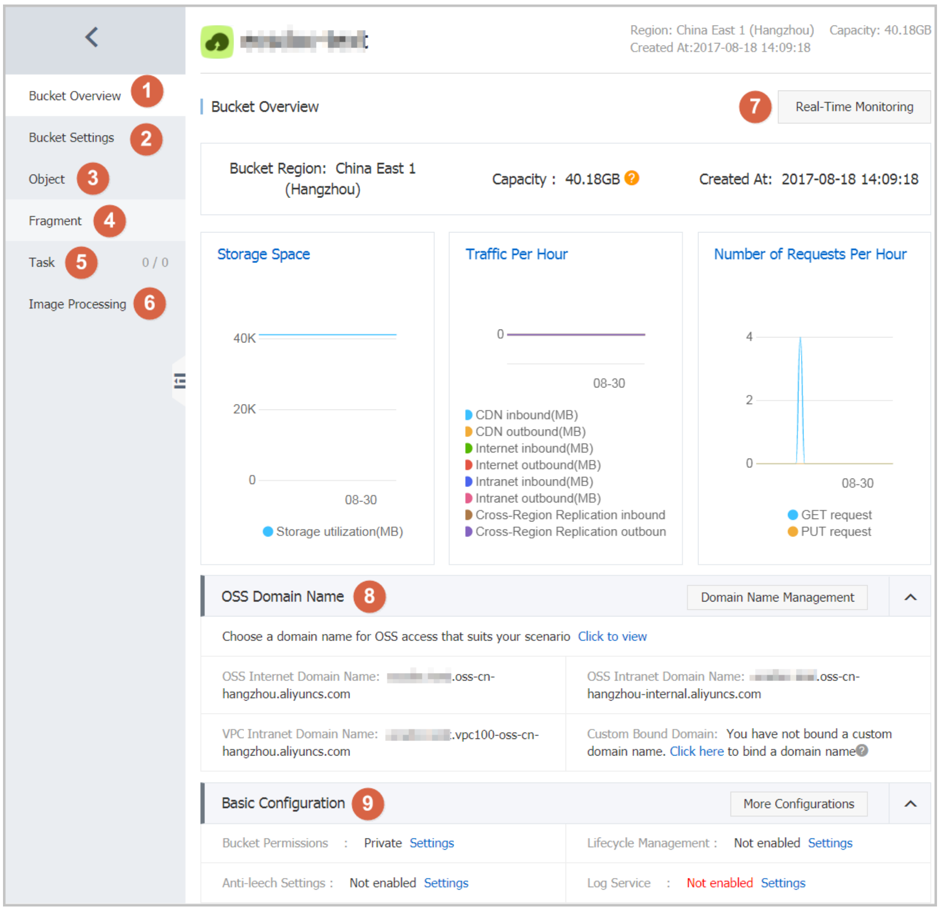
You can also click **Console** in the upper-right menu bar on the homepage to open Alibaba Cloud console, and click **Object Storage Service** in the left-side navigation pane to access the OSS console.

Manage buckets

All files of Alibaba Cloud OSS are stored in buckets. A bucket is a unit for managing the stored files. All objects must belong to a bucket. You can set the attributes of a bucket for region and file access control and file lifecycle management. These attributes apply to all files in the bucket. Therefore, you can create different buckets to implement different management functions flexibly.

The storage space in a bucket is non-hierarchical, i.e., it lacks the features of file systems, such as directories. Therefore, all files are directly affiliated with their corresponding buckets. However, you can group, classify, and manage relevant files by folders.

The bucket overview page includes the following content.



[redacted]

Region: China East 1 (Hangzhou) Capacity: 40.18GB
Created At:2017-08-18 14:09:18

Bucket Overview

Bucket Region: China East 1 (Hangzhou) Capacity : 40.18GB Created At: 2017-08-18 14:09:18

Choose a domain name for OSS access that suits your scenario Click to view

OSS Internet Domain Name: [redacted].oss-cn-hangzhou.aliyuncs.com

OSS Intranet Domain Name: [redacted].oss-cn-hangzhou-internal.aliyuncs.com

VPC Intranet Domain Name: [redacted].vpc100-oss-cn-hangzhou.aliyuncs.com

Custom Bound Domain: You have not bound a custom domain name. Click here to bind a domain name

Bucket Permissions : Private Settings

Lifecycle Management : Not enabled Settings

Anti-leech Settings : Not enabled Settings

Log Service : Not enabled Settings

SN	Content	Description
1	**Bucket Overview**	View the basic information of the bucket, including the resource usage, domain name, and configuration information.
2	**Bucket Settings**	View and modify the properties of the bucket.
3	**Object**	View and manage the files and folders in a bucket.
4	**Fragment**	View and delete file fragments caused by multipart upload.
5	**Task**	View the file upload status.
6	**Image Processing**	Enable/disable image service and manage image styles.
7	**Real-time Monitoring**	View the statistics of OSS requests.
8	**OSS Domain Name**	View the domain names and bind the custom domain name.
9	**Basic Configuration**	View the bucket

