Alibaba Cloud Object Storage Service

Console User Guide

Issue: 20190918

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.	 Notice: 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 `cd / d C :/ windows` command to enter the Windows system folder.
Italics	It is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	It indicates that it is a optional value, and only one item can be selected.	`ipconfig` *[-all|-t]*

Style	Description	Example
{} or {a|b}	It indicates that it is a required value, and only one item can be selected.	`swich {stand | slave}`

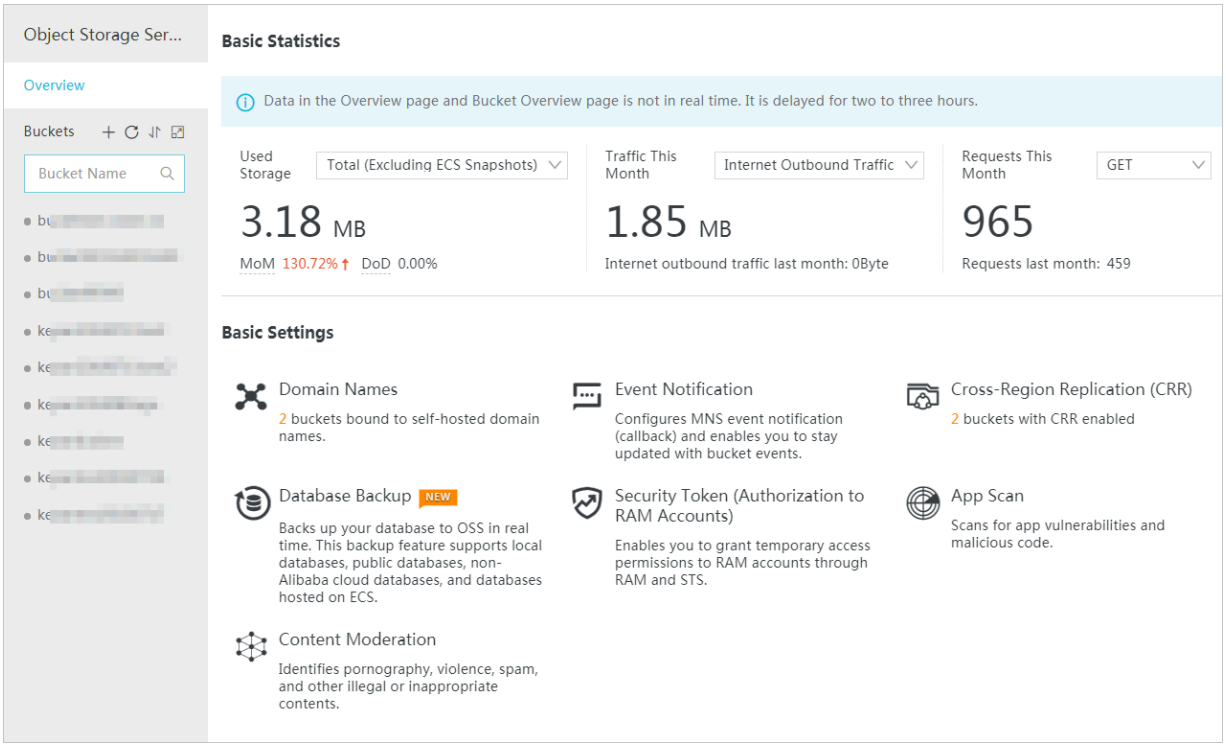
Contents

1 Manage buckets

1.1 Bucket overview

A bucket is a container of your objects. Each object must be stored in a bucket in OSS. The objects in a bucket are stored in a non-hierarchical structure instead of a directory-based file system. You can set and change the attributes of a bucket to control the region, ACL, and life cycle of the bucket. These attributes apply to all the objects stored in the bucket. Therefore, you can create buckets with different settings to complete different management tasks.

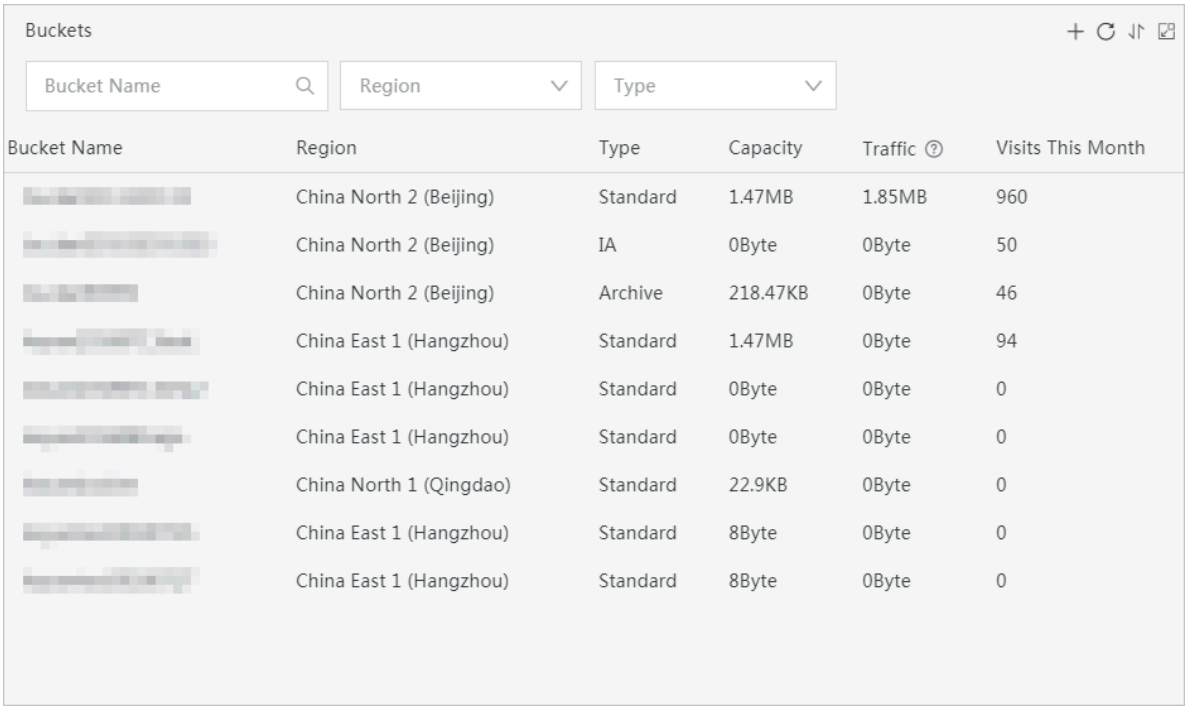
The following figure shows the overview page of a bucket.



View the overview 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 figure.



- You can click Export CSV in the right area of the page to export your bucket information including the bucket name, region, storage class, and creation time as a .csv file to your computer.

