

Object Storage Service

Console User Guide

Console User Guide

Log on to OSS console

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, make sure that you have registered an Alibaba Cloud account. If you do not have an Alibaba Cloud account, the system prompts you to register an account when you activate OSS.

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.

Log on to the OSS Console with an RAM Sub-account

The Alibaba Cloud OSS console provides an intuitive operation interface. Along with the Alibaba Cloud account, you can also log on to the OSS console using a sub-account (RAM user).

Log on to the OSS console using a RAM sub-account as follows:

1. Create a RAM user
2. Authorize a sub-account
3. Log on to the console with a sub-account

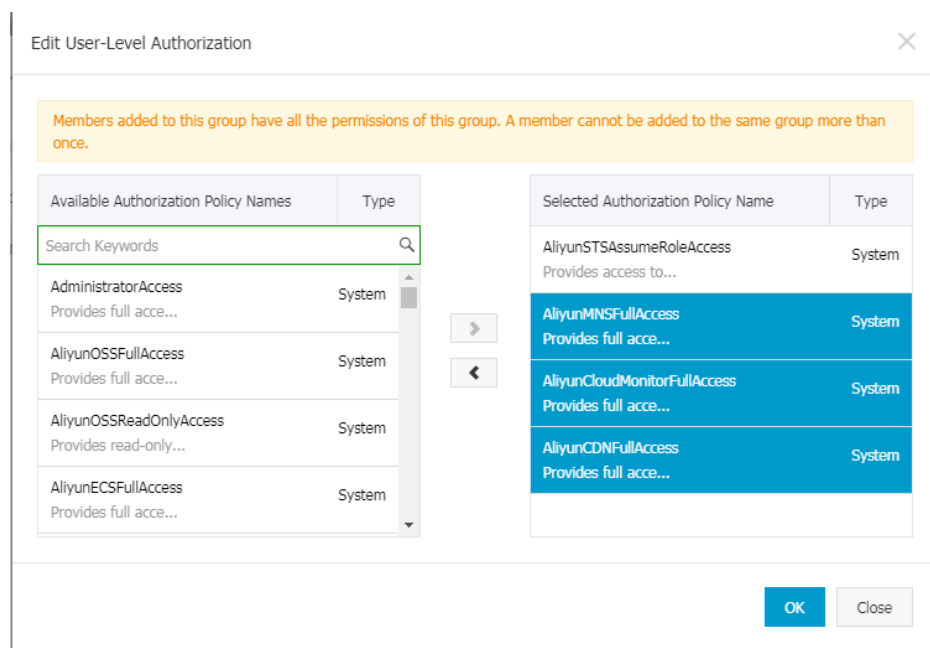
Create a RAM user

Log on to the RAM console, and create a RAM user through **User Management** > **New User**. For detailed procedure, see **Create a RAM user** in the RAM User Manual.

Authorize a sub-account

Log on to the RAM console, select the corresponding RAM user, and click **Authorize** for authorization. For detailed procedure, see RAM Authorization Help Documentation.

To make sure that the sub-account can use the OSS console features after logging on to the console, access permissions to MNS, CloudMonitor, and CDN are also required along with the related OSS permissions, as shown in the following figure:



Log on to the console with a sub-account

Do the following to logon to the console with a sub-account:

1. Log on to the RAM console, and click **User Management**.
2. Select the corresponding RAM user, and click **Manage** to configure related information.

3. Turn on **Enable Console Logon**.
4. Log on to the RAM console, view your **RAM user logon link**, and click the link to log on.

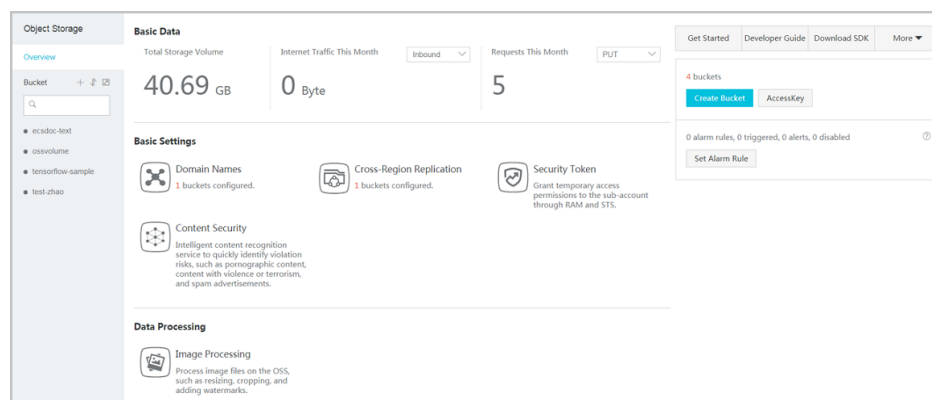
For more information, see RAM User Manual.

Manage buckets

Bucket overview

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, 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.



Create a bucket

Before uploading any files to the OSS, you must create a bucket to store files. You can specify the attributes of the bucket, including the region, access permission, and other metadata.

Procedure

Log on to the OSS console.

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

In the **Bucket Name** field, enter the bucket name.

The bucket name cannot be changed after the bucket is created.

The bucket name must comply with the naming conventions:

- The bucket name can contain only lower-case letters, digits, and hyphens (-).
- The bucket name must start and end with a lower-case letter or number.
- The bucket name must be at least 3 bytes and no more than 63 bytes in length.
- The bucket name must be unique across all existing bucket names in OSS.

In the **Region** drop-down box, select the data center of the bucket.

The region cannot be changed after the subscription. To access the OSS over the intranet of the ECS, select the same region with your ECS instance. For more information, see [Endpoint](#).

For **Storage Class**, select the storage type as needed.

Standard storage: provides highly reliable, highly available, and high-performance object storage services that support frequent data accesses.

Infrequent access: suitable for data that is stored for a long term and infrequently accessed. Its unit price is lower than that of the standard type. This storage class requires a minimum storage duration for the files. Charges are incurred if you delete files that are stored for less than 30 days. This storage class requires a minimum billable size for files. Files smaller than 128 KB are charged for 128 KB and data retrieval may cause a certain cost.

Archive storage: suitable for storing archival data that requires long-term persistence (more than half a year). The data is infrequently accessed during the storage period and restoring the data to a readable state may take one minute. It is suitable for storing archival data, medical images, scientific materials, and video footages for long-term persistence.

For **ACL**, select the expected permission for the bucket.

Private: Only the owner of the bucket and the authorized users can perform read, write, and delete operations on the objects in the bucket. Other users cannot access objects in the bucket.

Public Read: Only the owner of the bucket and the authorized users can perform write and delete operations on the objects in the bucket. Anyone (including anonymous access) can read the objects in the bucket.

- **Public Read/Write:** Anyone (including anonymous access) can read, write, and delete the objects in the bucket. The fees incurred by such operations are borne by the owner of the bucket. Use this permission with caution.

Click **OK**.

Delete a bucket

If you do not need a bucket, delete it to avoid further charges.

Prerequisite

To delete a bucket, make sure all objects in it are deleted, including parts generated by incomplete multipart upload. Otherwise, you are unable to delete the bucket.

