

Alibaba Cloud Object Storage Service

Console User Guide

Issue: 20181008

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.








1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.
2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company, or individual in any form or by any means without the prior written consent of Alibaba Cloud.
3. The content of this document may be changed due to product version upgrades, adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.
4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults" and "as available" basis. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, special, or punitive damages, including lost profits arising from the use or trust in this document, even if Alibaba Cloud has been notified of the possibility of such a loss.
5. By law, all the content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade

secrets. No part of the Alibaba Cloud website, product programs, or content shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates).

6. Please contact Alibaba Cloud directly if you discover any errors in this document.

Generic conventions

Table -1: Style conventions

Style	Description	Example
	This warning information indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	 Danger: Resetting will result in the loss of user configuration data.
	This warning information indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	 Warning: Restarting will cause business interruption. About 10 minutes are required to restore business.
	This indicates warning information, supplementary instructions, and other content that the user must understand.	 Note: Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	 Note: You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
Bold	It is used for buttons, menus, page names, and other UI elements.	Click OK .
Courier font	It is used for commands.	Run the <code>cd /d C:/windows</code> command to enter the Windows system folder.
<i>Italics</i>	It is used for parameters and variables.	<code>bae log list --instanceid Instance_ID</code>
[] or [a b]	It indicates that it is a optional value, and only one item can be selected.	<code>ipconfig [-all -t]</code>
{ } or {a b}	It indicates that it is a required value, and only one item can be selected.	<code>swich {stand / slave}</code>

Contents

Legal disclaimer.....	I
Generic conventions.....	I
1 Log on to the OSS Console with an RAM Sub-account.....	1
2 Manage buckets.....	4
2.1 Bucket overview.....	4
2.2 Create a bucket.....	6
2.3 Delete a bucket.....	7
2.4 Change bucket ACL.....	7
2.5 Host a static website.....	8
2.6 Set anti-leech.....	9
2.7 Set a WORM strategy.....	9
2.8 Manage a domain.....	10
2.9 Set Cross-Origin Resource Sharing (CORS).....	13
2.10 Set lifecycle.....	14
2.11 Set cross-region replication.....	16
2.12 Set back-to-origin rules.....	17
3 Manage fragments.....	20
4 Log analysis.....	21
5 Log on to OSS console.....	24
6 Manage objects.....	25
6.1 Overview.....	25
6.2 Upload objects.....	25
6.3 Create a folder.....	26
6.4 Search for objects.....	27
6.5 Change object ACL.....	28
6.6 Use bucket policies to authorize other users to access OSS resources.....	29
6.7 Download an object.....	31
6.8 Set an HTTP header.....	33
6.9 Delete an object.....	33
6.10 Delete a folder.....	34
7 Check resource usage.....	35

1 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.