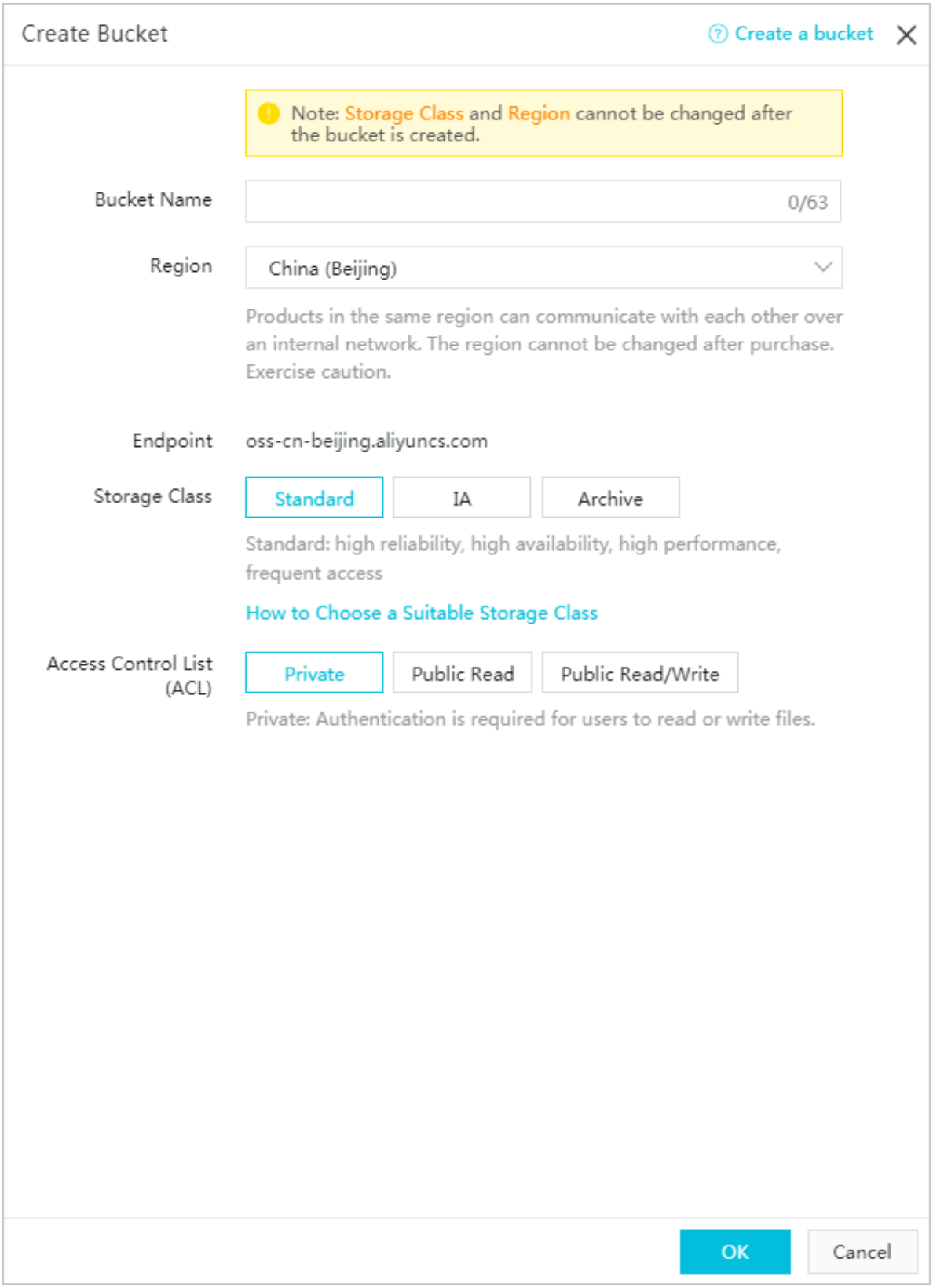
1.2 Create a bucket

Before uploading any file to OSS, you must create a bucket and specify the attributes of the bucket, including the region, ACL, and other metadata.

Procedure

1. Log on to the OSS console.
2. If the bucket list is empty, click Create Bucket on the left side. If you have created buckets, click + in the left-side bucket list or click Create Bucket in the upper right

corner to create a bucket. The Create Bucket dialog box is displayed, as shown in the following figure.



3. Enter a name for the bucket in Bucket Name.
   - The bucket name must comply with the naming conventions.
   - The bucket name must be unique among all existing OSS buckets.
   - The name of a bucket cannot be modified after the bucket is created.
   - For more information about the bucket naming conventions, see Basic concepts.
4. In the Region drop-down list, select the region where the bucket needs to be created.

   The region of a bucket cannot be modified after the bucket is created. Exercise caution when selecting the region. To access a bucket from an ECS instance through the intranet, select the region to which the ECS instance belongs when creating the bucket. For more information, see Endpoints.
5. Select one of the following storage classes for Storage Class according to your needs.
   - `Standard` : provides highly reliable, highly available, and high-performance object storage services that support frequent data accesses.
   - `IA` : applies to data that is stored long-term and infrequently accessed. Its unit price is lower than that of the Standard class. Objects of the IA storage class must be stored for a minimum period of 30 days. Fees are incurred if objects of the IA storage class are deleted before they are stored for 30 days. Objects of the IA storage class also have a minimum billable size of 64 KB. Any objects smaller than 64 KB are charged as 64 KB. Furthermore, data retrieval also incurs charges.
   - `Archive` : applies to archive data that has cold storage attributes (that is, the data is to be stored for more than half a year and is only to be accessed sporadically during the storage period). Note that if you need to convert Archive class data to IA class data, the conversion takes about one minute before the data can be accessed. Examples of objects suitable for the Archive storage class include archive data, medical images, scientific data, and video.

6. Select an ACL for the bucket in Access Control List (ACL).
   - `Private` : Only the bucket owner can read data from and write data to objects in the bucket. All other users (including anonymous users) cannot perform operations on objects in the bucket without authorization.
   - `Public Read` : Only the bucket owner can write data to objects in the bucket. All other users (including anonymous users) can only read from objects in the bucket.

      **Warning:**
     Any user can access the objects in the bucket through the Internet. This may result in data leakage and excessive fees. Therefore, set this ACL with caution.
   - `Public Read / Write` : All users (including anonymous users) can read from and write to objects in the bucket.

      **Warning:**
     Any user can access the objects in the bucket and write data to the bucket through the Internet. This may result in data leakage and excessive fees. Your legal rights may be infringed if illegal information is maliciously written to your bucket. Therefore, we recommend you do not set the ACL to public-read-write unless necessary.
7. Click OK.

1.3 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.

This topic 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.

   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 objects.
   - `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, which may result in data leakage and excessive charges.
   - `Public Read / Write` : Anyone (including anonymous users) can perform read and write operations on the objects in the bucket, which may result in data leakage and excessive charges. In addition, your rights may be damaged if illegal information is maliciously written to objects in your bucket. Therefore, we recommend you do not set the ACL of your bucket to public read/write except for specific scenarios.

5. Click Save.

1.4 Enable pay-by-requester mode for a bucket

You can enable pay-by-requester mode for a bucket. In this mode, requesters are charged for requests and traffic, and the bucket owner is charged only for the storage. Pay-by-requester mode is only available in the China South 1 (Shenzhen) region currently and will be supported in more regions.

Procedure

1. Log on to the OSS console.
2. In the left-side bucket list, click the bucket that you want to enable pay-by-requester mode for.
3. In the overview page of the bucket, click the Basic Settings tab, and then click Configure in the Pay by Requester area.
4. Enable or disable pay-by-requester mode for the bucket.
5. Click Save.