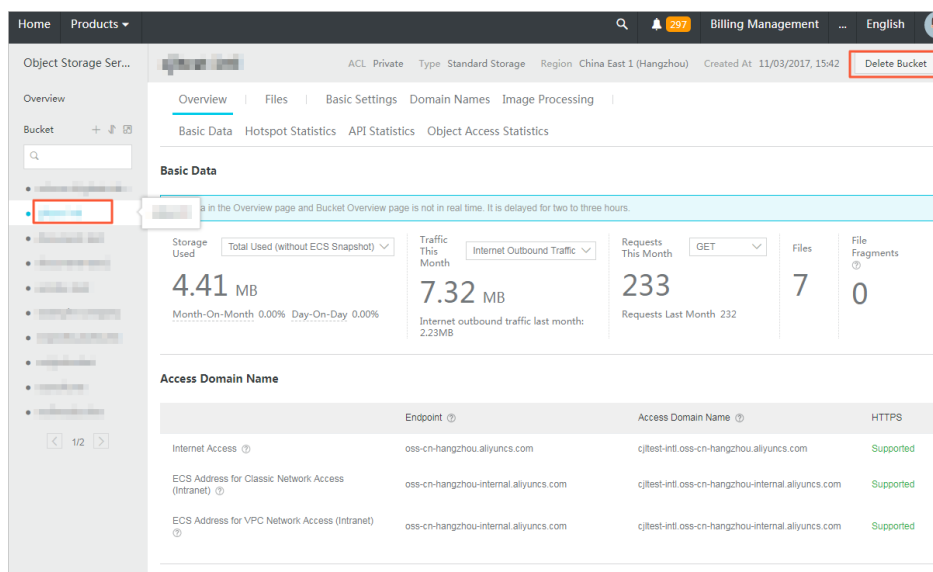
Note:

- If you want to delete all objects in a bucket, we recommend that you use **Lifecycle Management**.
- For detailed procedures on how to delete parts, see **Manage Parts**.

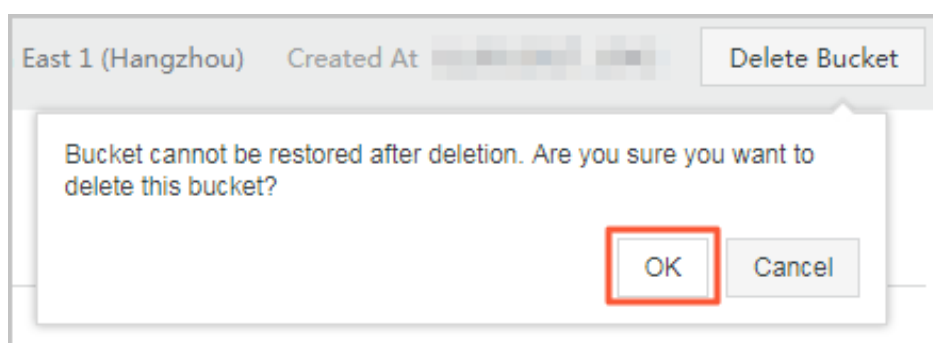
Procedure

Log on to the OSS console.

In the bucket list on the left, click the name of the target bucket, and then click **Delete Bucket** in the upper-right corner, as shown in the following figure:



In the dialog box that appears, click **OK**, as shown in the following figure:



Note: A deleted bucket cannot be recovered. Therefore, delete buckets with caution.

Change bucket ACL

OSS provides an Access Control List (ACL) for permission control. You can configure an ACL when creating a bucket and change the ACL after the bucket is created. If you do not configure an ACL for a bucket, the default ACL of the bucket is **Private**.

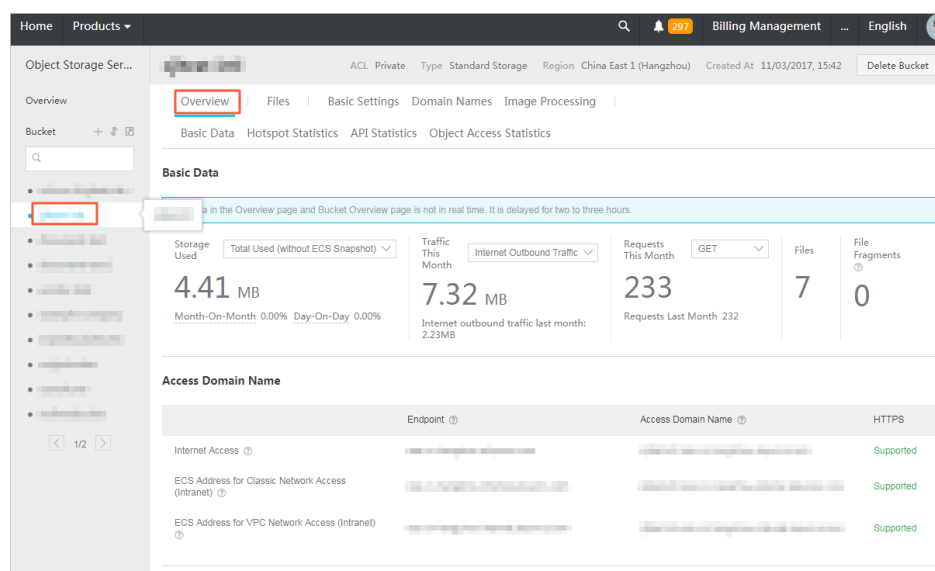
OSS ACL provides bucket-level access control. Currently, three access permissions are available for a bucket:

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

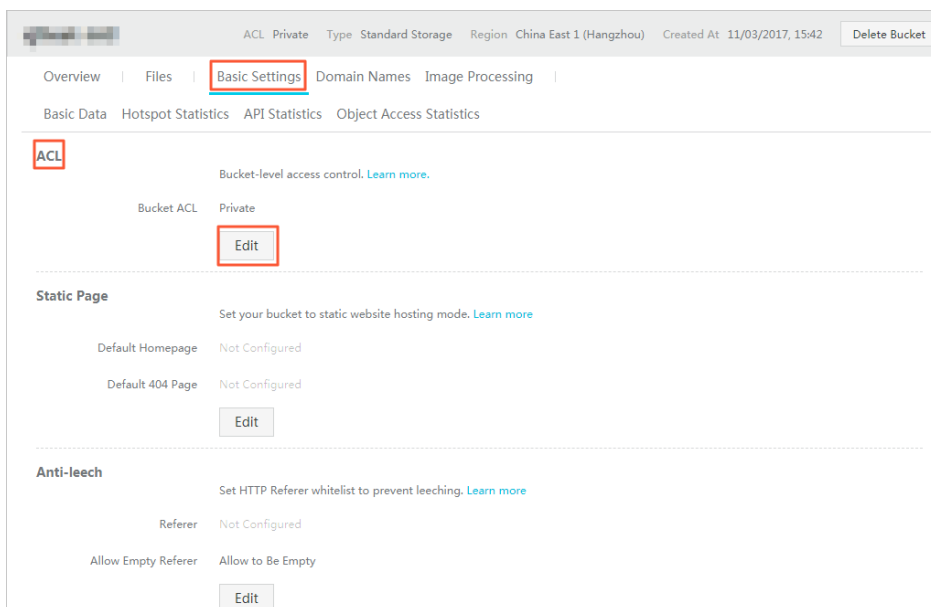
Procedure

Log on to the OSS console.