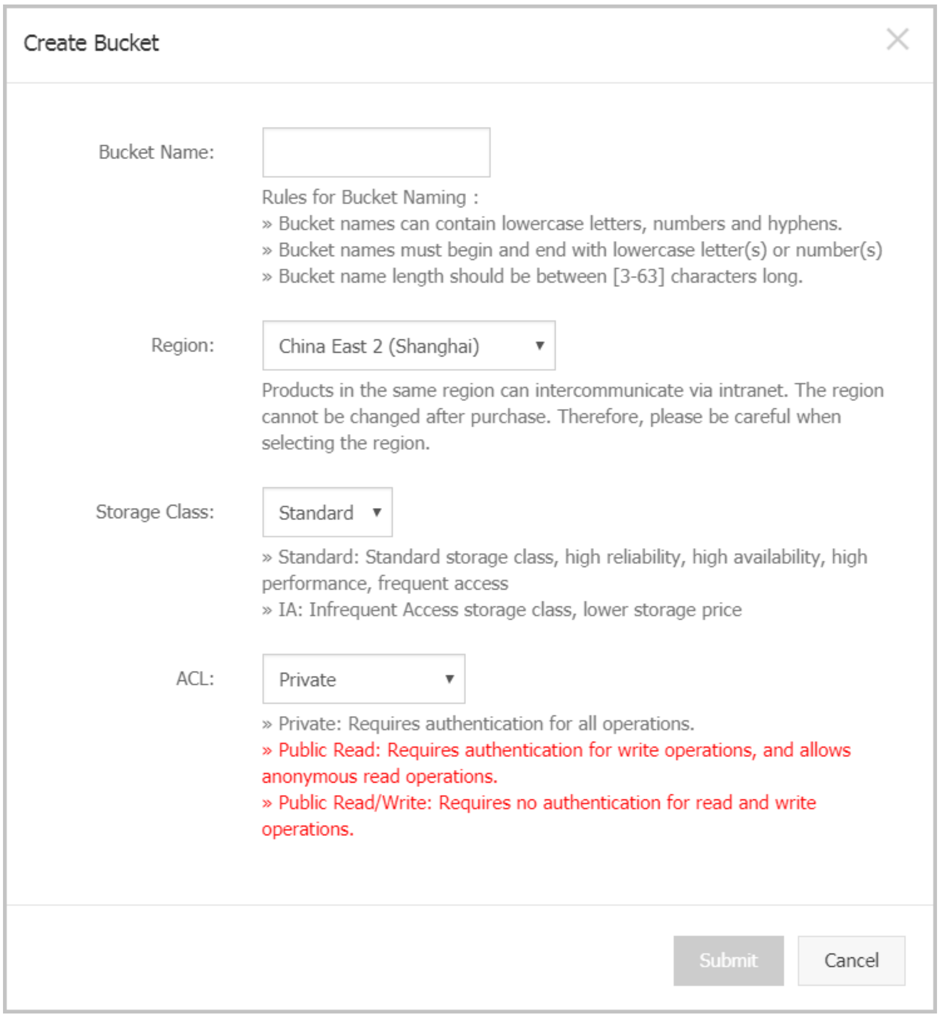
		configurations, and click the corresponding links to view and modify the configurations.

Before uploading any file to the OSS, you must create a bucket to store files. A bucket needs to be configured with various attributes, including its geographic region, access permission, and other metadata.

Operation procedure

Go to the OSS console.

Click **Create Bucket** to open the **Create Bucket** dialog box.



Create Bucket

Bucket Name:

Rules for Bucket Naming :
» Bucket names can contain lowercase letters, numbers and hyphens.
» Bucket names must begin and end with lowercase letter(s) or number(s)
» Bucket name length should be between [3-63] characters long.

Region: China East 2 (Shanghai)

Products in the same region can intercommunicate via intranet. The region cannot be changed after purchase. Therefore, please be careful when selecting the region.

Storage Class: Standard

» Standard: Standard storage class, high reliability, high availability, high performance, frequent access
» IA: Infrequent Access storage class, lower storage price

ACL: Private

» Private: Requires authentication for all operations.
» Public Read: Requires authentication for write operations, and allows anonymous read operations.
» Public Read/Write: Requires no authentication for read and write operations.

In the **Bucket Name** text box, enter the bucket name. The bucket name must comply with the naming rules and must be unique among all existing bucket names in Alibaba Cloud OSS. The bucket name cannot be changed after being created. For more information about bucket naming, see Basic OSS concepts.

In the **Region** drop-down box, select the data center of the bucket. The region cannot be changed after being subscribed. To access the OSS through the ECS intranet, you can select the same region with your ECS. For more information about regions, see Basic OSS concepts.

In the **Storage Class** drop-down box, select the storage class for the bucket.

In the **ACL** drop-down box, select an access permission option for the bucket. After creating a bucket, you can set bucket attributes to modify the access permission of the bucket. For more information about access permission, see Basic OSS concepts.

Private: Only the owner of the bucket can perform read/write operations on the files in the bucket. Other people cannot access the files.