1.5 Configure server-side encryption

OSS can perform server-side encryption on data uploaded to buckets to ensure data security.

OSS supports server-side encryption for uploaded data. This means that when user data is uploaded, OSS encrypts the data and permanently stores the data. Then, when the data is downloaded by a user, OSS automatically decrypts the data, returns the original data to the user, and declares in the header of the returned HTTP request that the data has been encrypted on the server.

 Note:
For more information about server-side encryption, see #unique_11.

You can enable server-side encryption on the OSS console in the following two methods:

- Method 1: Enable server-side encryption when creating a bucket.
- Method 2: Enable server-side encryption in the Basic Settings tab page.

Method 1: Enable server-side encryption when creating a bucket

1. Log on to the OSS console.
2. Click Create Bucket.

3. In the Create Bucket dialog box, input the parameters of the bucket.

   Select the following options for Server Encryption. For the settings of other parameters, see #unique_14.

   - None: Do not enable server-side encryption.
   - AES256: Encrypt objects using the AES256 algorithm. OSS uses different keys to encrypt each object. Furthermore, the keys are encrypted by a customer master key (CMK) that is updated periodically for higher security.
   - KMS: You can use a specified CMK ID or the default CMK managed by KMS to encrypt or decrypt data. For more information about KMS encryption algorithm, see #unique_11/unique_11_Connect_42_section_c24_wbd_5gb.
     - `alias / acs / oss` : Use the default CMK managed by KMS to encrypt different objects, and decrypt the objects when they are downloaded.
     - `CMK ID` : Use keys generated by a specified CMK to encrypt different objects, and record the specified CMK ID in the metadata of the encrypted object. Therefore, the objects are automatically decrypted when they are downloaded by users with the decryption permission. Before specifying a CMK ID, you must create a normal key or an external key in the same region as the bucket in the KMS console. This function is in the beta testing phase. To join the test, contact Alibaba Cloud technical support.

     Notice:
     - Before using the KMS encryption method, you must activate KMS.
     - API calling fees are incurred when you use CMKs to encrypt or decrypt data.
4. Click OK.

Method 2: Enable server-side encryption in the Basic Settings tab page

1. Log on to the OSS console.
2. In the left-side bucket list, select the bucket that you want to enable server-side encryption for.

3. Click Basic Settings, and then click Configure in the Server Encryption area.
   - None: Do not enable server-side encryption.
   - AES256: Encrypt objects using the AES256 algorithm. OSS uses different keys to encrypt each object. Furthermore, the keys are encrypted by a customer master key (CMK) that is updated periodically for higher security.
   - KMS: You can use a specified CMK ID or the default CMK managed by KMS to encrypt or decrypt data. For more information about KMS encryption algorithm, see #unique_11/unique_11_Connect_42_section_c24_wbd_5gb.
     - `alias / acs / oss` : Use the default CMK managed by KMS to encrypt different objects, and decrypt the objects when they are downloaded.
     - `CMK ID` : Use keys generated by a specified CMK to encrypt different objects, and record the specified CMK ID in the metadata of the encrypted object. Therefore, the objects are automatically decrypted when they are downloaded by users with the decryption permission. Before specifying a CMK ID, you must create a normal key or an external key in the same region as the bucket in the KMS console. This function is in the beta testing phase. To join the test, contact Alibaba Cloud technical support.

      Notice:

     - Before using the KMS encryption method, you must activate KMS.
     - API calling fees are incurred when you use CMKs to encrypt or decrypt data.
4. Click Save.

    Notice:
   Encryption methods for existing objects in a bucket are not added or modified when you enable or modify the default encryption method for the bucket.

Permissions

To use server-side encryption with a RAM user, you must have the following permissions:

- To configure the default encryption method for a bucket, you must have:
  - The management permission of the bucket.
  - The permission to perform the PutBucketEncryption and GetBucketEncryption operations.
  - The permission to perform the ListKeys, Listalias, ListAliasesByKeyId, and DescribeKeys operations when you use a specified CMK ID to encrypt data. The RAM policy used to set permissions for specified CMK IDs is as follows:

```
{
  " Version ": " 1 ",
  " Statement ": [
    {
      " Effect ": " Allow ",
      " Action ": [
        " kms : List *",
        " kms : DescribeKe  y "
      ],
      " Resource ": [
        " acs : kms :*: 1416614965  936597 :*" // This   example
   allows   the   user   to   use   all   CMKs   under   the
 account .  To   restrict   the   user   to   use   only   one
 CMK ,  input   the   CMK   ID .
      ]
    }
  ]
}
```

- To upload an object to a bucket with the default encryption method configured, you must have:
  - The permission to upload objects to the bucket.
  - The permission to perform the ListKeys, Listalias, ListAliasesByKeyId, DescribeKeys, and GenerateDataKey operations when you use a specified CMK ID to encrypt data. Otherwise, the object fails to be uploaded. The RAM policy used to set permissions for specified CMK IDs is as follows:

```
{
  " Version ": " 1 ",
  " Statement ": [
    {
      " Effect ": " Allow ",
      " Action ": [
        " kms : List *",
        " kms : DescribeKe  y ",
        " kms : GenerateDa  taKey "
      ],
      " Resource ": [
        " acs : kms :*: 1416614965  936597 :*"// This   example
   allows   the   user   to   use   all   CMKs   under   the
 account .  To   restrict   the   user   to   use   only   one
 CMK ,  input   the   CMK   ID .
      ]
```

```
    }
  ]
}
```

- To download an object from a bucket with the default encryption method configured, you must have:
  - The permission to access objects in the bucket.
  - The permission to perform the Decrypt operation when you use a specified CMK ID to decrypt data. Otherwise, the object fails to be downloaded. The RAM policy used to set permissions for specified CMK IDs is as follows:

```
{
  " Version ": " 1 ",
  " Statement ": [
    {
      " Effect ": " Allow ",
      " Action ": [
    " kms : Decrypt "
      ],
      " Resource ": [
        " acs : kms :*: 1416614965  936597 :*"// This   example
   indicates   that   the   RAM   user   has   the   permission
 to   decrypt   data   using   all   CMKs .  To   decrypt   data
 using   a   specified   CMK ,  input   the   CMK   ID .
      ]
    }
  ]
}
```

Reference

For more information, see #unique_16.

1.6 Configure a compliant retention policy

OSS uses the compliant retention policy (Write Once Read Many strategy) to specify the protection period of objects in a bucket. No one can modify or delete a protected object during the protection period.

Prerequisites

The compliant retention policy is in the beta testing phase. To use this policy, contact After-sales technical support.

Note:

For more information about the compliant retention policy, see Compliant retention policy.

Video tutorial

The following video provides a quick introduction to the compliant retention policy.

Procedure

1. Log on to the OSS console.
2. On the left-side bucket list, click the target bucket to open the overview page of the bucket.
3. Click the Basic Settings tab, find the Retention Policy section, and click Configure.
4. Click Create Policy. The Create Policy dialog box appears.
5. Set Retention Period for the compliant retention policy. Valid values of Retention Period range from one day to 70 years.
6. Click OK.

   After the policy is created, the status indicates "IN_PROGRESS." You can click Lock or Delete.
7. Click Lock.
8. In the message that appears, click OK.