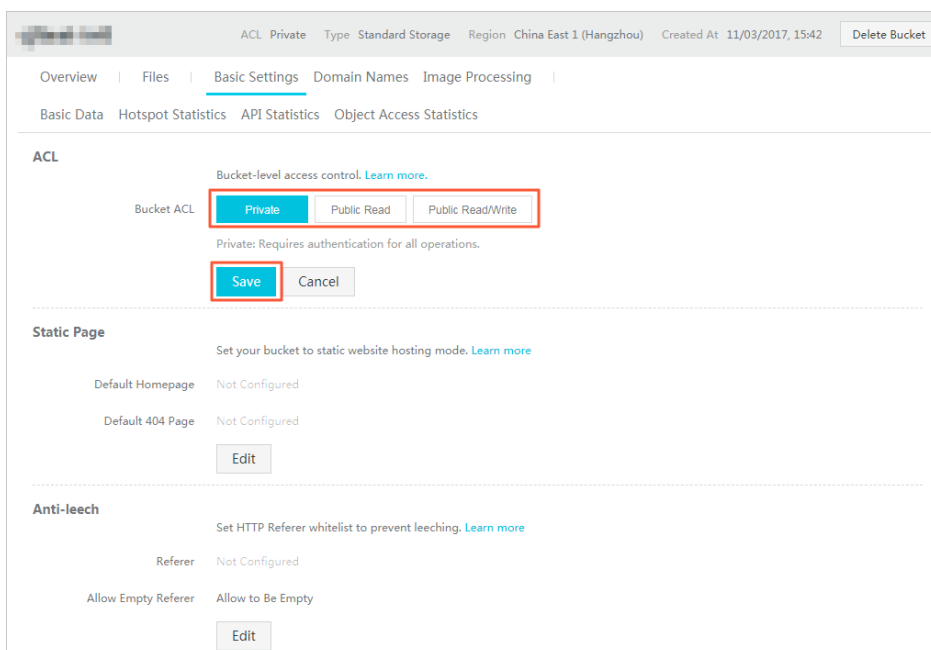
On the bucket list on the left, click the target bucket to open the overview page of the bucket, as shown in the following figure:



Click the **Basic Settings** tab, and click **Edit** in the **ACL** area, as shown in the following figure:



Select an ACL option for the bucket, and click **Save**, as shown in the following figure:



Host a static website

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

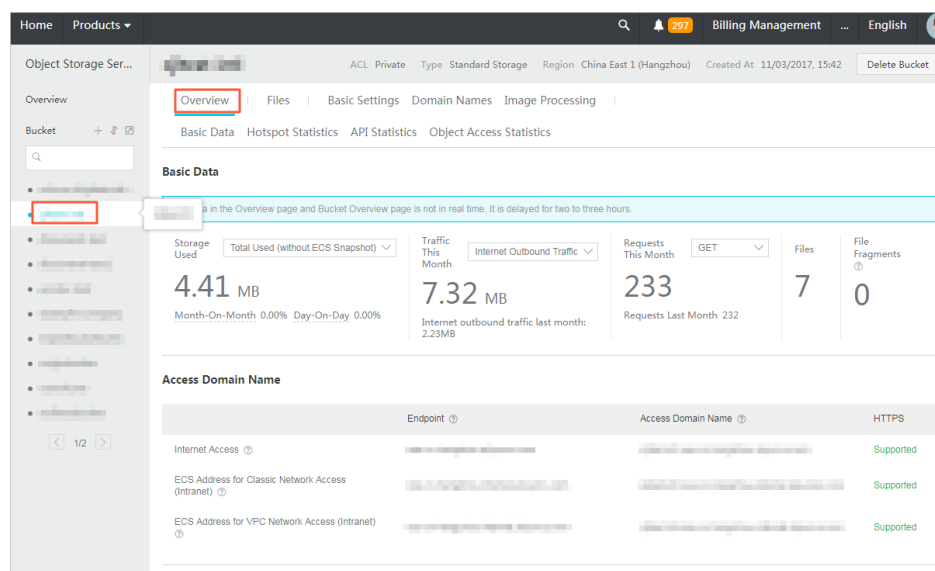
- If the default webpage is blank, static website hosting is disabled.
- If static website hosting is enabled, we recommend that you use CNAME to bind your domain name.
- If you directly access the static website root domain or any URL ending with "/" under this domain, the default homepage is returned.

For more information, see [Static Website Hosting](#).

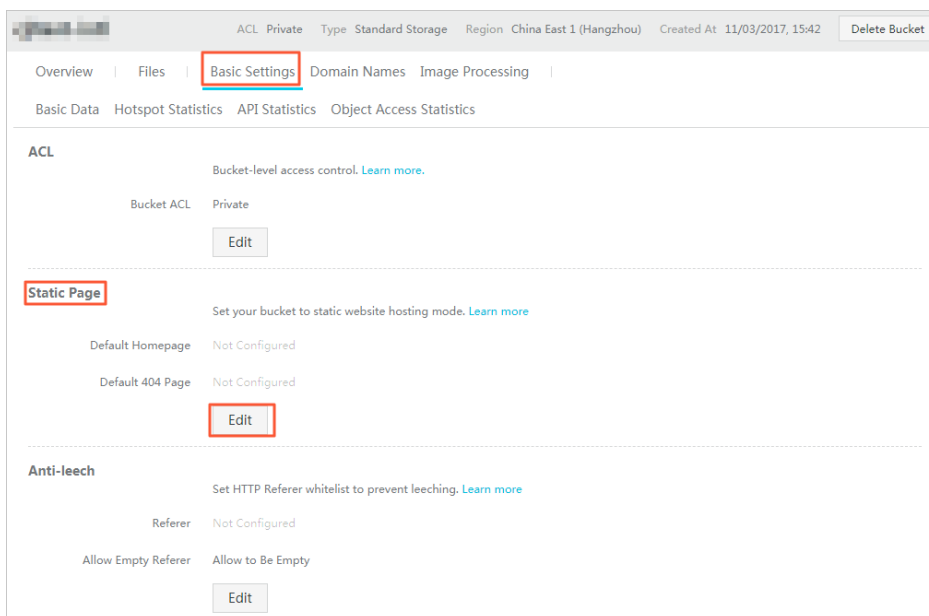
Procedure

Log on to the OSS console.

Select the target bucket to open the bucket overview page, as shown in the following figure:



In the **Basic Settings** tab, find the **Static Page** area and click **Edit**, as shown in the following figure:



Enter the following information and click **Save**, as shown in the following figure:

The screenshot shows a 'Static Page' configuration dialog box. It has a title 'Static Page' and a subtitle 'Set your bucket to static website hosting mode. Learn more'. There are two input fields: 'Default Homepage' and 'Default 404 Page', both highlighted with red boxes. Below the 'Default Homepage' field, there is a text description: 'Enter the file name of the default webpage. Only the .html format object under the root directory is supported. If you do not enter a file name, the default homepage will be disabled.' Below the 'Default 404 Page' field, there is a text description: 'Enter the file name of the 404 error default webpage. Only the .html, .jpg, .png, .bmp, and .webp formats are supported. If you do not enter a file name, the 404 error default webpage will be disabled.' At the bottom of the dialog, there are two buttons: 'Save' (highlighted with a red box) and 'Cancel'.

- **Default Homepage:** The index page (equivalent to the website's index.html). Only HTML files that have been stored in the bucket can be used.
- **Default 404 Page:** 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.