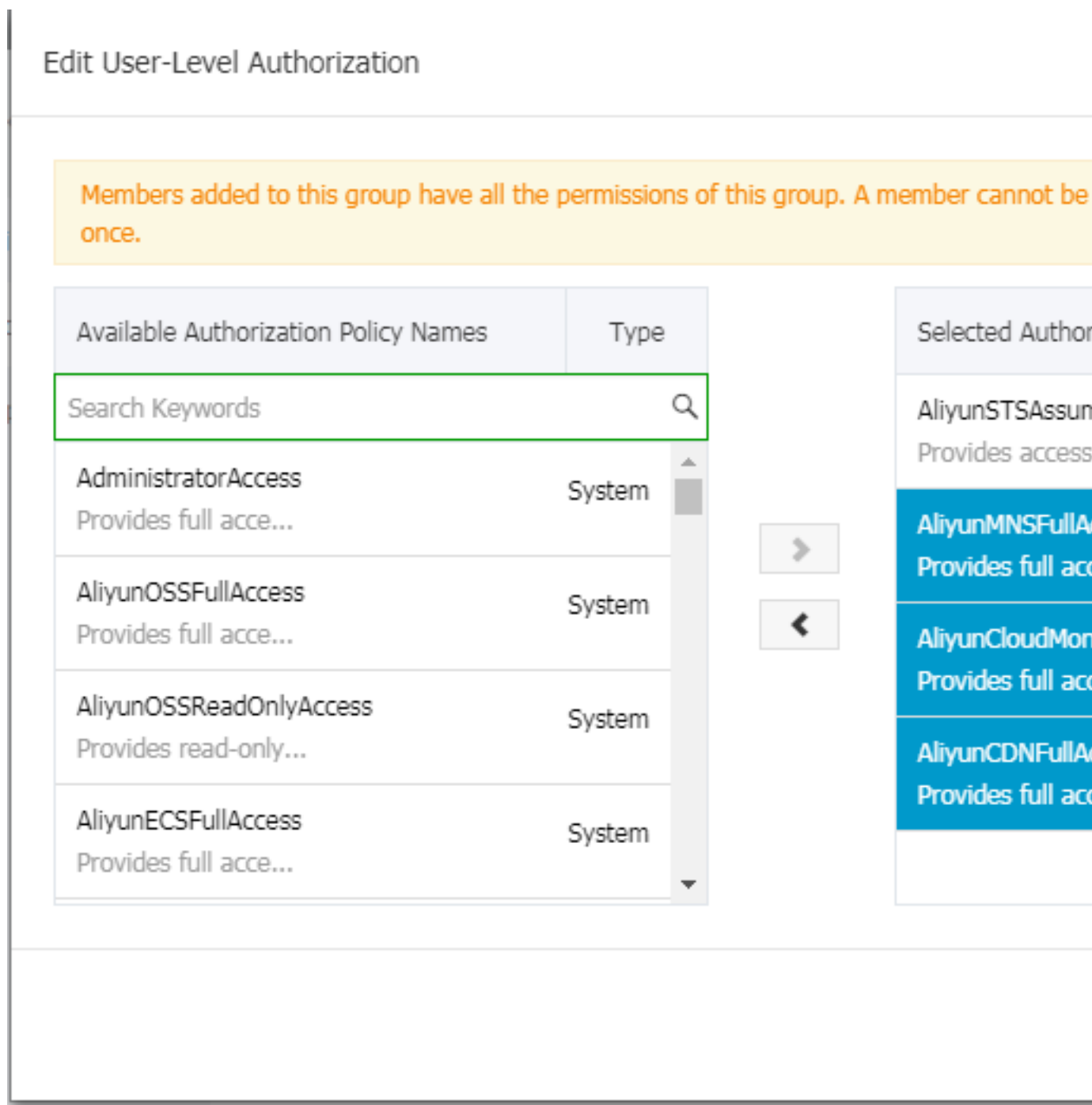
Create a RAM user

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

Authorize a sub-account

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

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 log on 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.

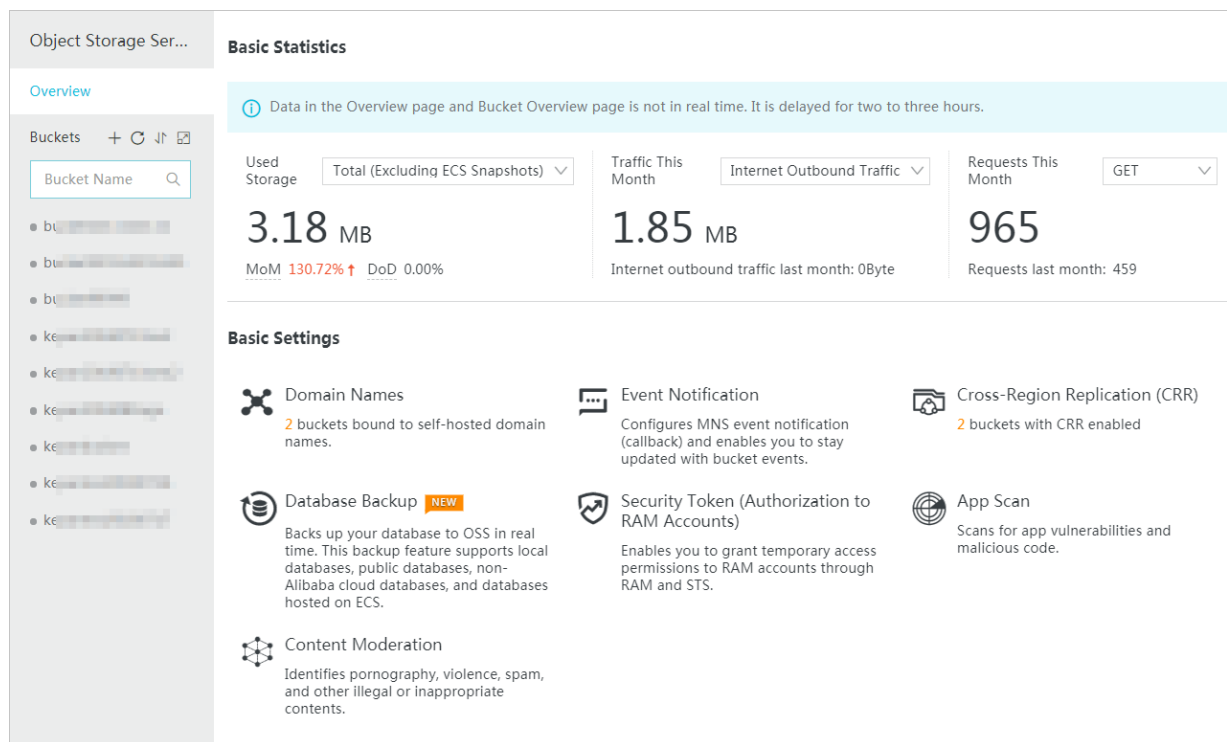
For more information, see .

2 Manage buckets

2.1 Bucket overview

All files of Alibaba Cloud OSS are stored in buckets. A bucket is a unit that allows you to manage stored files. Files in a bucket are stored in a non-hierarchical structure instead of a directory-based file system. You can set the attributes of a bucket to control the region, the ACL of stored files, and the life cycle of the stored files. These attributes apply to all files stored in the bucket. Therefore, you can create buckets with different settings to complete different management tasks.

The following picture shows the overview page of a bucket:



You can click the Expand Bucket List icon on the right of **Bucket** to view the bucket list and related information, including the region, storage class, capacity, Internet traffic

of the current month, and the visits of the current month, as shown in the following picture:

Buckets		
<input type="text" value="Bucket Name"/>	<input type="text" value="Q"/>	<input type="text" value="Region"/>
Bucket Name	Region	T
bucket1111111111	China North 2 (Beijing)	S
bucket555555555555	China North 2 (Beijing)	I
bucket99999	China North 2 (Beijing)	A
keyan20180711test	China East 1 (Hangzhou)	S
keyan20180711test2	China East 1 (Hangzhou)	S
keyan20180816go	China East 1 (Hangzhou)	S
keyanbucket	China North 1 (Qingdao)	S
keyantest20180716	China East 1 (Hangzhou)	S
keyantest20180717	China East 1 (Hangzhou)	S

2.2 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

1. Log on to the [OSS console](#).
2. Click **Create Bucket** to open the **Create Bucket** dialog box.
3. In the **Bucket Name** field, enter the bucket name.
 - The bucket name must comply with the naming conventions.
 - The bucket name must be unique across all existing bucket names in OSS.
 - The bucket name cannot be changed after the bucket is created.
 - For more information about bucket naming, see [Basic concepts](#).