> Note:
>
> - The policy status becomes LOCKED. You cannot delete the policy or shorten the protection period. However, you can click Edit to prolong the protection period for objects.
> - During the protection period, data in the bucket is protected. If you attempt to delete or modify the data, error message `The operation failed. The object has been locked.` is displayed.

Calculate the expiration time for objects

You can calculate the expiration time by adding the retention period and last update time of objects in buckets. For example, bucket A is configured with the compliant retention policy in which the retention period is 10 days. The last update time of an object in the bucket is 12:00 on March 1, 2019. The object expires at 12:01 on March 11, 2019. For more information about the rules of the compliant retention policy, see Rules.

1.7 Manage a domain

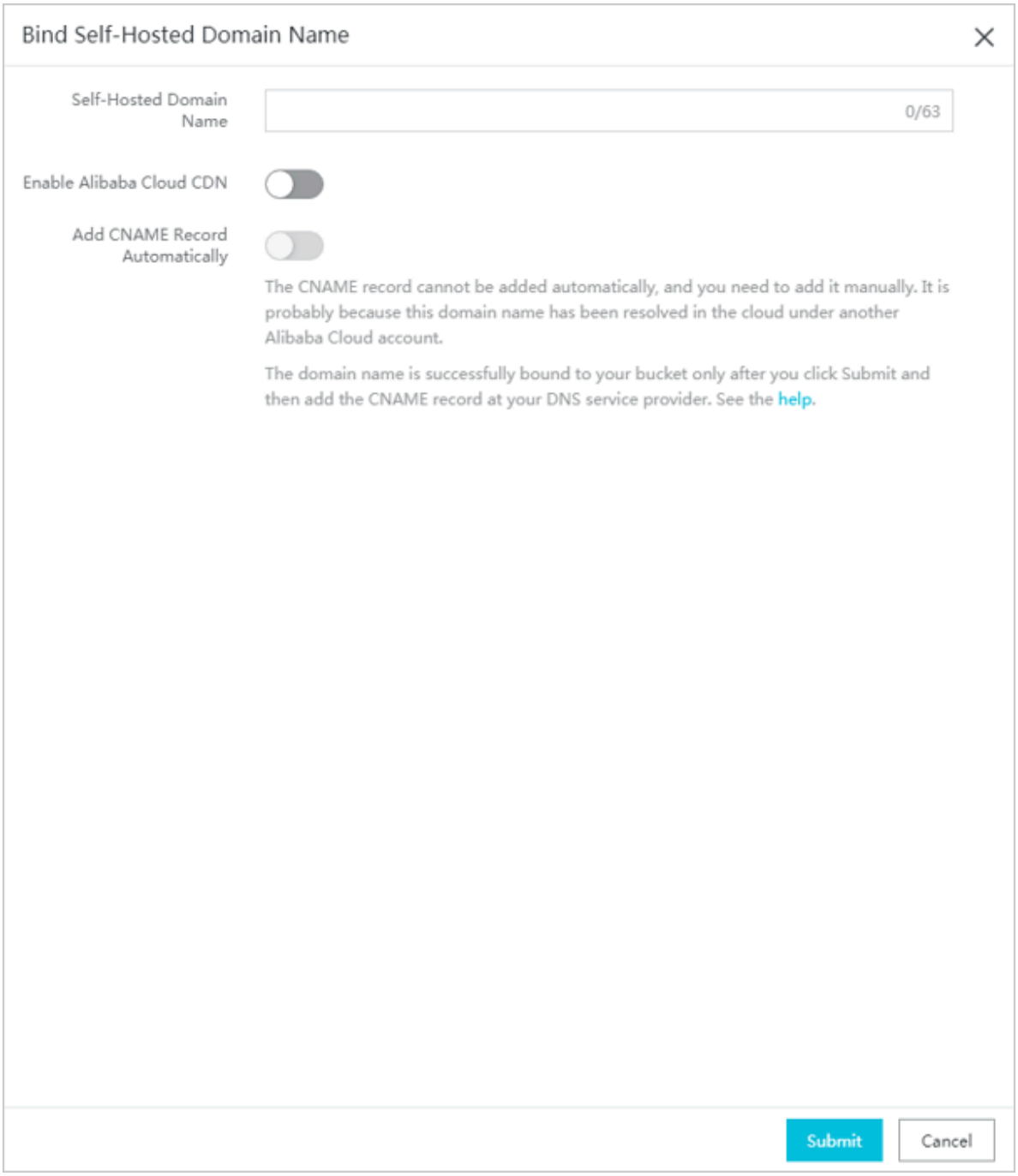
1.7.1 Attach a custom domain name

After an object is uploaded to an OSS bucket, a URL is automatically generated for the object. You can use this URL to access the object in the bucket. To access an uploaded object by using a custom domain name, you must attach the custom domain name to the bucket where the object is stored and add a CNAME record that directs to the Internet domain name of the bucket. This topic describes how to attach a custom domain name to a bucket and how to add a CNAME record.

Attach a domain name to a bucket

1. Log on to the OSS console. In the left-side bucket list, click the name of the bucket that you want to attach a custom domain name.

2. Click Domain Names > Bind Self-Hosted Domain Name. In the Bind Self-Hosted Domain Name page, you can set the following parameters:



- Self-Hosted Domain Name: Enter the domain name that you want to attach, such as `hello-world.com`. The maximum length of a domain name is 63 characters.
- Enable Alibaba Cloud CDN: If you want to enable CDN-based OSS acceleration, see Attach a CDN acceleration domain name.
- Add CNAME Record Automatically: The record of a CNAME managed by your Alibaba Cloud account can be automatically added. To add a record of a domain

name that is not managed by your Alibaba Cloud account, you must manually configure the DNS of your DNS provider. For more information, see Manually add a CNAME record.

3. Enter your self-hosted domain name and enable Add CNAME Record Automatically. Click Submit.

   Note:

   - If a Domain name conflict message is prompted, the domain name has been attached to a bucket owned by another user. You can click Obtain TXT and add a txt record of the domain name to the DNS of your DNS provider to verify the ownership of the domain name and forcibly attach the domain name to your bucket. However, if you forcibly attach a domain name to a new bucket, the domain name is detached from the bucket to which it is currently attached. For more information, see Verify domain name ownership.
   - If a message is prompted that indicates the domain name is not filed, you must file the domain name first.

4. If you want to detach the domain name from the bucket, click Domain Names > Binding Configuration > Unbind.

Manually add a CNAME record

The following steps apply only to scenarios where a CNAME record is not automatica lly added.

You must add a CNAME record to the DNS of your DNS provider. In this topic, Alibaba Cloud DNS is used as an example to describe the process of adding a CNAME record.

1. Log on to the Alibaba Cloud DNS console.
2. In the domain name list, click Configure on the right of the domain name that you want to add a record.
3. Click Add Record and enter the DNS information. The following table describes the parameters that you can configure.

Parameter	Description
Type	Select the type of record to which the domain name directs. In this example, select CNAME.