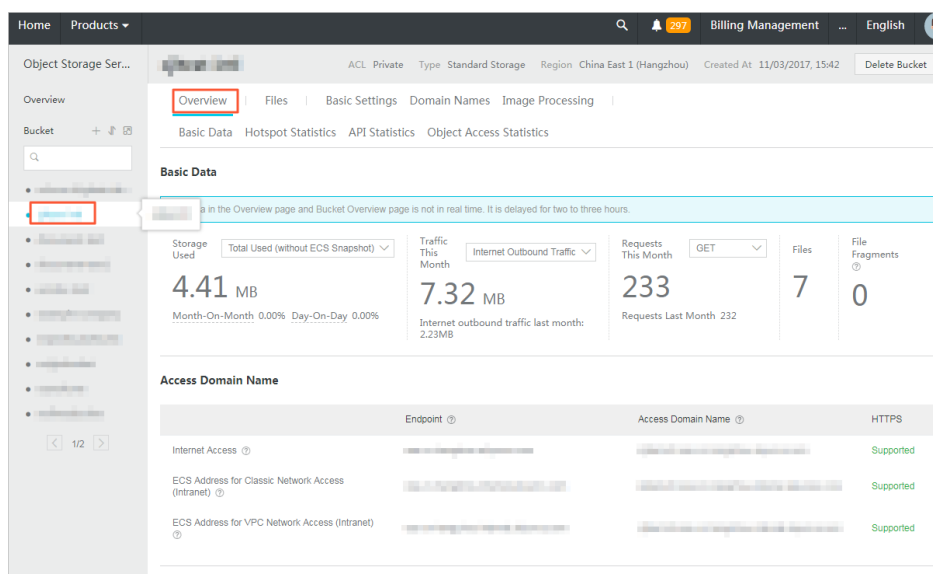
Set logging

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](#).

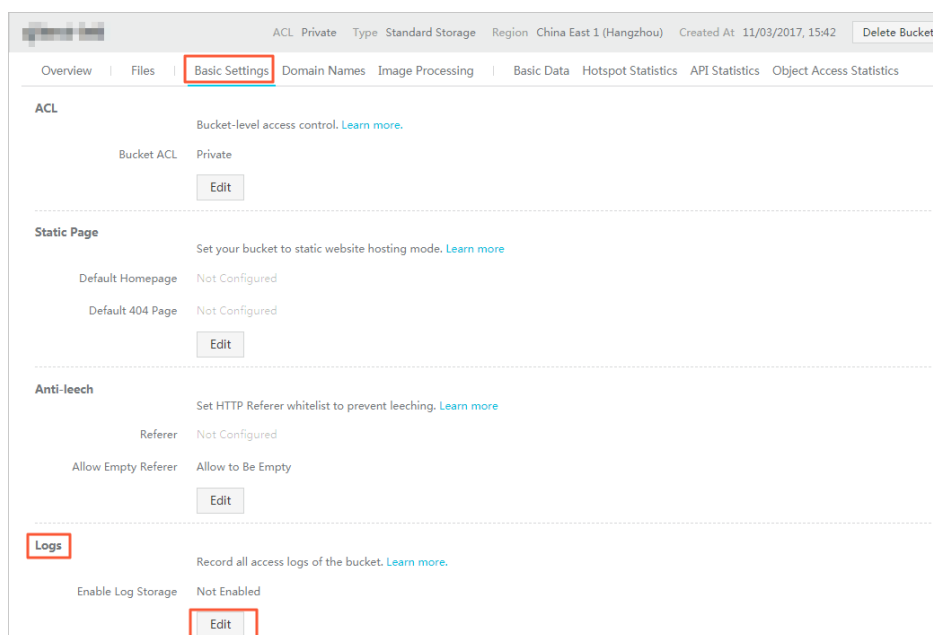
Procedure

Log on to the OSS console.

On the bucket list on the left, click the bucket you want to enable logging for to open the overview page of the bucket, as shown in the following figure:



Click the **Basic Settings** tab, and click **Edit** in the **Logs** area, as shown in the following figure:



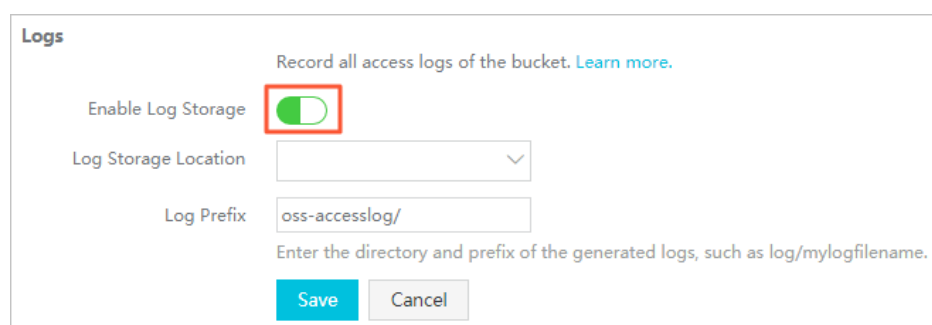
Edit the logging settings as follows:

If you do not want to store logs on OSS, disable the **Enable Log Storage** switch, as shown in the following figure:

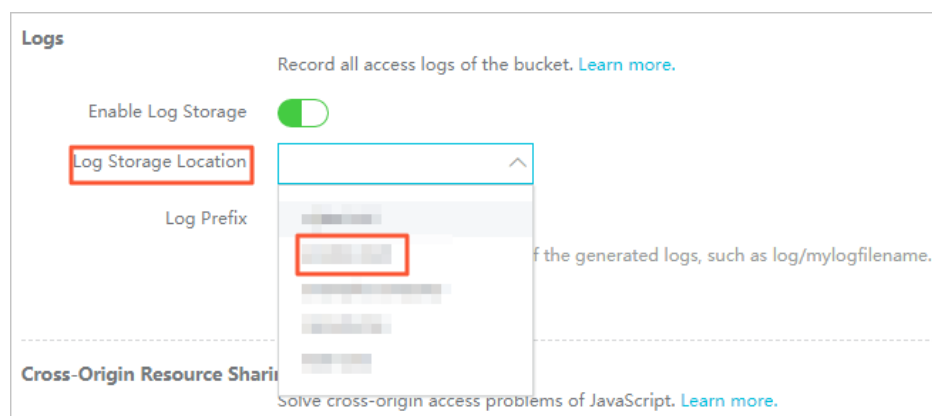


If you want to store logs on OSS, do as follows:

Enable the **Enable Log Storage** switch, as shown in the following figure:

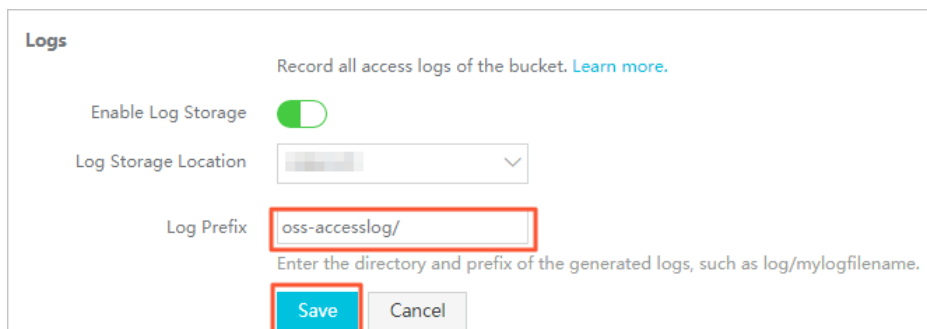


In the **Log Storage Location** drop-down box, select the name of a bucket to store the logs.



Note: Only buckets of the same user and region can be selected.

In the **Log Prefix** text box, use the default log prefix **oss-accesslog/** or enter another prefix (<TargetPrefix> described in the following logging naming conventions), and click **Save**, as shown in the following figure:



Logging naming conventions

The following is the naming conventions for access log records: <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, in which 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 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.