Public Read: Only the owner of the bucket can perform write operations on the files in the bucket, while anyone (including anonymous users) can perform read operations on the files.

Public Read/Write: Anyone (including anonymous users) can perform read and write operations on the files in the bucket. The fees incurred by these operations will be borne by the owner of the bucket. Select this option with caution.

Click **Submit** to create the bucket.

If you no longer need a bucket, delete it to avoid further fees. Before deleting a bucket, ensure that all files in it are cleared, including file fragments caused by incomplete multipart upload. Otherwise, the bucket cannot be deleted. If you want to delete all files in a bucket, we recommend that you use lifecycle management.

Operation procedure

Go to the OSS console.

Click the delete icon of the target bucket.

Click **Confirm** to delete the bucket.

The OSS provides an Access Control List (ACL) for permission control. You can configure an ACL when creating a bucket and modify the ACL after creating the bucket. If no ACL is configured, the default value is **Private**.

The OSS ACL provides bucket-level access control. Currently, three access permissions are available for a bucket:

- **Private**: Only the owner of the bucket can perform read/write operations on the files in the bucket. Other people cannot access the files.
- **Public Read**: Only the owner of the bucket can perform write operations on the files in the bucket, while anyone (including anonymous users) can perform read operations on the files.
- **Public Read/Write**: Anyone (including anonymous users) can perform read and write operations on the files in the bucket. The fees incurred by these operations will be borne by the owner of the bucket. Use this permission with caution.

Operation procedure

Go to the OSS console.

Select a bucket to open the **Bucket Overview** page.

Select **Bucket Settings** > **ACL**.

In the **Read and Write Permissions** drop-down list, select an access permission option for the bucket.

Click **Set** to save the setting.

You can set your bucket to host a static website and access this static website through the bucket domain name.

- If the default webpage is blank, static website hosting is disabled.
- If static website hosting is enabled, we recommend that you use CNAME to bind your domain name.
- Directly accessing the static website root domain or any URL ending with “/ ” under this domain will return the default homepage.

For more detailed information, see Static Website Hosting.

Operation procedure

Go to the OSS console.

Select a bucket to open the **Bucket Overview** page.

Select **Bucket Settings** > **Website**.

Set **Default Webpage**, which is the index page (equivalent to the website’s index.html). Only HTML files that have been stored in the bucket can be used.

Set **404 Error Default Webpage**, which is the default 404 page returned when an incorrect path is accessed. Only HTML and image files that have been stored in the bucket can be used. If this field is left empty, the default 404 page is disabled.

Click **Set** to save the static website setting.

You can enable or disable logging for a bucket through the console. You can store logs in the same logging-enabled bucket or a new bucket. For more information about the bucket logging format, see Set access logging.

Operation procedure

Go to the OSS console.

Select a bucket to open the **Bucket Overview** page.

Select **Bucket Settings** > **Logging**.

In the **Log Storage Location** drop-down list, select the name of a bucket to store the logs. Only buckets of the same user and region can be selected. To disable logging, select **No Bucket**.

In the **Log Prefix** text box, type the prefix of the log name, that is, *<TargetPrefix>* in the following logging naming conventions.

Click **Set** to save the logging setting.

Logging naming conventions

The following is the naming conventions for the access log record:*<TargetPrefix><SourceBucket>* YYYY-MM-DD-HH-MM-SS-*<UniqueString>*

- *<TargetPrefix>*: indicates the log prefix specified by the user.
- *<SourceBucket>*: indicates the name of the source bucket.
- YYYY-MM-DD-HH-MM-SS: indicates the time when the log is created. YYYY indicates the year, MM indicates the month, DD indicates the day, HH indicates the hour, MM indicates the minute, and SS indicates the second.
- *<UniqueString>*: indicates the string generated by the OSS.

An example object name used to store OSS access logs is as follows:
MyLog-OSS-example2015-09-10-04-00-00-0000
In the preceding example, **MyLog** is the log prefix specified by the user, **oss-example** is the name of the source bucket, **2015-09-10-04-00-00** is the log creation time, and **0000** is the string generated by the OSS.

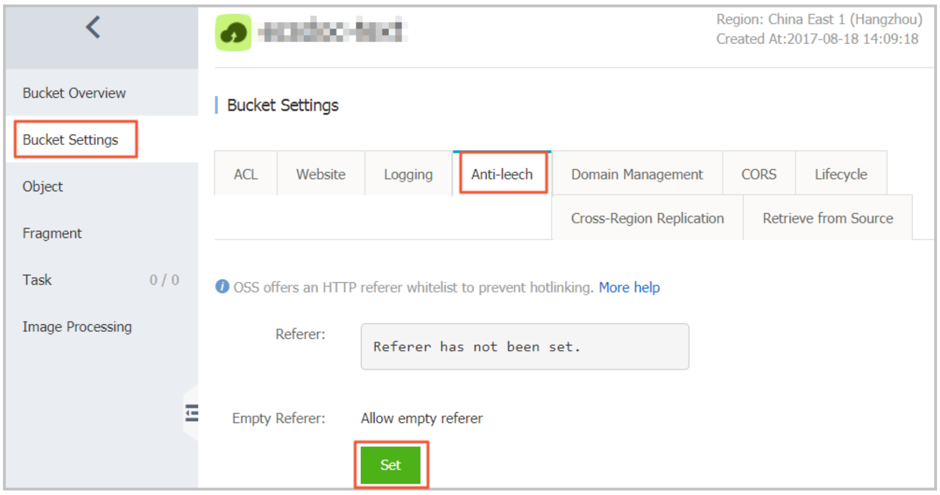
The OSS is a Pay-As-You-Go service. To reduce extra fees caused in case your data on the OSS is stolen by others, the OSS supports anti-leech based on the referer field in the HTTP header. You can configure a referer whitelist for a bucket and configure whether to allow the access requests that have an empty referer field.