4. 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 [Endpoints](#).

5. 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.
6. 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.

**Note:**

The fees incurred by such operations are borne by the owner of the bucket. Use this permission with caution.

7. Click **OK**.

2.3 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 [Set lifecycle](#).
- For detailed procedures on how to delete parts, see [Manage fragments](#).

Procedure

1. Log on to the [OSS console](#).
2. In the bucket list on the left, click the name of the target bucket, and then click **Delete Bucket** in the upper-right corner.
3. In the dialog box that appears, click **OK**.

**Note:**

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

2.4 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.

This section describes how to change permission access control at the bucket level.

Procedure

1. Log on to the [OSS console](#).
2. On the bucket list on the left, click the target bucket to open the overview page of the bucket.
3. Click the **Basic Settings** tab and find **ACL** area.
4. Click **Setting** and change the bucket ACL.
5. Click **Save**.

2.5 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

1. Log on to the [OSS console](#).
2. In the left bucket lists, click one target bucket name to open the bucket overview page.
3. In the **Basic Settings** tab, find the **Static Page** area.
4. Click **Settings** to set the following parameters:

- **Default Homepage:** that is the index page (equivalent to the website's index.html), only HTML files that have been stored in the bucket can be used. If this field is left empty, the default home page settings are not enabled.
- **Default 404 Page:** The default 404 page returned when an incorrect path is accessed, only html, jpg, png, bmp, and webp files that have been stored in the bucket can be used. If this field is left empty, the default 404 page is disabled.

5. Click **Save**.

2.6 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

1. Log on to the [OSS console](#).
2. On the bucket list on the left, click the bucket you want to configure anti-leech to open the overview page of the bucket.
3. Click the **Basic Settings** tab, and click **Edit** in the **Anti-leech** area.
4. Enter the following information:
 - **Referer:** Add one or more URLs into the whitelist. Separate URLs with carriage returns.
 - **Allow Empty Referer:** Configure whether to allow empty referers.
5. Click **Save**.

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`.

2.7 Set a WORM strategy

A Write Once Read Many (WORM) strategy is used to specify the protection period of files in the bucket. No one can modify or delete files during the protection period.

Procedure

1. Log on to the [OSS console](#).

2. In the bucket list on the left, click the name of the target bucket.
3. Click the **Basic Settings** tab, locate **WORM settings** area, and click **Configure**.
4. Click **Create Strategy** to open the **Create Strategy** dialog box.
5. Set the **Lifecycle** for the WORM strategy.

The value range of **Lifecycle** is 1 day to 70 years.

6. Click **OK**.

After a WORM strategy is created, it is in **IN_PROGRESS** state.

7. Click **Lock**.

After a WORM strategy is locked, it cannot be deleted, but you can click **Edit** to extend the lifecycle of the strategy.

2.8 Manage a domain

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`

Custom domain names can be bound to OSS domain names through the console to implement custom domain name access storage space under the document, you can also configure the Ali cloud CDN to implement the acceleration function at the same time.

Bind a domain name

1. Go to the [OSS console](#).
2. On the left-side navigation pane, select a bucket from the bucket list to open the bucket overview page.
3. Click the **Domain Names** tab.
4. Click **Bind Self-Hosted Domain Name** to open the **Bind Self-Hosted Domain Name** dialog box.

Bind Self-Hosted Domain Name

Self-Hosted Domain Name

0/256

Enable Alibaba Cloud CDN

☐

Add CNAME Record Automatically

☐

The CNAME record cannot be added automatically, and you need to add it manually. It is probably because this domain name has been resolved in the cloud under another Alibaba Cloud account.

The domain name is successfully bound to your bucket only after you click Submit and then add the CNAME record at your DNS service provider. See the [help](#).

Submit

Cancel

5. Bind your domain.
 - a. In the **Self-Hosted Domain Name** text box, enter your domain name.
 - b. If you need CDN acceleration, open the **Enable Alibaba Cloud CDN** switch.

**Note:**

For more information about CDN acceleration, see the best practice [CDN-based OSS acceleration](#).

- c. 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.

6. 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.

If you need to unbind the domain name, click **Binding Configuration**, and then click **Unbind**.

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), and upload your certificate in the OSS console.

- If Alibaba Cloud CDN is not enabled for OSS, you can upload your certificate in the OSS console:
 1. On the **Domain Names** tab page, click **Upload Certificate** under **Action**.
 2. On the **Upload Certificate** page, enter your public key and private key, and then click **Upload**.

**Note:**

For certificate format requirements, see .

- If Alibaba Cloud CDN is enabled for OSS, you must upload your certificate in the CDN console . For more information, see .

Procedure for verifying domain name ownership

1. Click **Obtain TXT**. The system generates a TXT record based on your information.
2. Log on to your DNS provider and add the corresponding TXT record.
3. 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. From the left-side navigation pane, click Alibaba Cloud DNS to enter the domain name resolution list page.
2. Click the **Configure** link corresponding to the target domain name.
3. Click **Add Record**.
4. 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.
5. Click **Confirm**.

2.9 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

1. Log on to the [OSS console](#).
2. In the left-side navigation pane, select the target bucket to open the bucket overview page.
3. Click **Basic Settings**. In the **Cross-Origin Resource Sharing (CORS)** area, click **Edit**.
4. In the cross-origin access page, click **Create Rule**.
5. 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 (*) is 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 (*) is allowed for each matching rule.
- **Exposed Headers:** Indicates the response headers that users are allowed to access from an application (for example, 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.