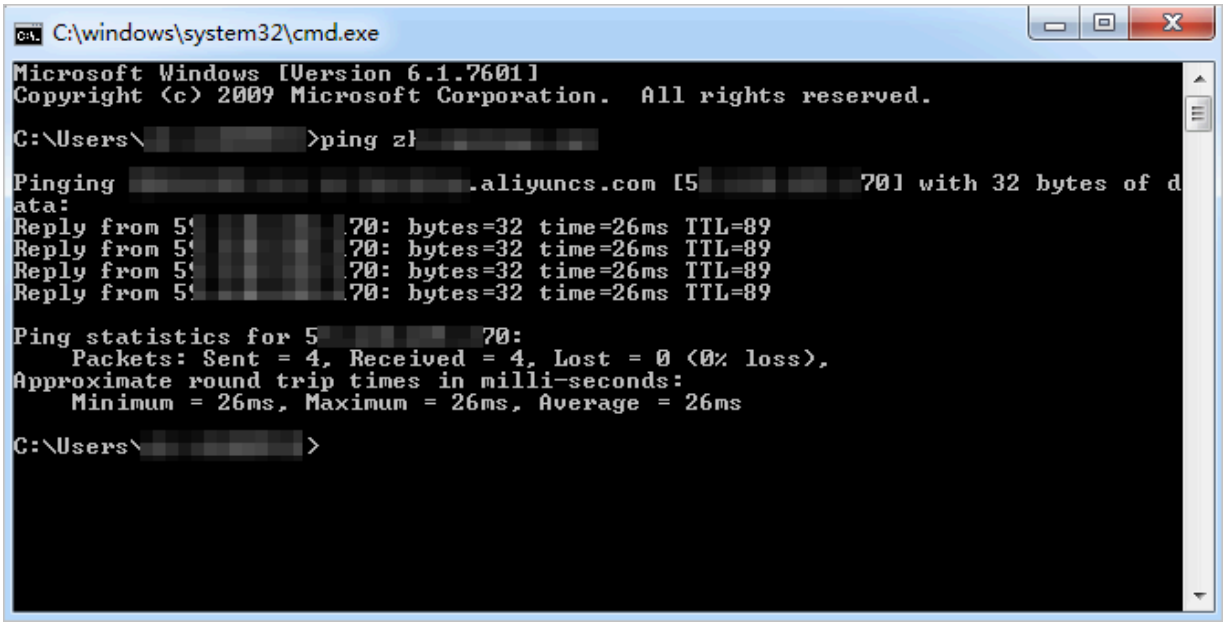
Parameter	Description
Host	Enter the host record according to the prefix of the domain name. For example: · If the domain name is `www . aliyun . com` , enter "www". · If the domain name is `aliyun . com` , enter a character "@". · If the domain name is `abc . aliyun . com` , enter "abc". · If the domain name is a second-level domain name, such as `a . aliyun . com` or `b . aliyun . com` , enter an asterisk "*".
ISP Line	Select the ISP line used to resolve the domain name. We recommend that you select Default to allow the system to select the optimal line.
Value	Enter the value of the record based on the selected record type. In this example, enter the Internet URL of the bucket.
TTL	Select the update period of the record. In this example, select the default value.

4. ClickOK.

 Note:
An added CNAME record takes effect immediately. However, modifications to a CNAME record take up to 72 hours to take effect.

Check CNAME status

After a CNAME record is configured, the time period required for the record to take effect varies according to DNS providers. You can run the `ping` or `lookup` command to check the status of an added CNAME. If it directs to `*. oss - cn -*. aliyuncs . com` , the CNAME has taken effect.

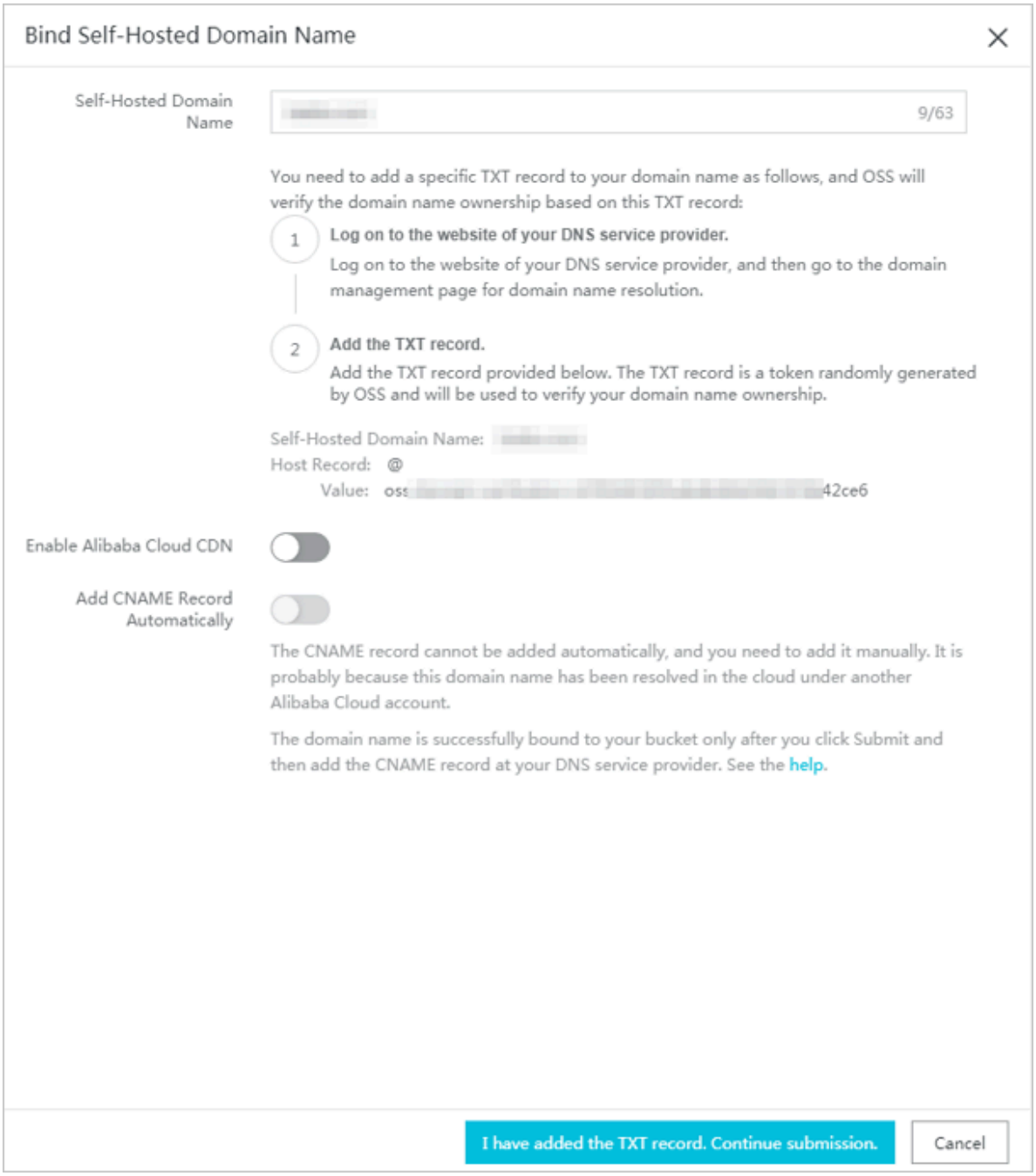


Verify domain name ownership

If your user domain name is attached to a bucket owned by another user, follow these steps to verify the ownership of the domain name and forcibly detach the domain name from the current bucket.