Operation procedure

Go to the OSS console.

Select a bucket to open the **Bucket Overview** page.

Select **Bucket Settings** > **Anti-leech**, and then click **Set**.



[redacted]

Region: China East 1 (Hangzhou)
Created At:2017-08-18 14:09:18

Bucket Settings

OSS offers an HTTP referer whitelist to prevent hotlinking. More help

Referer: Referer has not been set.

Empty Referer: Allow empty referer

Add a website whitelist in the **Referer** field and select whether to allow an empty referer in the **Empty Referer** field.

Click **Submit** to save the anti-leech setting.

Example

For a bucket named test-1-001, set its referer whitelist to http://www.aliyun.com. Then, only requests with a referer of http://www.aliyun.com can access the objects in the bucket.

After uploading an object to a bucket, you can obtain an object address including two parts: an OSS domain name address (<*BucketName*>.<*Endpoint*>) and an object file name. To avoid possible cross-origin or security problems in your business, we recommend that you access OSS using a user-defined domain name. After the domain name is successfully bound, you also need to add a CNAME record pointing to the Internet domain name of the bucket to ensure proper domain name-based access to the OSS.

Note:

- You must apply for an ICP license for your bound domain name. Otherwise, the domain name will not be accessible.
- Each bucket can be bound with a maximum of 20 domain names.

After a user-defined domain name is successfully bound, access addresses of the files stored in your OSS will use the user-defined domain name. For example, if your bucket test-1-001 is located at the Hangzhou node, the object file name is test001.jpg, and the bound user-defined domain name is hello-world.com, then the access address of this object is as follows:

- Before binding: test-1-001..oss-cn-hangzhou.aliyuncs.com/test001.jpg

- After successful binding: hello-world.com/test001.jpg

Bind a domain name

Go to the OSS console.

Select a bucket to open the **Bucket Overview** page.

Select **Bucket Settings** > **Domain Management**.

Click **Add Domain Name**.

Enter the domain name you want to bind in the dialog box.

Click **Next**. The **Add Canonical Name** page is displayed.

> **NOTE:** If the domain name you want to bind has been maliciously bound by another user, you can verify the ownership of the domain name by adding a TXT record. In this way, the domain name can be forcibly bound to the correct bucket and its binding to the previous bucket is released.

Select the automatic or manual adding method.

Add automatically: The system will automatically add the corresponding CNAME record in the Alibaba Cloud DNS. Make sure you change the domain name’ s DNS to Alibaba Cloud DNS if this domain name has not been resolved in Alibaba Cloud DNS already.

Add manually: Select this option if the domain name has already been resolved in the Alibaba Cloud DNS of another account.

Click **Finish** to complete domain name binding.

Verify domain name ownership

Wait for the system to generate a TXT record based on your information.

Log on to your DNS provider and add the corresponding TXT record.

Click **Verify** on the console. If the system detects that the TXT record value for this domain name is as expected, the domain name ownership passes verification.

The OSS provides Cross-Origin Resource Sharing (CORS) in the HTML5 protocol to help users achieve cross-origin access. When the OSS receives a cross-origin request (or OPTIONS request), it reads the bucket’ s CORS rules and then checks the relevant permissions. The OSS checks each rule sequentially, uses the first rule that matches to approve the request, and returns the corresponding header. If none of the rules match, the OSS does not attach any CORS header.