6. Click **OK**.

**Note:**

You can also edit or delete an existing rule.

2.10 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

1. Log on to the [OSS console](#).
2. In the left-side bucket list, click the name of the target bucket to open the overview page of the bucket.
3. Click the **Basic Settings** tab, locate the **Lifecycle** area, and then click **Edit**.
4. Click **Create Rule** to open the **Create Lifecycle Rule** dialog box.
5. 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 Files**
 - **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.

6. Click **OK**.



Note:

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

2.11 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

1. Log on to the [OSS console](#).
2. In the left-side bucket list, click the name of the target bucket to open the overview page of the bucket.
3. Click the **Basic Settings** tab, and locate the **Cross-region Replication**.
4. Click **Enable Synchronization** to open the **Cross-region Replication** dialog box.
5. 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.

6. 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.

7. 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.

8. 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.

9. 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.

2.12 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-source rules, which are executed in sequence.

Procedure

1. Log on to the [OSS console](#).
2. Click one of the bucket names on the left.
3. Click **Basic Settings**, locate **Back-to-Origin** area, and click **Edit**.
4. Click **Create Rule**.
5. Select **Mirroring** or **Redirection**.

- If you choose **Mirroring** and a requested file cannot be found on OSS, OSS will automatically fetch the file from the origin, save it locally, and return the content to the requester.
 - If you choose **Redirection**, OSS redirects requests that meet the prerequisites to the origin URL over HTTP, and then a browser or client returns the content from the origin to the requester.
6. Set **Prerequisite** and **Origin URL**. In the Mirroring mode, you can choose to enable **Transfer queryString** or not. In the Redirection mode, you can set **Redirection Code**.
 7. In the Mirroring mode, you can set the transmission rule of HTTP header.

The configuration example is as follows:

Set transmission rule of HTTP header ?

Allow

☐ Transmit all HTTP headers

☒ Transmit the specified HTTP header

*

aaa-header

×

Add(9)

Deny

☒ Prohibit the transmission of specified HTTP header

*

bbb-header

×

Add(9)

Configure

☒ Set the specified HTTP header parameter

*

ccc-header

:

ccc

Add(9)

If the HTTP header in a request that sent to OSS is as follows:

```
GET /object
host : bucket.oss-cn-hangzhou.aliyuncs.com
```



```
aaa-header : aaa  
bbb-header : bbb  
ccc-header : 111
```

After the back-to-origin is triggered, the request that OSS sends to the origin is as follows:

```
GET /object  
host : source.com  
aaa-header : aaa  
ccc-header : ccc
```

**Note:**

The following HTTP headers do not support transmission rules:

- The headers with the following prefixes:
 - x-oss-
 - oss-
 - x-drs-
- All the standard HTTP headers, such as:
 - content-length
 - authorization2
 - authorization
 - range
 - date

8. Click **OK**.

**Note:**

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

3 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 [Introduction](#).
- 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 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 [Introduction](#) the API documentation.

Procedures

1. Log on to the [OSS console](#).
2. In the left-side bucket list, click the name of the target bucket to open the overview page of the bucket.
3. Click the **File** tab.
4. Click the **Fragments** to open the **Fragments (Multipart)** page.
5. Delete the part files.
 - To delete all the part files in a bucket, click **Clear Fragments**.
 - To delete some of the part files in a bucket, select or search for the expected part files and click **Delete Fragments**.
6. In the dialog box that appears, click **OK**.

4 Log analysis

OSS users often need to analyze data about access logs and resource consumption, such as:

- Usage of OSS storage, traffic, and requests
- Logs generated during the lifecycle of a file (create, modify, delete)
- Hot files, accesses to these files, and the traffic generated by the accesses
- Errors and list of logs including error requests

You can use the log analysis function on the OSS console to analyze massive logs. This document describes how to activate and use the log analysis service on the OSS console.

Procedure

1. Activate the log service.
 - a. Log on to the [OSS console](#).
 - b. In the **Data Processing** area, find **Log Analysis**, move the mouse cursor to the Log Analysis icon, click **Activate Log Service**.
 - c. On the activation page, select I Agree, and click **Activate**.
2. Authorize the log service so that it can obtain data from OSS.
 - a. On the OSS console, click **Overview** on the upper left corner to refresh the page. Move the mouse cursor to the **Log Analysis** icon, click **Authorize Log Collection**.

**Note:**

Before authorization, you must click **Overview** on the OSS console to refresh the page.

- b. On the **Cloud Resource Access Authorization** page, confirm that the role to authorize is **AliyunLogArchiveRole**, click **Authorize**.
3. Associate the log analysis service with a bucket.
 - a. On the OSS console, click **Overview** on the upper left corner to refresh the page. Move the mouse cursor to the **Log Analysis** icon, click **Manage Log Service**.

**Note:**

You must click **Overview** on the OSS console to refresh the page before managing the log service.

- b. On the **Log Analysis** page, click **Create association**.

- c. The **Create Log Analysis Association** page is displayed on the right. In Step 1, select **Region**, enter the **Project name** and **Description** (optional), and click **Next**.

Pay attention to the following two points:

- When selecting **Region**, you must select regions in which available buckets are created.
- When selecting **Project name**, you must follow the following rules:
 - A project name can only include lower-case letters, numbers, and hyphens.
 - A project name must start and end with a lower-case letter or a number.
 - The length of a project name can be 3 to 63 characters.

- d. In Step 2, enter **Log store name**, select **Data storage period** and **Partition (Shard) number**, and click **Next**.