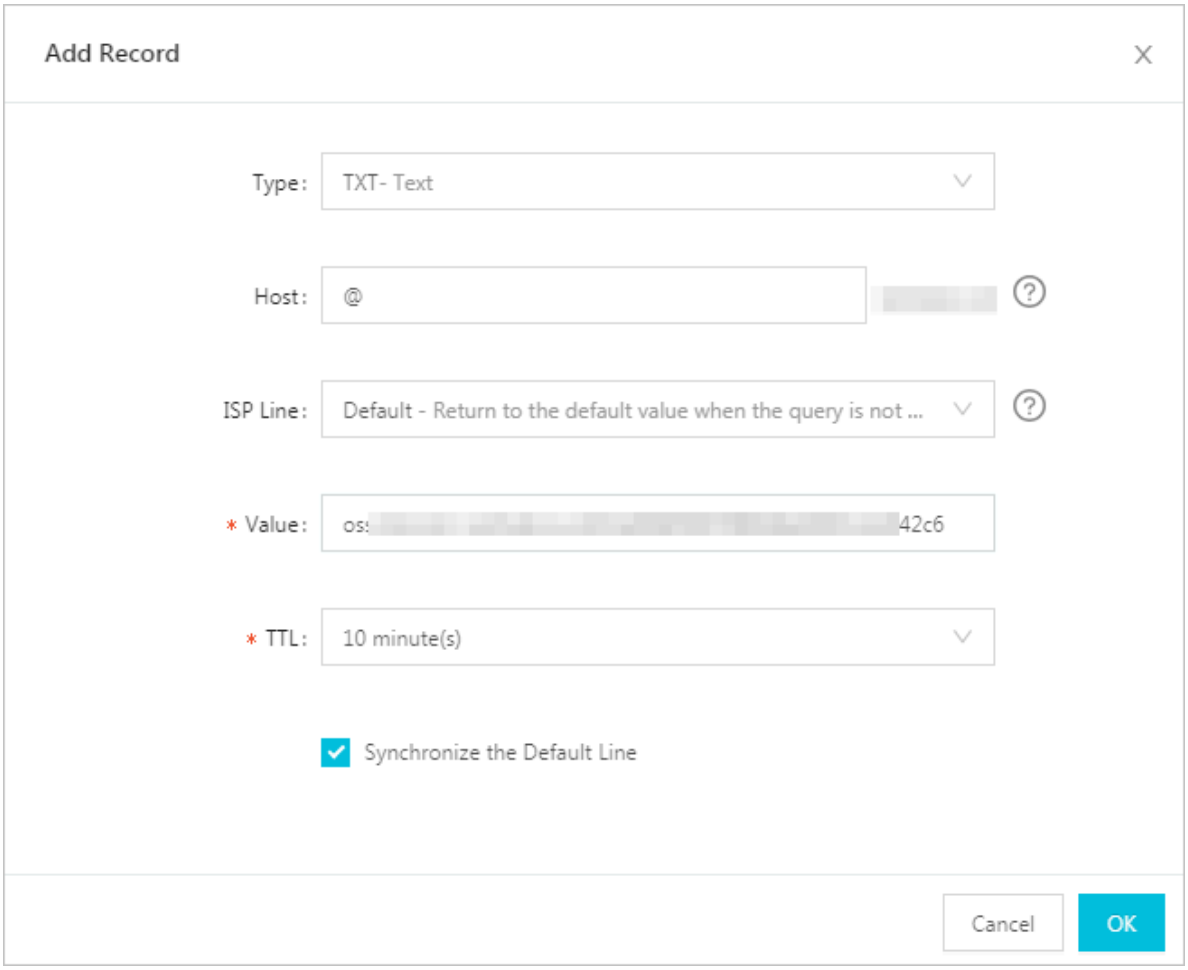
> Note:
> The following steps apply only in scenarios where a Domain name conflict message is prompted when you Attach a custom domain name.

1. Click Obtain TXT to obtain a txt record generated by the system based on your information.



2. Add the txt record to the DNS of your DNS provider. For a domain name added to Alibaba Cloud DNS, you can add a record in the Add Record page following the

procedures described in Manually add a CNAME record. Then, you can configure the parameters as follows:



- Type: Select TXT.
- Host: Enter "@".
- Value: Enter the value generated on theBind Self-Hosted Domain Name page in the OSS console.
- Retain default values for other parameters.

3. On the Bind Self-Hosted Domain Name page, click I have added the TXT record, Continue submission.. If the system confirms that the information is correct, the verification is passed.

1.7.2 Attach a CDN acceleration domain name

You can read objects in OSS buckets by using the Alibaba Cloud CDN-based acceleration service. The acceleration service uses OSS buckets as origin sites and distributes the content from the origin sites to edge nodes. With its precise scheduling system, Alibaba Cloud CDN assigns requests to optimal edge nodes so that

end users can quickly read their required content, easing Internet traffic congestion and improving response time.

To enable the Alibaba Cloud CDN-based acceleration service, you must direct your self-hosted domain name to a CDN acceleration domain name assigned by Alibaba Cloud CDN. Afterwards, all requests for your self-hosted domain name are redirected to the CDN edge nodes.