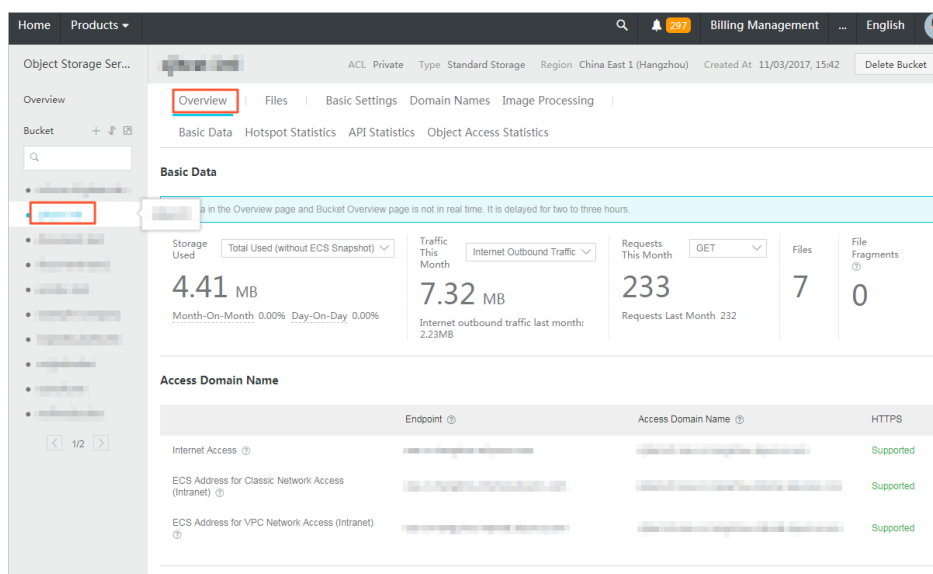
Set anti-leech

OSS is a Pay-As-You-Go service. To reduce extra fees caused in case your data on OSS is stolen by others, 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 access requests with an empty referer field.

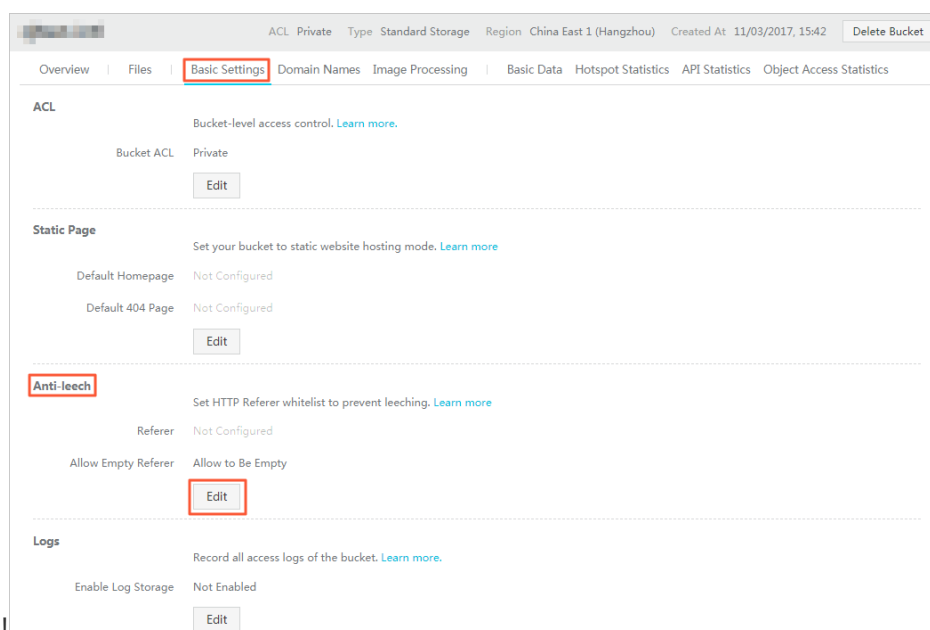
Procedure

Log on to the OSS console.

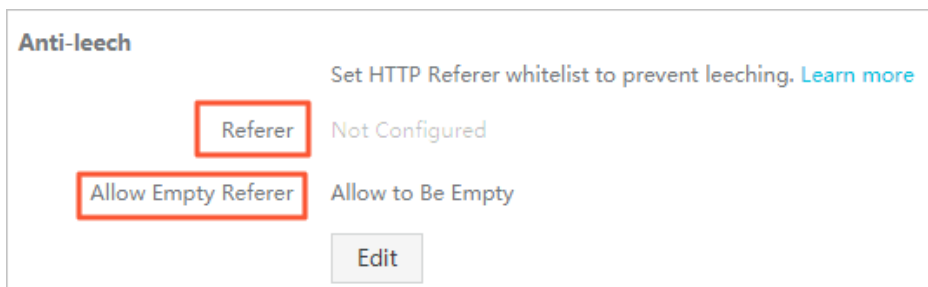
On the bucket list on the left, click the bucket you want to configure anti-leech to open the overview page of the bucket, as shown in the following figure:



Click the **Basic Settings** tab, and click **Edit** in the **Anti-leech** area, as shown in the following figure:



Enter the following information, and click **Save**, as shown in the following figure:



Anti-leech

Set HTTP Referer whitelist to prevent leeching. [Learn more](#)

Referer Not Configured

Allow Empty Referer Allow to Be Empty

Edit

- **Referer**: Add one or more URLs into the whitelist. Separate URLs with carriage returns.
- **Allow Empty Referer**: Configure whether to allow empty referers.

Example

Set the referer whitelist of a bucket named **test-1-001** to `http://www.aliyun.com`.

After the referer whitelist is set, only requests with a referer `http://www.aliyun.com` can access the objects in **test-1-001**.

Manage a domain name

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 guarantee 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 is not 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 uses 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.

On the left-side navigation pane, select a bucket from the bucket list to open the bucket overview page.

Click the **Domain Names** tab.

Click **Bind User Domain** to open the **Bind User Domain** dialog box.

Bind your domain.

- In the **User Domain** textbox, enter your domain name.
- If you need CDN acceleration, open the **Alibaba Cloud CDN** switch. For more information, see **CDN-based OSS acceleration**.
- If you want to add a CNAME record automatically, open the **Add CNAME Record Automatically** switch.

Note: If the domain name has completed cloud resolution under another Alibaba Cloud account, then a CNAME record cannot be automatically added for this domain name under your account. In this case, you must add a CNAME record manually. For more information, see the **Procedure for domain name resolution** section.

Click **Submit**.

Note: If the domain name you want to bind has been maliciously bound by another user, the system message **Domain name conflict** is displayed. 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. For detailed procedure, see the **Procedure for verifying domain name ownership** section.

Upload an HTTPS certificate

If you want your domain to access OSS through HTTPS, you must purchase an HTTPS certificate. You can purchase an HTTPS certificate from any certificate provider or from Alibaba Cloud Certificates Service (see [Certificate Service Quick Start](#)), and upload your certificate on the OSS console.

If Alibaba Cloud CDN is not enabled for OSS, you can upload your certificate on the OSS console:

- i. On the **Domain Names** tab page, click **Upload Cert** under **Action**.
- ii. On the **Upload Cert** page, enter your public key and private key, and then click **Upload**.

If Alibaba Cloud CDN is enabled for OSS, you must upload your certificate on the CDN console. For more information, see [HTTPS Security Acceleration](#).

Procedure for verifying domain name ownership

Click **Obtain TXT**. The system generates a TXT record based on your information.

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

In the OSS console, click **I have added the TXT verification file. Continue submission**. If the system detects that the TXT record value for this domain name is as expected, the domain name ownership passes verification.