Each item you enter and select is described below:

- **Log store name:** The name of the log store, which must follow the following rules:
 - A log store name can only include lower-case letters, numbers, hyphens, and understores.
 - A log store name must start and end with a lower-case letter or a number.
 - The length of a log store name can be 3 to 63 characters.
- **Data storage period:** Number of days that data is stored.
- **Partition (shard) number:** For detailed information, see [Partition](#).

- e. In Step 3, select **Bucket to associate with** and click **Submit**.

4. Configure index information.

- a. Click **Go to log service console to configure index information**.
- b. If you do not have special requirements, you can keep the basic and default configuration and click **Next**.



Note:

If you want to configure index information separately, see [Index and query](#).

- c. Configure the log data delivery and ETL functions. If you do not need to deliver log data, click **OK**. If you want to deliver log data, click **Enable delivery** on the required delivery method and ETL function, and then click **OK**.
- For methods of how to delivery log data to OSS, see [Ship logs to OSS](#).

- For methods of how to configure ETL function, see [Configure Function Compute log consumption](#).

5. Analyze logs.

- a. On the OSS console, move the mouse cursor to the **Log Analysis** icon, click **Manage Log Service**, as shown in the following figure:
- b. On the **Log Analysis** page, click **Analyze logs**.
- c. The log analysis page is displayed. You can view the log analysis result either in the database or in the dashboard.

5 Log on to OSS console

Context

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 when you activate OSS.

Procedure

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

6 Manage objects

6.1 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.

6.2 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 [Introduction](#).

**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

1. Log on to the [OSS console](#).
2. Click the name of the bucket which you want to upload objects to.
3. Click the **Files** tab.
4. Click **Upload** to open the **Upload** box.

**Note:**

You can upload a file to a specified folder or to a default folder. You can select [Create a folder](#) before clicking **Upload** to upload the file to a specified folder. You can also directly click **Upload** to upload a file to a default OSS folder.

5. 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](#).

6. 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.

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

8. 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.

6.3 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).

Procedure

1. Log on to the [OSS console](#).
2. Click to open the target bucket.
3. Select the **Files** tab.
4. Click **Create Directory**, and enter a directory name.
5. Click **OK**.

6.4 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

1. Log on to the [OSS console](#).
2. Click to open the target bucket.
3. Click **Files**.
4. 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.

**Note:**

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.

6.5 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-level 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 [Add a signature to a URL](#).
- **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 operations 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

1. Log on to the [OSS console](#).
2. In the left-side bucket list, click the name of the target bucket to open the overview page of the bucket.
3. Click the **Files** tab.
4. Click the name of the target file to open the **Preview** page of the file.
5. 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 **link validity period** (in seconds) in the **Signature** field.
6. Click **OK**.

6.6 Use bucket policies to authorize other users to access OSS resources

You can use bucket policies to authorize other users to access your OSS resources.

Compared with the [RAM policies](#), bucket policies can be directly configured by the bucket owner in the graphical console for access authorization. You can use bucket policies in the following common scenarios:

- Authorize RAM users of other accounts to access your OSS resources.

You can authorize RAM users of other accounts to access your OSS resources.

- Authorize anonymous users to access your OSS resources using specific IP addresses or IP ranges.

In some cases, you must authorize anonymous users to access OSS resources using specific IP addresses or IP ranges. For example, confidential documents of an enterprise are only allowed to be accessed within the enterprise but not in other regions. It takes a lot of effort to configure RAM policies for every user because of the large number of internal users. In this case, you can configure access policies with IP restrictions based on bucket policies to authorize users easily and efficiently.

Authorize RAM users of other accounts to access your OSS resources

1. Log on to the [OSS console](#).
2. In the bucket list on the left, click the name of the bucket you want to authorize the user to access.
3. On the overview page of the bucket, click the **Files** tab, and then click **Authorize**.
4. On the **Authorize** page, click **Authorize**.
5. On the **Authorize** page, configure **Applied To**.
 - **Whole Bucket**: The authorization policy applies to the whole bucket.
 - **Specified Resource**: The authorization policy applies only to specified resources in the bucket. If you select this option, you must enter the path of the specified resources, such as `abc/myphoto.png`. If the policy applies to a directory, you must add an asterisk (*) at the end of the path, such as `abc/`.
6. In the **Accounts** field, enter the account IDs you want to authorize. If you want to authorize multiple users, separate their IDs with commas (,).
7. Configure **Authorized Operation**.

- **Read Only:** Authorized users can only read the resources.
- **Read/Write:** Authorized users can read and write the resources.
- **Any Operation:** Authorized users can perform any operation on the resources.
- **None(Deny):** Authorized users cannot perform any operation on the resource.

**Note:**

If multiple bucket policies are configured for a user, the user's access is determined by the combination of these policies. However, the user cannot perform any operation if the authorized operation is configured to **None(Deny)** in any of the policies. For example, if the authorized operation of a user is configured to **Read Only** in a bucket policy and **Read/Write** in another, the user has the **Read/Write** access which is the combination of the **Read Only** and **Read/Write** access. If the authorized operation of the user is configured to **None(Deny)** in another policy, the user only has the **None(Deny)** access.

8. (Optional) Configure **Conditions** to authorize the user to access OSS resources using only specified IP addresses. You can select **IP is** or **IP is not** to allow or prohibit IP addresses or IP ranges used to access OSS resources.
 - You can specify an IP address or multiple IP addresses as the condition, such as 10.10.10.10. Separate multiple IP addresses with commas (,).
 - You can also specify an IP range as the condition, such as 10.10.10.1/24.
9. Click **OK**.