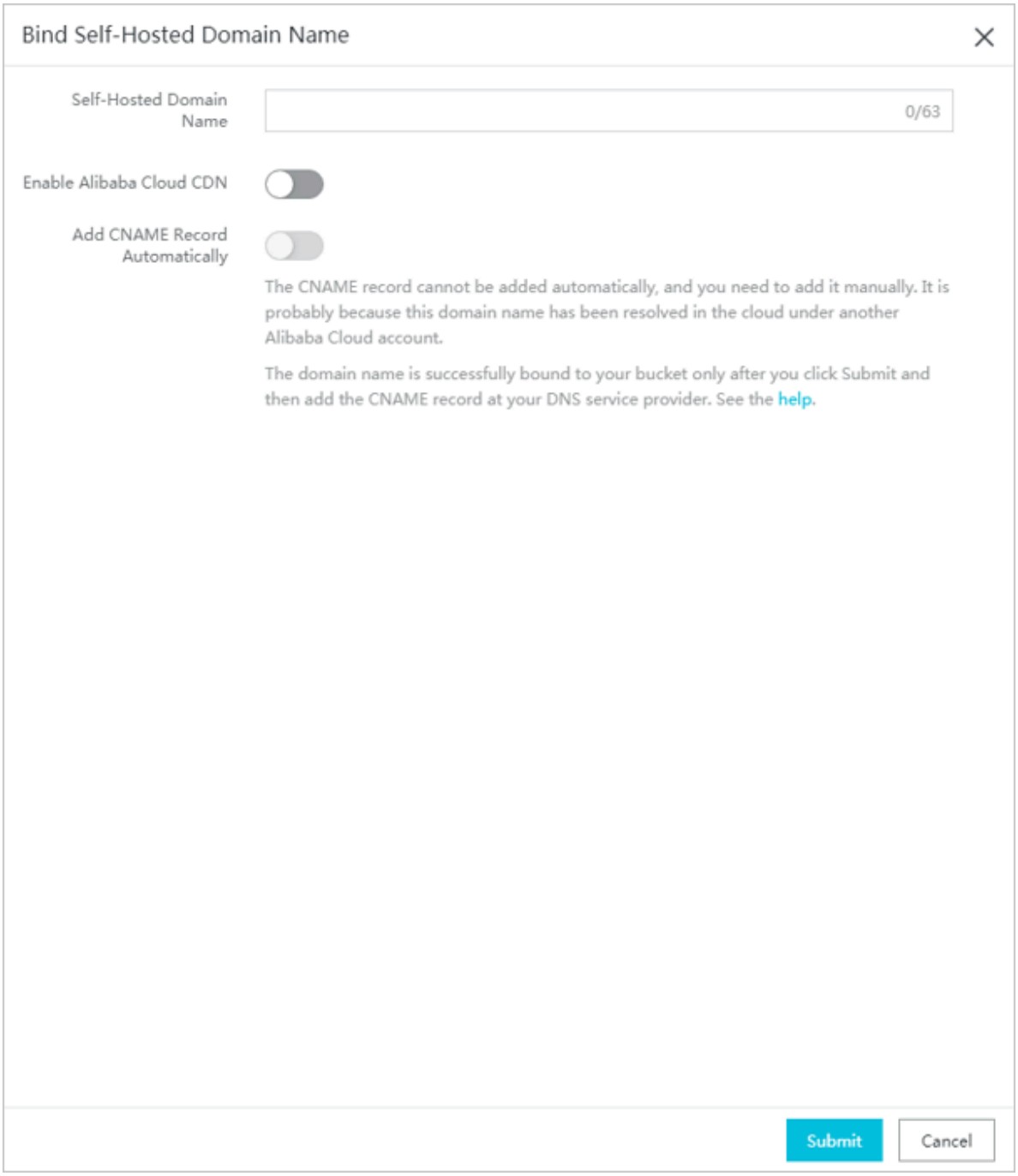
You can enable the Alibaba Cloud CDN-based acceleration service by the following two methods:

- Attach your self-hosted domain name to the domain name of an OSS bucket and enable the CDN-based acceleration service. For more information, see Method 1: Enable the CDN-based acceleration service through the OSS console.
- Direct the domain name of an OSS bucket to a CDN acceleration domain name, and then attach your self-hosted domain name to the CDN acceleration domain name (CNAME). For more information, see Method 2: Enable the CDN-based acceleration service through the CDN console.

Method 1: Enable the CDN-based acceleration service through the OSS console.

1. Log on to the OSS console. In the left-side bucket list, click the name of the bucket to which you want to attach a custom domain name.

2. Click Domain Names > Bind Self-Hosted Domain Name. In the Bind Self-Hosted Domain Name page, you can set the following parameters:



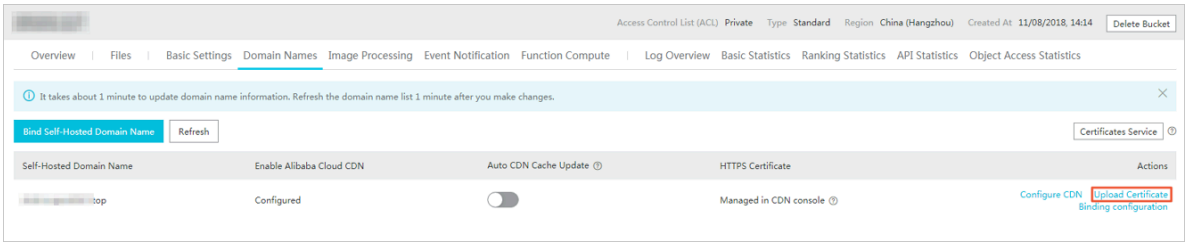
- Self-Hosted Domain Name: Enter the domain name that you want to attach, such as `hello-world.com`. The maximum length of a domain name is 63 characters.
- Enable Alibaba Cloud CDN: Enable the CDN-based accelerationservice.
- Add CNAME Record Automatically: The record of a CNAME managed by your Alibaba Cloud account can be automatically added. To add a record of a domain name that is not managed by your Alibaba Cloud account, you must manually

configure the DNS of your DNS provider. For more information, see Manually add a CNAME record.

3. Enter your self-hosted domain name, and enable Enable Alibaba Cloud CDN and Add CNAME Record Automatically.
4. Click Submit.

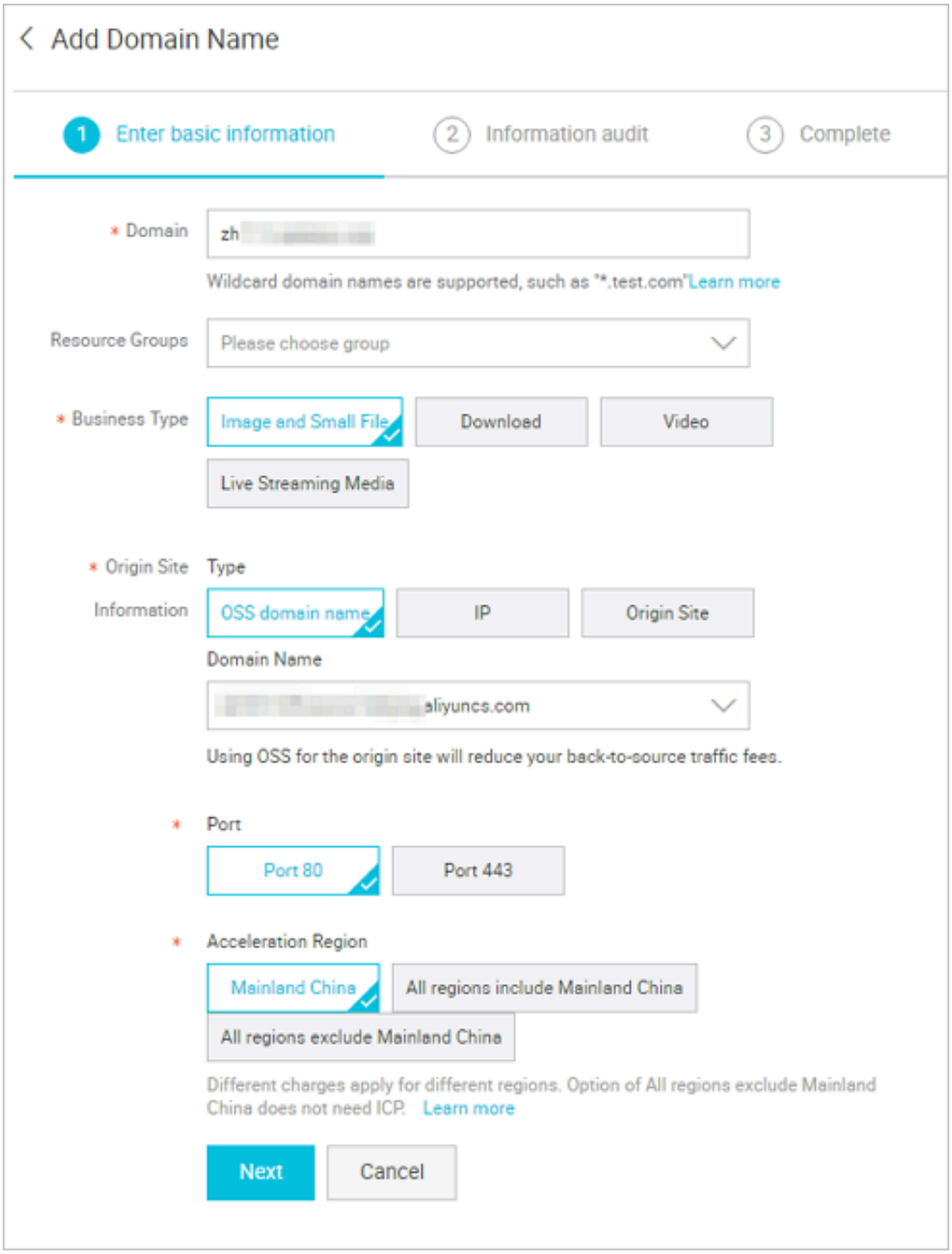
> Note:
> If a domain name conflict message is prompted, the domain name is currently attached to a bucket owned by another user. To resolve this issue, click Obtain TXT and add a txt record of the domain name to the DNS of your DNS provider to verify the ownership of the domain name and forcibly attach the domain name to your bucket. However, if you forcibly attach a domain name to a new bucket, the domain name is detached from the bucket to which it is currently attached. For more information, see Verify domain name ownership.