Procedure for domain name resolution

1. Go to the Alibaba Cloud console.
2. From the left-side navigation pane, click **Alibaba Cloud DNS** to enter the domain name resolution list page.
3. Click the **Configure** link corresponding to the target domain name.
4. Click **Add Record**.
5. In the **Add Record** dialog box, select **CNAME** from the **Type** drop-down box, , and enter the Internet domain name of the bucket in the **Value** text box.
6. Click **Confirm**.

Set Cross-Origin Resource Sharing (CORS)

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.

Procedure

Log on to the OSS console.

In the left-side navigation pane, select the target bucket to open the bucket overview page.

Click **Basic Settings**.

In the **Cross-Origin Resource Sharing (CORS)** area, click **Edit**.

In the cross-origin access page, click **Create Rule**.

In the **Cross-Origin Rules** dialog box, configure the following items:

Source: Indicates the origins allowed for cross-origin requests. Multiple matching rules are allowed, which are separated by a carriage return. Only one wildcard (*) are allowed for each matching rule.

Allowed Methods: Indicates the allowed cross-origin request methods.

Allowed Headers: Indicates the allowed cross-origin request headers. Multiple matching rules are allowed, which are separated by a carriage return. Only one wildcard (*) are allowed for each matching rule.

Exposed Headers: Indicates the response headers that 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.

Note: A maximum of 10 rules can be configured for each bucket.

Click **OK** to save this rule.

Set lifecycle

You can define and manage the lifecycle of all or a subset of objects in a bucket by specifying a key name prefix in the console. Lifecycle rules are generally applied to operations such as batch file management and automatic fragment deletion.

- For objects that match such a rule, the system makes sure that data is purged or converted to another storage type within two days of the effective date.
- Data deleted in batch based on a lifecycle rule can never be restored, so use caution when configuring such a rule.

Procedure

Log on to the OSS console.

In the left-side bucket list, click the name of the target bucket to open the overview page of the bucket.

Click the **Basic Settings** tab, locate the **Lifecycle** area, and then click **Edit**.

Click **Create Rule** to open the **Create Lifecycle Rule** dialog box.

Configure the lifecycle rule.

Status: Specify the status of the rule, whether it is enabled or disabled.

Policy: Select an object matching policy. You can select either **Match by Prefix** (matching by object name prefix) or **Apply to Bucket** (matching all objects in the bucket).

Prefix: If you select **Match by Prefix** for the **Policy**, enter the prefix of the object

name. For example, you have stored some image objects in a bucket, and the names of these objects are prefixed with **img/**. To perform lifecycle management on these objects, enter **img/** in this field.

Delete File

- **Expiration Period:** Specify the number of days for which an object file is retained since it was last modified. Once the period expires, the system triggers the rule and deletes the file or converts it to another storage type (Infrequent Access or Archive). For example, if it is set to 30 days, objects last modified on January 1, 2016 are scanned and deleted or converted to another storage type by the backend program on January 31, 2016.

Configuration options include:

- Transition to IA after specified days
- Transition to Archive after specified days
- Delete all objects after specified Days

Expiration date: Delete all the files that were last modified before the specified date or convert them to another storage type (Infrequent Access or Archive). For example, if it is set to 2012-12-21, objects last modified before this date are scanned and deleted or converted to another storage type by the backend program. Configuration options include:

- Transition to IA after specified date
- Transition to Archive after specified date
- Delete files before specified date

Not Enabled: Disable auto-deletion of files or storage type conversion.

Delete Fragments

Expiration Period: Specify the number of days for a multipart upload event is retained since it was initialized. Once the period expires, the system triggers the rule and deletes the event. For example, if it is set to 30 days, events initialized on January 1, 2016 are scanned and deleted by the backend program on January 31, 2016.

Expiration date: Delete all multipart upload events initialized before the specified date. If it is set to 2012-12-21, the upload events initialized before this date are scanned and deleted by the backend program.

- **Note Enabled:** Disable auto-deletion of fragments.

Click **OK**.

Note: After a lifecycle rule is saved successfully, you can view, edit, or delete it in the policy list.

Set cross-region replication

Currently, cross-region replication supports the synchronization of buckets with different names. If you have two buckets belonging to different regions, you can enable the cross-region replication feature in the console to synchronize data from the source bucket to the target bucket.

Note: Currently, the cross-region replication feature is only supported between different regions in Mainland China and between Eastern and Western United States. It is not supported in other regions currently.

Procedure

Log on to the OSS console.

In the left-side bucket list, click the name of the target bucket to open the overview page of the bucket.

Click the **Basic Settings** tab, and locate the **Cross-region Replication**.

Click **Enable Synchronization** to open the **Cross-region Replication** dialog box.

Select the region and name of the target bucket.

Note:

- The two buckets for data synchronization must belong to different regions. Data synchronization is unavailable between buckets in the same region.
- The two buckets with cross-region replication enabled cannot have a synchronization relationship with any other buckets.

Select the **Data Synchronization Object**.

- **Synchronize all files:** Synchronize all the files in the bucket to the target bucket.
- **Synchronize files with specific prefixes:** Synchronize files with specific prefixes in the bucket to the target bucket. Up to 10 prefixes can be added.

Select the **Data Synchronization Policy**.

- **Full synchronization (add/delete/change)**: Synchronize all the data in the bucket to the target bucket, including added, changed, and deleted data.
- **Write synchronization (add/modify)**: Synchronize only the added and changed data in the bucket to the target bucket.

Choose whether to **Synchronize Historical Data**.

Note: During the synchronization of historical data, objects replicated from the source bucket may overwrite the objects with the same names in the target bucket. Therefore, check the data consistency before replication.

Click **OK**.

Note:

- After the configuration is complete, it may take three to five minutes for cross-region replication to be enabled. Synchronization-related information is displayed after the bucket synchronization.
- Since the cross-region replication of a bucket is asynchronous, it usually takes several minutes or hours to copy data to the target bucket, depending on the size of data.

Set back-to-origin rules

You can set back-to-origin rules to define whether to retrieve origin data by mirroring or redirection. Back-to-origin rules are usually used for hot migration of data and redirection of specific requests. You can configure up to five back-to-origin rules, which is executed by the system in sequence.

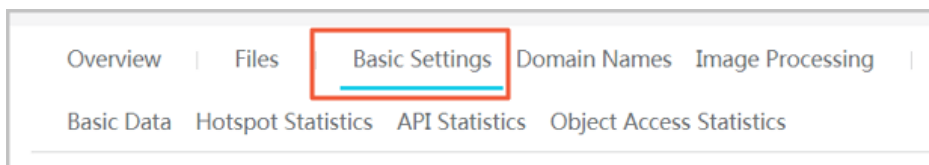
Note: Back-to-origin does not support intranet endpoint. For more information on traffic fees, see [Pricing](#).

Procedure

Log on to the OSS console.

Click to open the target bucket.

Click the **Basic Settings** tab.



In the **Back-to-Origin** area, click **Edit**.

Click **Create Rule**.

In the **Back-to-Origin Type** area, select **Mirroring** or **Redirect**.

When **Mirroring** is configured, if a requested file is not found on OSS, it is automatically retrieved from the source site, saved to the OSS, and the content is returned to the user.

When **Redirect** is configured, the requests that meet the response condition are returned to the redirected URL through HTTP redirection. A browser or client then obtains the content from the source site.

Click **OK** to save the rule.

Note: After the rule is successfully saved, you can view the configured rule in the rule list and perform corresponding **Edit** or **Clear** operations.

Manage objects

Overview

In OSS, the basic data unit for user operations is an object. The size of a single object is limited to

48.8 TB. An infinite number of objects can exist in a single bucket.

After you create a bucket in a region, the objects uploaded to the bucket are retained in this region, unless you transmit the objects to another region on purpose. Objects stored in an Alibaba Cloud OSS region are physically retained in this region. OSS does not retain copies or move the objects to any other region. However, you can access these objects from anywhere if you have permissions.