Authorize anonymous users to access your OSS resources using specific IP addresses or IP ranges

1. Log on to the [OSS console](#).
2. In the bucket list on the left, click the name of the bucket you want to authorize the user to access.
3. On the overview page of the bucket, click the **Files** tab, and then click **Authorize**.
4. On the **Authorize** page, click **Authorize**.
5. On the **Authorize** page, configure **Applied To**.
 - **Whole Bucket:** The authorization policy applies to the whole bucket.
 - **Specified Resource:** The authorization policy applies only to specified resources in the bucket. If you select this option, you must enter the path of the specified resources, such as

abc/myphoto.png. If the policy applies to a directory, you must add an asterisk (*) at the end of the path, such as abc/*.

6. In the **Accounts** field, select `Anonymous User (*)`.

**Warning:**

We strongly recommend that you configure IP address conditions if you authorize anonymous users to access OSS resources. If you do not configure IP address conditions, your resources can be accessed by any user.

7. Configure **Authorized Operation**.

- `Read Only`: Authorized users can only read the resources.
- `Read/Write`: Authorized users can read and write the resources.
- `Any Operation`: Authorized users can perform any operation on the resources.
- `None(Deny)`: Authorized users cannot perform any operation on the resource.

**Note:**

If multiple bucket policies are configured for a user, the user's access is determined by the combination of these policies. However, the user cannot perform any operation if the authorized operation is configured to `None(Deny)` in any of the policies. For example, if the authorized operation of a user is configured to `Read Only` in a bucket policy and `Read/Write` in another, the user has the `Read/Write` access which is the combination of the `Read Only` and `Read/Write` access. If the authorized operation of the user is configured to `None(Deny)` in another policy, the user only has the `None(Deny)` access.

8. Configure **Conditions**. You can select `IP is` or `IP is not` to allow or prohibit IP addresses or an IP range used to access OSS resources.

- You can specify an IP address or multiple IP addresses as the condition, such as 10.10.10.10. Separate multiple IP addresses with commas (,).
- You can also specify an IP range as the condition, such as 10.10.10.1/24.

9. Click **OK**.

6.7 Download an object

After uploading an object to a bucket, you can share or download the object.

Procedure

1. Log on to the [OSS console](#).

2. In the left-side bucket list, click the name of the target bucket.
3. In the overview page of the bucket, click the **Files** tab.
4. Click the name of the target file. In the **Preview** page of the file, you can perform the following operations:

- **Download:** You can download the file to your local storage.

You can also download files in the following methods:

- Download one or more files: On the **Files** page, select one or more files, and then select **Batch operation > Download**.
- Download a single file: On the **Files** page, select a file, and then select **More > Download**.
- **Open File URL:** You can directly open the file in a browser. A file that cannot be opened directly, such as Excel files, is downloaded when the URL is opened.
- **Copy File URL:** You can obtain the URL of a file and share it with others, allowing them to browse and download the file.

You can also obtain the URL of a file in the following methods:

- Obtain the URL of one or more files: On the **Files** page, select one or more files, and then select **Batch operation > Export URL List**.
- Obtain the URL of a single file: On the **Files** page, select **More > Copy File URL**.
- **Copy File Path:** You can search a file or add watermarks to an image file.

**Warning:**

If the bucket is configured with Referer Whitelist and Empty Referer is not allowed, then the URL cannot be opened directly in a browser.

5. If your bucket ACL is set to **Private**, you must set the **Validity Period** in the **Signature** field when obtaining the URL of a file. The validity period is 3,600 seconds by default and cannot exceed 64,800 seconds.

**Note:**

- The validity period of a signed URL is calculated based on NTP. You can share a URL to others, allowing them to access the file within the validity period. If your bucket ACL is set to Private, a signature will be added to the URL. For more information, see [Add a signature to a URL](#).

- You can change the ACL of a bucket or a file anytime. For more information, see [Change bucket ACL](#) and [Change object ACL](#).

6.8 Set an HTTP header

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

Procedure

1. Log on to the [OSS console](#).
2. In the left-side bucket list, click the name of the target bucket to open the overview page of the bucket.
3. Click **Files**.
4. Select one or multiple files, and then select **Batch operation > Set HTTP Header**.

You can also set an HTTP header for a single file as follows: Click the target file name, and then click **Set HTTP Header** in the **Preview** page.

- To set the HTTP header for one or multiple files, select one or multiple files, and then select **Batch operation > Set HTTP Header**.
 - To set the HTTP header for a single file, click **Configure** for the file. On the **Preview** page, click **Set HTTP Header**.
 - To set the HTTP header for a single file, you can also select **More > Set HTTP Header**.
5. Set the related parameters. You can also add user-defined metadata.



Note:

For more information about each parameter, see [Definitions of common HTTP headers](#).

6. Click **OK**.

6.9 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 **1000** 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 [Delete an object](#).
- API: See [DeleteObject](#) and [DeleteMultipleObjects](#).
- SDK: See Delete multiple objects in .

Procedure

1. Log on to the [OSS console](#).
2. Click to open the target bucket.
3. Click **Files**.
4. Select one or multiple files, and then click **Delete**.
5. Click **OK**.

6.10 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

1. Log on to the [OSS console](#).
2. Click to open the target bucket.
3. Click **Files**.
4. Select the target folder, and then click **Delete**.



Note:

Deletion may fail if the folder contains too many files.