Operation procedure

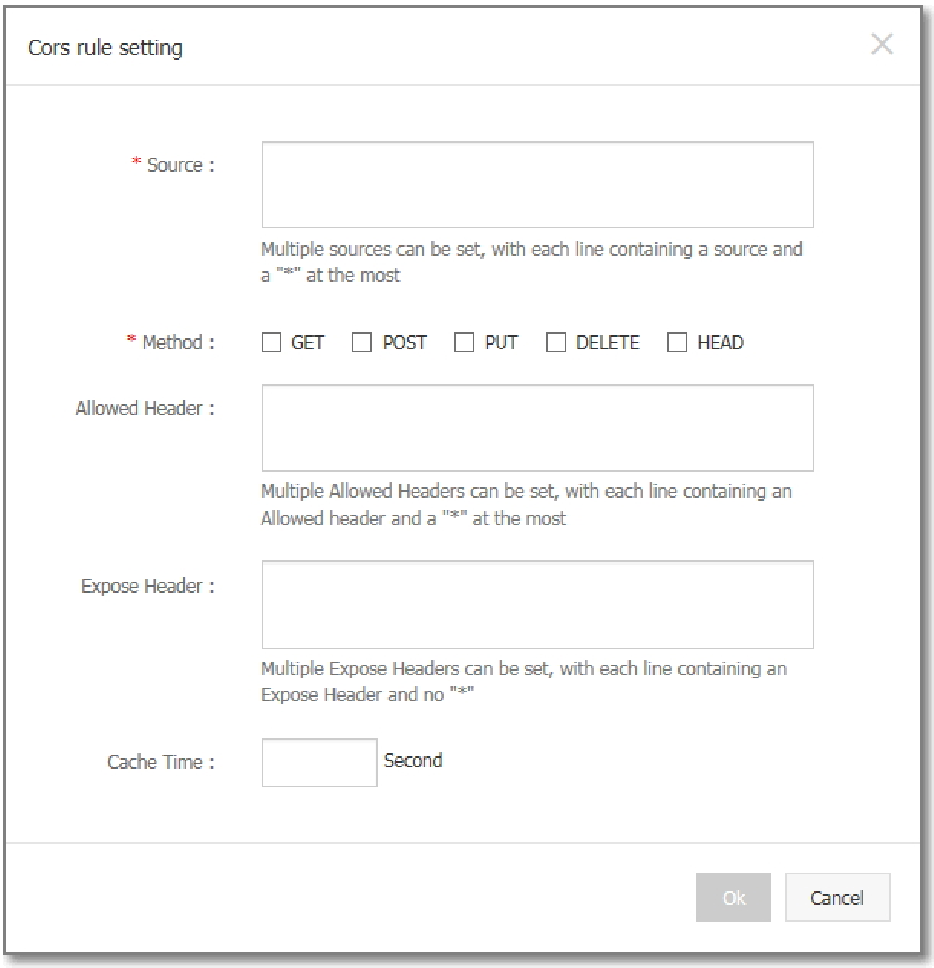
Go to the OSS console.

Select a bucket to open the **Bucket Overview** page.

Select **Bucket Settings** > **CORS**.

Click **Add Rule**. The **Set CORS Rule** dialog box is displayed.

Configure the CORS rule in the dialog box. A maximum of 10 rules can be configured for each bucket.



Cors rule setting

* Source :

Multiple sources can be set, with each line containing a source and a "*" at the most

* Method : □ GET □ POST □ PUT □ DELETE □ HEAD

Allowed Header :

Multiple Allowed Headers can be set, with each line containing an Allowed header and a "*" at the most

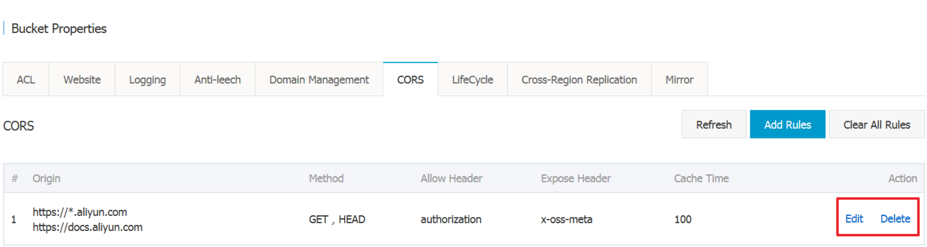
Expose Header :

Multiple Expose Headers can be set, with each line containing an Expose Header and no "*"

Cache Time : Second

- **Source**: Indicates the origins allowed for cross-origin requests. Multiple matching rules are allowed, which are separated by a carriage return. Each matching rule allows up to one “* ” wildcard.
- **Method**: Indicates the allowed cross-origin request methods.
- **Allowed Header**: Indicates the allowed cross-origin request headers. Multiple matching rules are allowed, which are separated by a carriage return. Each matching rule allows up to one “* ” wildcard.
- **Expose Header**: Indicates the response headers users are allowed to access from an application (e.g., a Javascript XMLHttpRequest object).
- **Cache Time**: Indicates the cache time for the returned results of browser prefetch (OPTIONS) requests to a specific resource.

Click **OK** to save this rule. You can also edit or delete the configured rules.



Bucket Properties

CORS

#	Origin	Method	Allow Header	Expose Header	Cache Time	Action
1	https://*.aliyun.com https://docs.aliyun.com	GET , HEAD	authorization	x-oss-meta	100	Edit Delete

You can define and manage the lifecycle of all the objects or the objects with the same prefix in a bucket. Lifecycle management is used for batch file deletion and automatic fragment deletion.

The system will ensure that data is cleared for objects that match a lifecycle rule, within two days from the effective date. Configure rules with caution because data deleted based on a lifecyle rule cannot be recovered..