You must have the write permission to the bucket before uploading an object to OSS. In the console, the uploaded objects are displayed as files or folders to users. This section describes how to create, manage, and delete files and folders using the console.

Upload objects

After you create a bucket, you can upload objects (files) to the bucket in either of the following ways:

You can upload the object smaller than 5 GB by using the OSS console.

You can upload the object larger than 5 GB by using SDKs or APIs. For more information, see [Multipart upload](#).

This topic describes how to upload objects by using the OSS console.

Note: If the name of the object to be uploaded is duplicate with that of the existing one in the bucket, it overwrites the existing one.

Procedure

Log on to the OSS console.

Click the name of the bucket which you want to upload objects to, and then click the **Files** tab.

Click **Upload**.

In the **Directory Address** box, set the directory for the objects to be uploaded.

Current Directory: If you select this option, the objects will be uploaded to the

current directory.

Specify Directory: If you select this option, enter the directory such as **photos**. Then OSS will automatically create a folder named **photos** and upload the objects to it.

Note: You can also create a folder manually. For more information, see [Create a folder](#).

In the **File ACL** area, select the read/write permissions of the objects to be uploaded.

- **Inherited from Bucket:** By default, the read/write permissions of the objects are inherited from the bucket which the objects are uploaded to.

Private: Only the owner of the bucket and the authorized users can perform read, write, and delete operations on the objects. Other users cannot access the objects.

Public Read: Only the owner of the bucket and the authorized users can perform write and delete operations on the objects. Anyone (including anonymous access) can read the objects.

- **Public Read/Write:** Anyone (including anonymous access) can read, write, and delete the objects. The fees incurred by such operations are borne by the owner of the bucket. Use this permission with caution.

Drag one or multiple objects to be uploaded to the **Upload** area, or click **upload them directly** to select the objects to be uploaded.

Object naming conventions

Object names must comply with the naming conventions:

- Object names must use UTF-8 encoding.
- Object names must be at least 1 byte and no more than 1023 bytes in length.
- Object names cannot start with a backslash (/) or a forward slash (\).
- Object names are case sensitive.

Create a folder

Alibaba Cloud OSS does not have the term **folder**. All elements are stored as objects. To use a folder in

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. In 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 more information about how to create and use simulated folders, see [API - Get Bucket](#) and [Folder Simulation in Java SDK- Object](#).

Procedure

Log on to the OSS console.

Click to open the target bucket.

Select the **Files** tab.

Click **Create Directory**.

Enter a directory name.

Click **OK**.

Search for objects

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 more information about how to use the forward slash (/) on OSS, see [View the object list](#).

Procedure

Log on to the OSS console.

Click to open the target bucket.

Click **Files**.

Enter the search prefix, such as **abc**, in the search box, and press **Enter** or click the search icon. The system lists the names of the objects and folders prefixed with **abc** 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.

Change object ACL

OSS provides an Access Control List (ACL) for permission control. You can configure an ACL when uploading a file and change the ACL after uploading the file. If no ACL is configured, the default value is Private.

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

Private: Only the creator of the bucket can perform read and write operations on the files in the bucket. Other users cannot access those files.

If the read and write permissions of the bucket are "Private" , you must set a **link validity period** when obtaining the file access URL.

The validity period for URL signature links is calculated based on NTP. You can give this link to any visitor who can then use it to access the file within the validity period. If the bucket has a private permission, the obtained addresses are generated using the URL signature method.

Public Read: Only the owner of the bucket can perform write operations on the files in the bucket. Anyone (including anonymous visitors) can perform read operations on the files.

- **Public Read/Write:** Anyone (including anonymous visitors) can perform read and write

operators on the files in the bucket. Use this permission with caution because the fees incurred by these operations are borne by the owner of the bucket.

Procedure

Log on to the OSS console.

In the left-side bucket list, click the name of the target bucket to open the overview page of the bucket.

Click the **Files** tab.

Click the name of the target file to open the **Preview** page of the file.

Click **Set ACL** to change the read and write permissions of the file.

- If the read and write permissions of the bucket are **Private**, you must set a link validity period when obtaining the file access URL.
- On the **Preview** page of the target file, enter a link validity period (in seconds) in the **Signature** field.

Click **OK**.

Get object URL

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

Procedure

Log on to the OSS console.

Click to open the target bucket.

Click the **Files** tab.

Click the name of the target file.

The **Preview** page is displayed.

Copy File URL: used to download the file.

Copy File Path: used to search a file or watermarking an image file.

Click **Copy File URL** and give it to any user who needs to browse or download the file.

If the ACL of your bucket is set to **Private**, you must set the **Validity** in the **Signature** field when getting a file URL. The default value of **Validity** is 3600 seconds, and the maximum value is 64800 seconds.

Note:

- The link validity period for URL signature is calculated based on NTP. You can give this link to any visitor who can then use it to access the file within the validity period. If the bucket has a private permission, the obtained addresses are generated by **adding a signature to URL**.
- You can change the ACL of a bucket or a file anytime. For more information, see [Change bucket ACL](#) and [Change object ACL](#).

Set an HTTP header

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 **CopyObject** operation.
- SDK: The object header is set through the **CopyObject** method in Java SDK - **Manage objects**.

Procedure

Log on to the OSS console.

Click to open the target bucket.

Click **Files**.

Select one or multiple files, and then click **Set HTTP Header**.

You can also click one file name and then click **Set HTTP Header** on the **Preview** page.

Enter the values. For more information about each field, see [Definitions of common HTTP headers](#).

Click **OK**.

Delete an object

If you do not need to store uploaded files any longer, delete them to avoid further fees. You can delete a single file or multiple files 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 on the 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 more information, see the relevant sections of the [Developer Guide](#).

- API: [Delete Object and Delete Multiple Objects](#)
- SDK: [Delete multiple objects](#) in Java SDK - Manage objects

Procedure

Log on to the OSS console.

Click to open the target bucket.

Click **Files**.

Select one or multiple files, and then click **Delete**.

Click **OK**.

Delete a folder

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.

Procedure

Log on to the OSS console.

Click to open the target bucket.

Click **Files**.

Select the target folder, and then click **Delete**.

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

Click **OK** to delete the folder.

Manage fragments

What are parts?

When you use the Multipart Upload mode, you divide the object into several parts. After you upload the parts to the OSS server, you can call the CompleteMultipartUpload to combine the parts into a complete object.

Note:

You can call the CompleteMultipartUpload to combine the parts into a complete object. For more information on how to use MultipartUpload, see **Multipart Upload**.

You can regularly clear unnecessary parts by setting the lifecycle management. It is used to clear the parts for which the CompleteMultipartUpload is not complete for a long term in the bucket to reduce the consumption of space. For the detailed procedure, see [Set the Lifecycle](#).

A part cannot be read before it is combined with other parts into an object. To delete a bucket, you must delete its objects and parts first. Parts are mainly generated by Multipart Upload. For more information, see the [Multipart Upload API documentation](#).

Procedure

Log on to the OSS console.

In the left-side bucket list, click the name of the target bucket to open the overview page of the bucket.

Click the **File Management** tab.

Click the **Part Management** to open the **Part Management** page.

Delete the part files.

- To delete all the part files in a bucket, click **Clear**.
- To delete some of the part files in a bucket, select or search for the expected part files and click **Delete**.

In the dialog box that appears, click **OK**.