5. Click **OK** to delete the folder.

7 Check resource usage

Overview

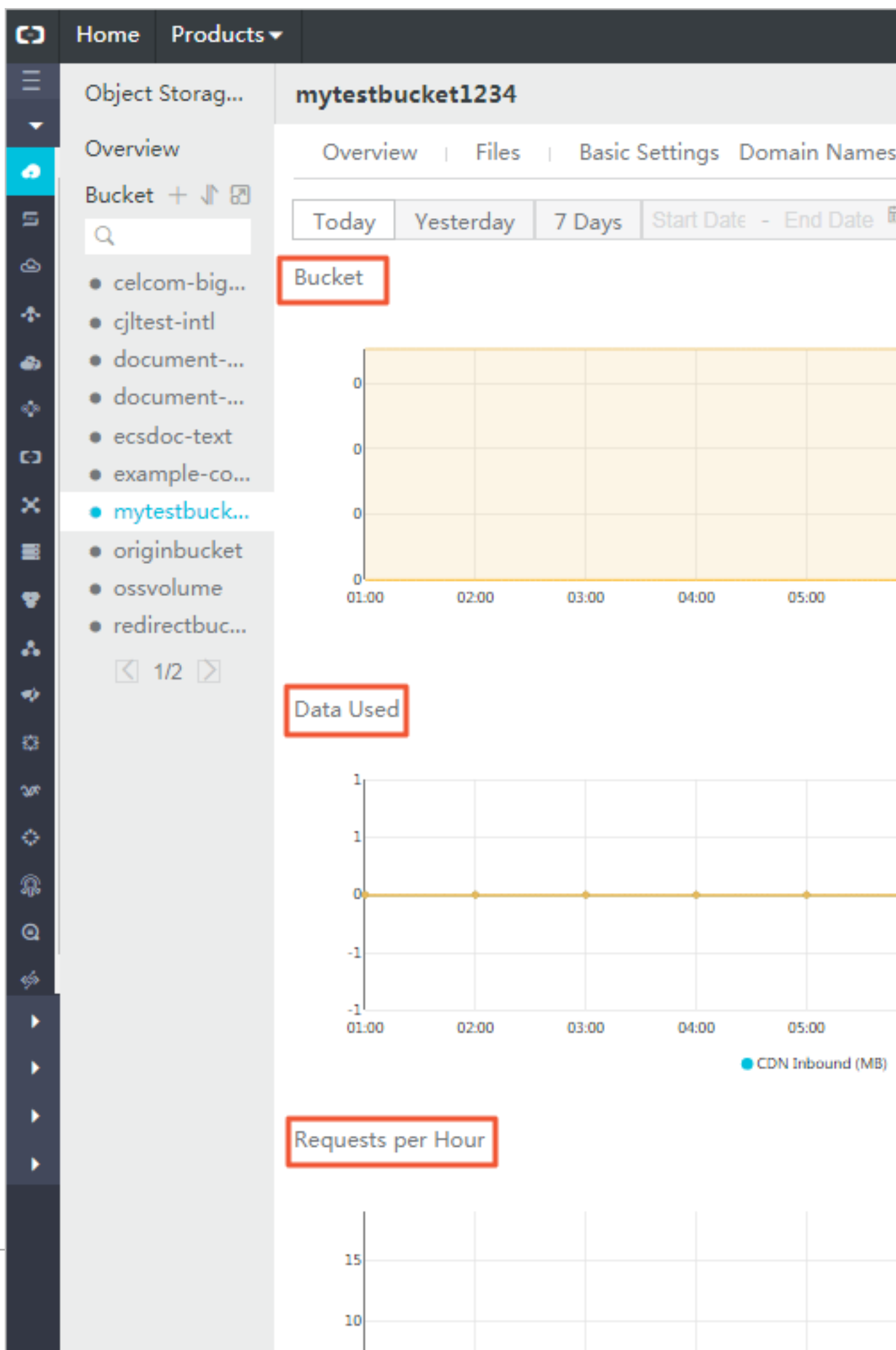
You can check the usage of the following resources on the OSS console:

- 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

1. Log on to the [OSS console](#).
2. In the bucket list on the left, click the target bucket name to open its information page.
3. 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:

Table 7-1: 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

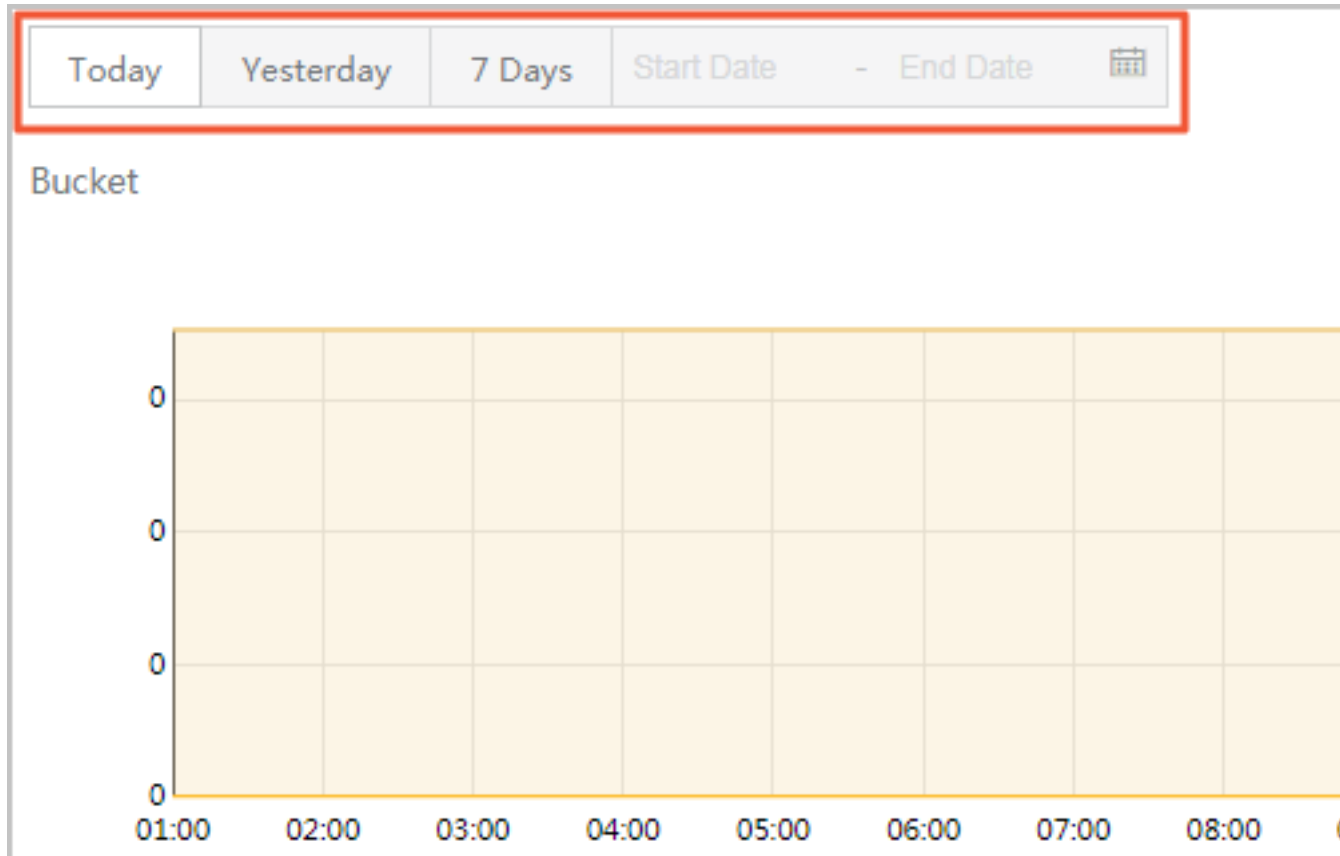
Table 7-2: Data Used

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

Table 7-3: Request per Hour

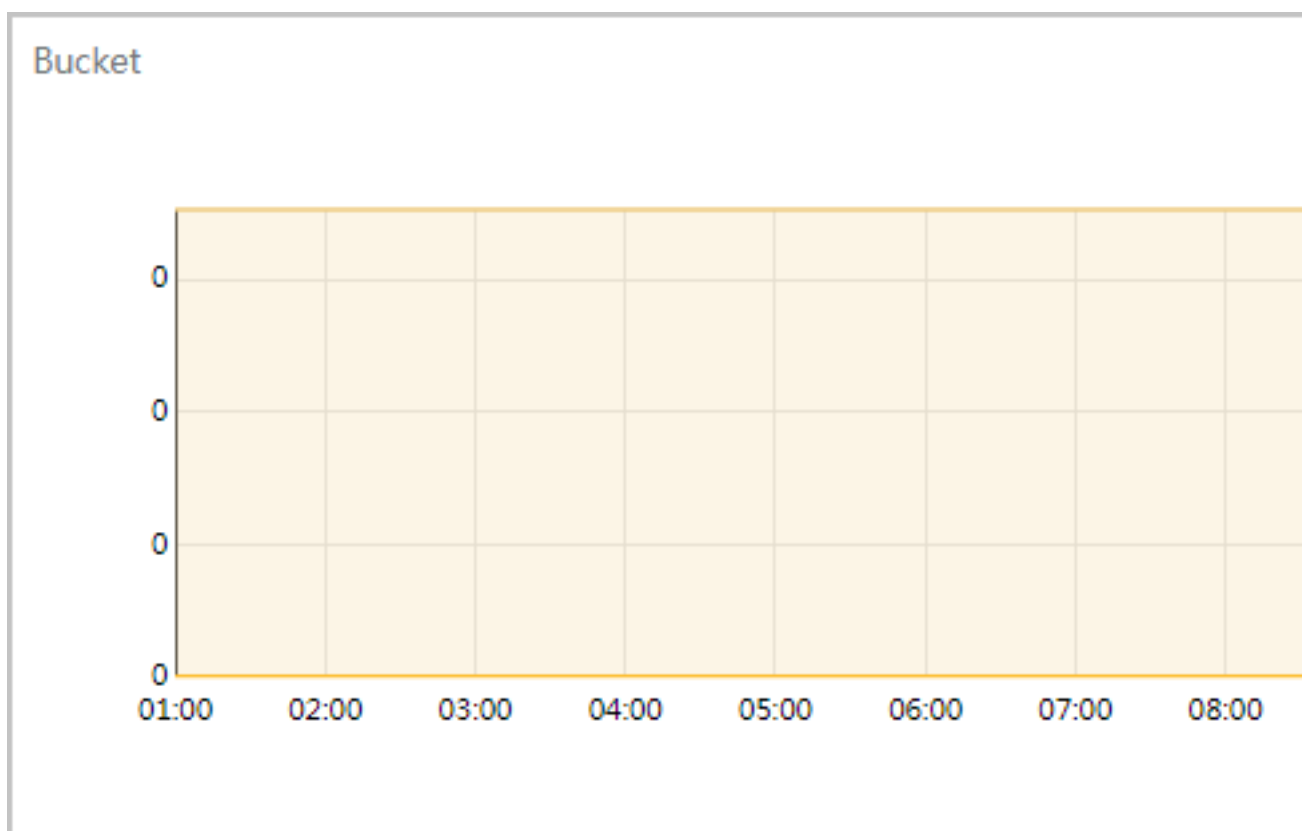
Basic Data	Description
GET Request	Number of GET requests per hour
PUT Request	Number of PUT requests per hour

4. 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.
5. 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 : 1. Show the basic data item in the diagram. 2. 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: 1. Only show this basic data item in the diagram. 2. Show all basic data items in the diagram.