Operation procedure

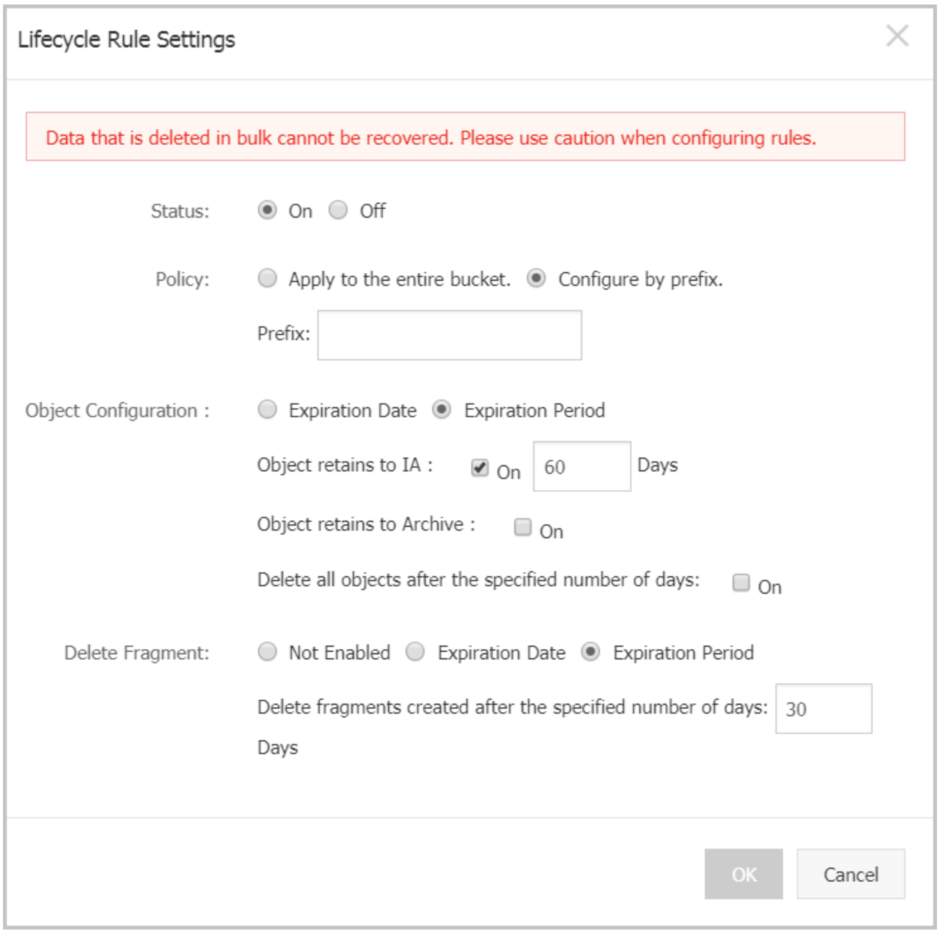
Go to the OSS console.

Select a bucket to open the **Bucket Overview** page.

Select **Bucket Settings** > **Lifecycle**.

Click **Add Rule**. The **Lifecycle Rule Settings** dialog box is displayed.

Set the lifecycle in the dialog box.



Lifecycle Rule Settings

Data that is deleted in bulk cannot be recovered. Please use caution when configuring rules.

Status: ● On ○ Off

Policy: ○ Apply to the entire bucket. ● Configure by prefix.

Prefix:

Object Configuration : ○ Expiration Date ● Expiration Period

Object retains to IA : ☑ On 60 Days

Object retains to Archive : □ On

Delete all objects after the specified number of days: □ On

Delete Fragment: ○ Not Enabled ○ Expiration Date ● Expiration Period

Delete fragments created after the specified number of days: 30 Days

Status: Specifies whether to enable or disable the rule.

Policy

- **Apply to the entire bucket**: If you select this option, then the rule applies to all objects in the bucket.
- **Configure by prefix**: If you select this option, you must specify **Prefix**. Then the rule only applies to the objects with the specified prefix, such as **img/**.

Object Configuration

- **Expiration Date**: The objects whose last modification time is earlier than the specified date will be deleted. For example, if **Expiration Date** is set to **2012-12-21**, the objects whose last modification time is earlier than 2012-12-21 will be scanned and deleted by the backend program.
- **Expiration Period**: The number of days for retaining an object. If the number of days from the last modification time of the object exceeds the specified number of days, the object will be deleted. For example, if **Expiration Period** is set to **30**, the objects whose last modification date is 2016-1-1 will be scanned and deleted by the backend program on 2016-1-31.

Delete Fragment

- **Not Enabled**: If this option is selected, fragments will not be automatically deleted.
- **Expiration Date**: The multipart upload tasks whose last modification time is earlier than the specified date will be deleted. For example, if the **Expiration Date** is set to **2012-12-21**, the multipart upload tasks whose last modification time is earlier than 2012-12-21 will be scanned and deleted by the backend program.
- **Expiration Period**: The number of days for storing a multipart upload task. If the number of days from the initialization date of a multipart upload task exceeds the specified number of days, the task will be deleted. For example, if **Expiration Period** is set to **30**, the multipart upload tasks whose initialization date is 2016-1-1 will be scanned and deleted by the backend program on 2016-1-31.