Check resource usage

Overview

You can check the usage of the following resources on the OSS console:

- **Basic data:** Including bucket, data used, and requests per hour

- **Hotspot statistics:** Including PV/UV, original, and hot spot
- **API statistics:** Including method statistics and return code
- **Object access statistics:** Including statistics about object access

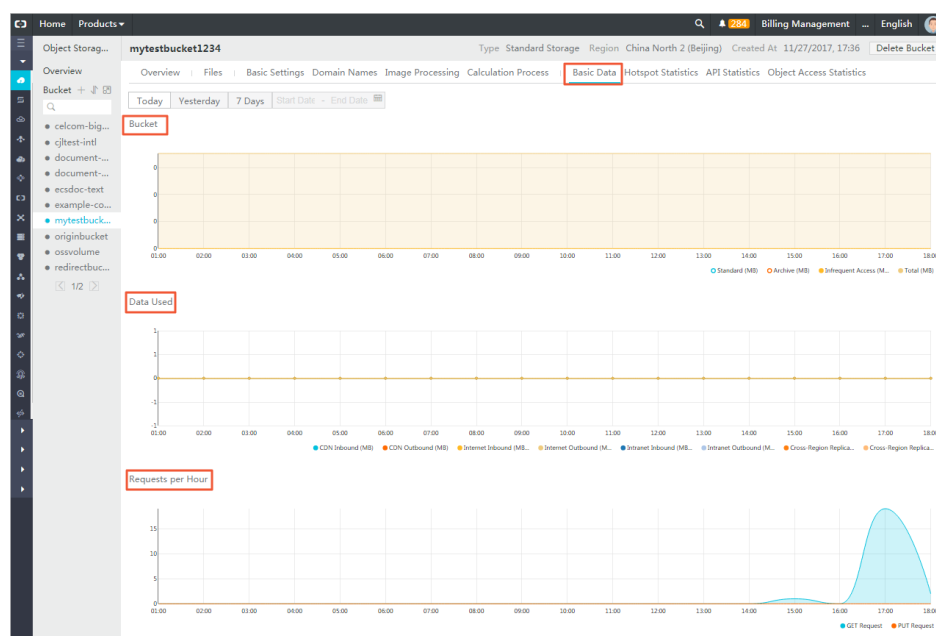
This document uses the **basic data** as an example to describe the resource checking method.

Procedures

Log on to the OSS Console.

In the bucket list on the left, click the target bucket name to open its information page.

Click the **Basic Data** tab, and diagrams of the following three kinds of basic data are displayed, as shown in the following figure:



- Bucket
- Data Used
- Requests per Hour

The following three tables describe the basic data items included in the three diagrams and the description of the items:

Bucket

Basic Data	Description
Standard	Size of data stored in the standard type
Archive	Size of data stored in the archive type

Infrequent Access	Size of data stored in the infrequent access type
Total	Total size of data

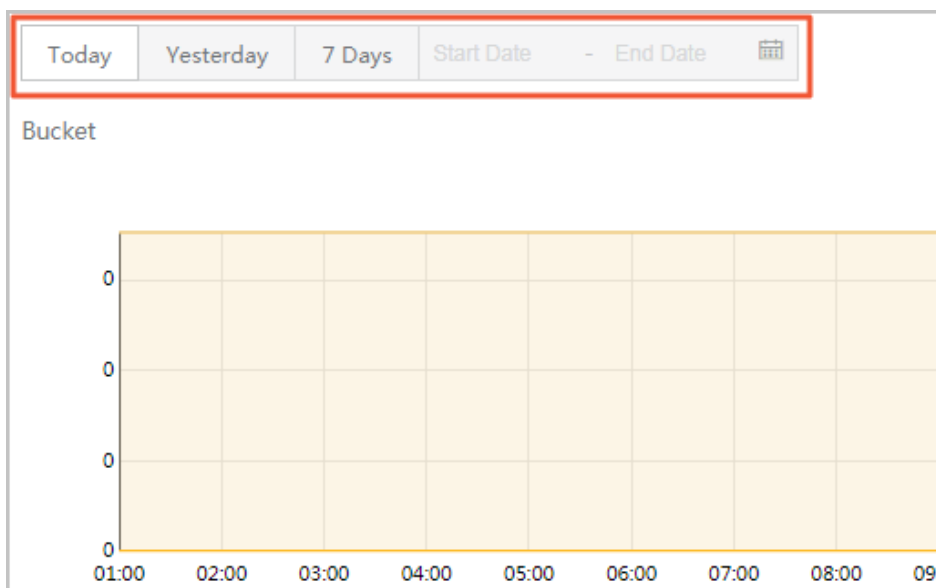
Data Used

Basic Data	Description
CDN Inbound	Data uploaded from local to OSS through CDN service layer
CDN Outbound	Data downloaded from OSS through CDN service layer
Internet Inbound	Data uploaded from local to OSS through Internet
Internet Outbound	Data downloaded from OSS to local through Internet
Intranet Inbound	Data uploaded from ECS servers to OSS through Alibaba intranet
Intranet Outbound	Data downloaded from OSS to ECS servers through Alibaba intranet
Cross-Region Replication Inbound	Data synchronously replicated from the target bucket to the source bucket using the cross-region replication function
Cross-Region Replication Outbound	Data synchronously replicated from the source bucket to the target bucket using the cross-region replication function

Request per Hour

Basic Data	Description
GET Request	Number of GET requests per hour
PUT Request	Number of PUT requests per hour

Select the time granularity of the resource usage diagrams, as shown in the following figure:



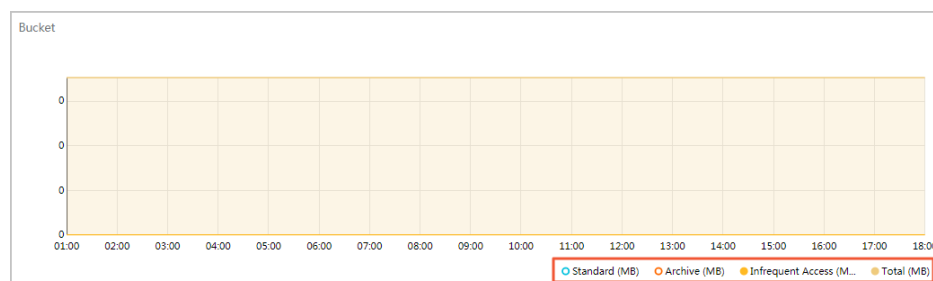
- **Today:** Only the data of the current day is shown in diagrams.
- **Yesterday:** Only the data of yesterday is shown in diagrams.
- **7 Days:** Only the data of the latest seven days is shown in diagrams.
- **Customized time period:** You can select the Start Date and the End Date of a time period. The data in this period is shown in diagrams.

Check the required basic data in the corresponding diagram. The following part uses the Bucket diagram as an example to describe the checking method of basic data.

The display status of a basic data item is shown on the lower right of a diagram.

- If the circle before a basic data item is empty, the basic data item is not shown in the diagram.
- If the circle before a basic data item is solid, the basic data item is shown in the diagram.

For example, in the following figure, the **Standard** and **Archive** data items are not shown in the diagram, and the **Infrequent Access** and **Total** data items are shown in the diagram.



Note: All data items are shown in diagrams by default.

By clicking the circle before a basic data item, you can switch between the following status:

- Show the basic data item in the diagram.
- Do not show the basic data item in the diagram.

By double-clicking the circle before a basic data item, you can switch between the following two status:

- Only show this basic data item in the diagram.
- Show all basic data items in the diagram.