Click **OK** to save this rule. After the rule is successfully saved, you can view the configured lifecycle rule in the policy list and perform corresponding **Edit** or **Delete** operations.

Cross-region replication supports synchronization of buckets with different names. If you have two buckets belonging to different regions, you can enable cross-region replication on the console to synchronize data from the origin bucket to the target bucket in a real-time manner. Currently, only the regions in China supports cross-region replication.

Operation procedure

Go to the OSS console.

Click the name of the source bucket to enter the **Bucket Overview** page.

Click **Bucket Settings** > **Cross-Region Replication**.

Click **Enable Cross-Region Replication**. A dialog box is displayed.

Select the region and name of the target bucket, and choose whether to synchronize historical data.

Cross-region replication rules:

- Two buckets involved in data synchronization must belong to different regions. Data synchronization cannot be performed between buckets in the same region.

- Two buckets enabled with cross-region replication cannot have a synchronization relationship with any other buckets.
- During synchronization of historical data, objects replicated from the origin bucket may overwrite the objects with the same names in the target bucket. Therefore, ensure data consistency before replication.

Click **OK** to save the setting. After the configuration is complete, it takes 3 to 5 minutes for cross-region replication to be enabled. Synchronization-related information will be displayed after bucket synchronization.

Data replication is an asynchronous process and depends on data size.

You can set mirroring rules to define whether to get source data by mirroring or redirection. Mirroring rules are usually used for hot migration of data and redirection of specific requests. You can configure up to five mirroring rules, which will be executed by the system in sequence.

Operation procedure

Go to the OSS console.

Select a bucket to open the **Bucket Overview** page.

Select **Bucket Settings** > **Retrieve from Source**.

Click **Add Rule**. The **Set Source Retrieval Rule** dialog box is displayed.

Select **Mirroring** or **Redirect** type from the dialog box to configure a rule.

Click **OK** to save the rule. After the rule is successfully saved, you can view the configured mirroring rule in the rule list and perform corresponding **Edit** or **Delete** operations.

Manage objects

After you create a bucket, you can upload all types of files (objects) to the bucket. Using the OSS console, you can upload files smaller than 500 MB. To upload files larger than 500 MB, you can use an application programming interface (API) or software development kit (SDK). For details, see the relevant chapter of the Alibaba Cloud OSS Developer Guide.

> **Note:** If the name of the file to be uploaded is duplicate with that of the existing file in the bucket, it will overwrite the existing one.

Operation procedure

Go to the OSS console.

Click the name of the target bucket to open the **Bucket Overview** page.

Click **Object** in the left-side navigation pane.

Click **Upload** to open the **Select File** dialog box.

Select one or multiple files to be uploaded and click **Open**. After the files are uploaded successfully, click **Refresh** to display the uploaded files.

Alibaba Cloud OSS does not has the term "folder". All elements are stored as objects. To use a folder on the OSS console, you actually create an object with a size of 0 ending with a slash (/) used to sort the same type of files and process them in batches. By default, the OSS console displays objects ending with a slash as folders. These objects can be uploaded and downloaded normally. On the OSS console, you can use OSS folders like using folders in the Windows operating system.

> **Note**: The OSS console displays any object ending with a slash as a folder, whether or not it contains data. The object can be downloaded only using an application programming interface (API) or software development kit (SDK). For details about how to create and use simulated folders, see API - Get Bucket and **Folder Simulation** in Java SDK- Object.

Operation Procedure

Go to the OSS console.

Click the name of the target bucket to open the **Bucket Overview** page.

Click **Object** in the left-side navigation pane.

Click **Create Folder**.

Enter a folder name in the **Folder Name** text box.

Click **Submit** to save the created folder.

This section describes how to use the OSS console to search for objects with the same name prefix in a bucket or folder.

When you perform search by name prefix, the search string is case-sensitive and cannot contain the forward slash (/). The search range is limited to the root level of the current bucket or the objects in the current folder (not including subfolders and objects in them). For details about how to use the forward slash (/) on OSS, see View the object list.

Operation procedure

Go to the OSS console.

Click the target bucket to open the **Bucket Overview** page.

Click **Object** in the left-side navigation pane.

Enter the search prefix (for example, aliyun) in the search box, and press **Enter** or click **Search**. The system lists the names of the objects and folders prefixed with “aliyun” in the root directory of the bucket.

To search in a folder, open the folder and enter a search prefix in the search box. The system lists the names of the objects and folders matching the search prefix in the root directory of the folder.

After you upload an object to a bucket, you can get the file address used to share and download the file.

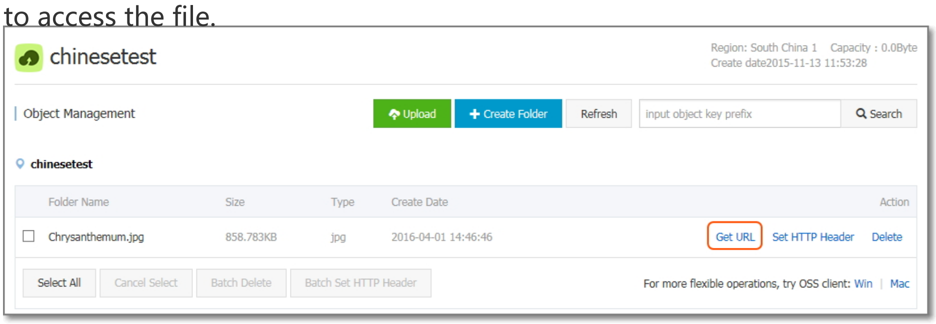
Operation procedure

Go to the OSS console.

Click the target bucket name to open the **Bucket Overview** page.

Click **Object** in the left-side navigation pane.

Click the **Get URL** link of the target object. A dialog box is displayed, showing the URL used to access the file.

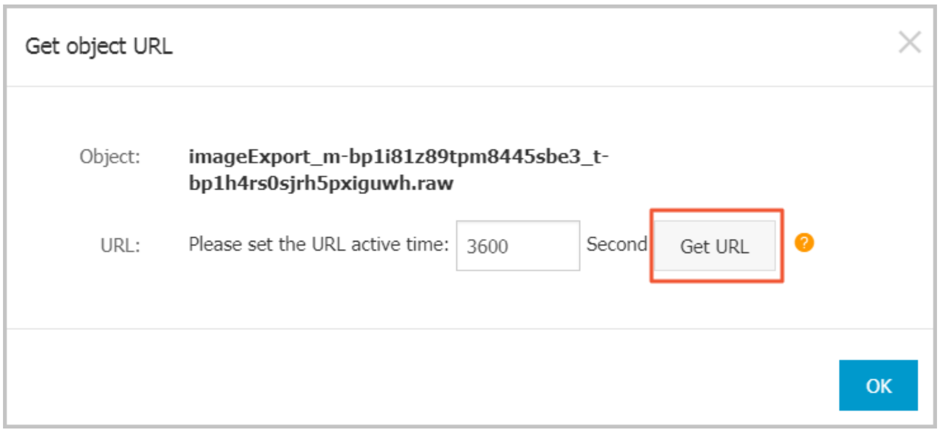


Region: South China 1 Capacity : 0.0Byte
Create date2015-11-13 11:53:28

Folder Name	Size	Type	Create Date	Action
□ Chrysanthemum.jpg	858.783KB	jpg	2016-04-01 14:46:46	Get URL Set HTTP Header Delete

For more flexible operations, try OSS client: Win | Mac

If your bucket is set to **Private** read/write, you must set the URL validity period (active time) when getting an object URL. Click **Get URL** to get the file link. The active time of an URL signature link is calculated based on NTP. You can give this link to any user, who can use it to access the file within the validity period. If the bucket is set to **Private** read/write, file addresses are generated using the URL signature method.



Object: imageExport_m-bp1i81z89tpm8445sbe3_t-bp1h4rs0sjrh5pxiguwh.raw

URL: Please set the URL active time: 3600 Second

Copy the file link and give it to any user who needs to browse or download the file.

You can set an HTTP header for one or multiple files on the OSS console.

You can set an HTTP header for up to 1,000 files using the batch process on the OSS console.

- API: The object header is set through the Copy Object operation.
- SDK: The object header is set through the CopyObject method in the Java SDK-Object.

Procedure

Log on to the OSS console.

Select a bucket to open the **Bucket Overview** page.

Select **Objects** in the left-side navigation pane.

Click the **Edit** link of the target file.

To set an HTTP header for multiple fiiles, select the target files and click **Edit Selected**.

Complete the setting. For details about each field, see Header Field Definitions.

Click **OK** to save the setting.

If you do not need to store uploaded files any longer, delete them to avoid further fees. You can delete a single file or delete files in batches on the OSS console.

Note: The deleted file cannot be recovered. Perform this operation with caution.

You can delete up to 1,000 files at a time using the Batch Delete function of the OSS console. If you want to delete only the selected files or perform batch deletion in a larger volume, follow the procedures in API or SDK documents. For details, see the relevant sections of the Developer Guide.

- API: Delete Object and Delete Multiple Object
- SDK: **Deleting Objects** in the Java SDK-Object

Operation procedure

Go to the OSS console.

Select a bucket to open the **Bucket Overview** page.

Select **Object** in the left-side navigation pane.

Click the **Delete** link of the target file. The **Delete Object** dialog box is displayed.

Click **Confirm** to delete the file.

To delete files in batches, select the files to be deleted and click **Batch Delete**.

After you delete a folder on the OSS console, all files and sub folders in this folder are automatically deleted. If you want to retain the files, move them to other places before you delete the folder.

Operation procedure

Go to the OSS console.

Select a bucket to open the **Bucket Overview** page.

Select **Object** in the left-side navigation pane.

Click the **Delete** link of the target folder. The **Delete Folder** dialog box is displayed.

> **Note:** Deletion may fail if the folder contains too many files.

Click **Confirm** to delete the folder.

After logging on to the OSS console, you can click **Fragment** in the left-side navigation pane of a bucket to view or delete fragments produced in the bucket.

Fragments are mainly produced by multipart upload operations. For details, see Multipart Upload.