5. Updates to your domain name information take about one minutes to take effect. After updating a domain name, you can click Binding configuration to view CDN Domain Name and OSS Access Domain Name.



Method 2: Enable the CDN-based acceleration service through the CDN console.

1. Log on to the Alibaba Cloud CDN console.
2. Select Domain Names > Add Domain Name.
3. Enter the CDN acceleration domain name, and select the OSS bucket that you want to accelerate as the origin site.



Parameter	Description
Domain	Enter your domain name, such as ch.aliyun.com.
Resource Group	Select the default resource group.

Parameter	Description
Business Type	Select the optimal business type for your scenario based on the content you have stored in OSS and how it is generally used.
Origin Site Information	Select the OSS domain name that you want to accelerate.
Port	Select the access port as needed.
Acceleration Region	Select the region in which you want to use the acceleration service.

4. Click Next.

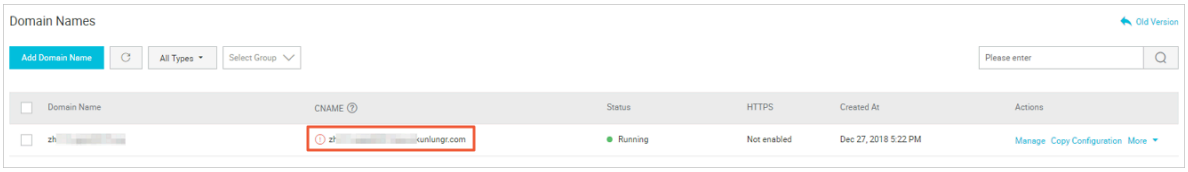
   After you add a CDN acceleration domain name, a CNAME record is generated. You must add the CNAME record to the DNS of your DNS provider to enable the CDN-based acceleration service. For more information, see Manually add a CNAME record.

Manually add a CNAME record

The following steps apply only to scenarios where a CNAME record is not automatica lly added.

You must add a CNAME record to the DNS of your DNS provider. In this topic, Alibaba Cloud DNS is used as an example to describe the process of adding a CNAME record.

1. Log on to the Alibaba Cloud CDN console and open the Domain Names page.



2. Copy the CNAME of the domain name that you want to add.
3. Log on to the Alibaba Cloud DNS console.
4. In the domain name list, click Configure on the right of the domain name that you want to add a record.

5. Click Add Record and enter the DNS information. The following table describes the parameters that you can configure.

Parameter	Description
Type	Select the type of record to which the domain name directs. In this example, select CNAME.
Host	Enter the host record according to the prefix of the domain name. For example: · If the domain name is `www . aliyun . com` , enter "www". · If the domain name is `aliyun . com` , enter a character "@". · If the domain name is `abc . aliyun . com` , enter "abc". · If the domain name is a second-level domain name, such as `a . aliyun . com` or `b . aliyun . com` , enter an asterisk "*".
ISP Line	Select the ISP line used to resolve the domain name. We recommend that you select Default to allow the system to select the optimal line.
Value	Enter the value of the record based on the selected record type. In this example, enter the CNAME record that you copied in Step 2.
TTL	Select the update period of the record. In this example, select the default value.

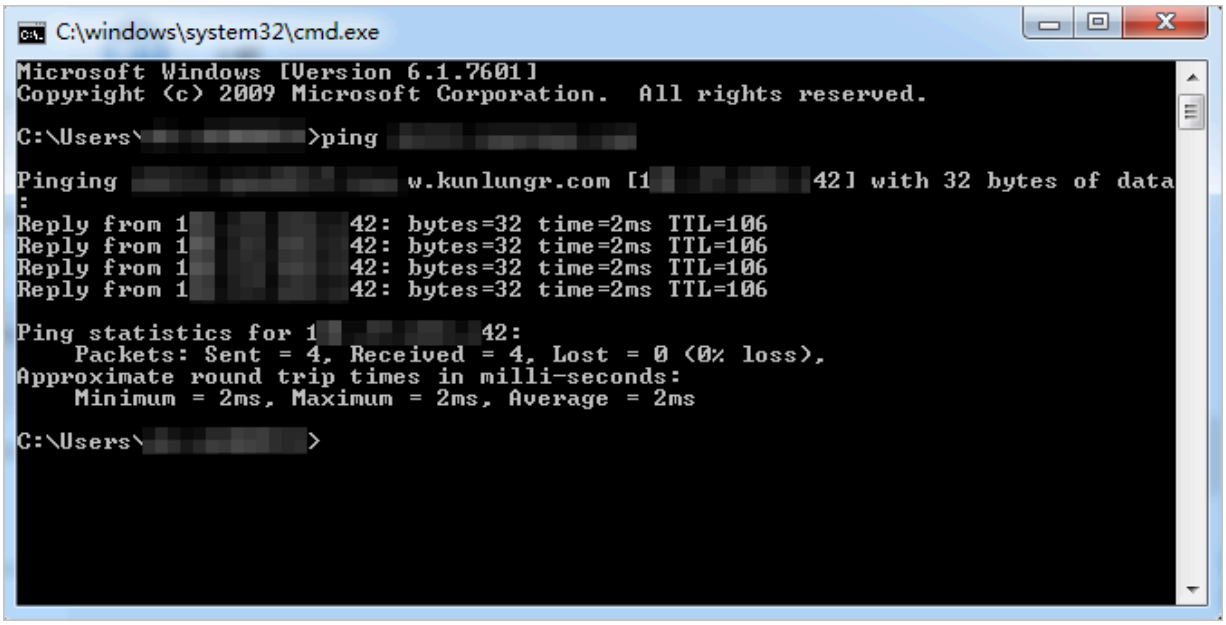
6. Click OK.

> **Note:**
> An added CNAME record takes effect immediately. However, modifications to a CNAME record take up to 72 hours to take effect.

Check CNAME status

After a CNAME record is configured, the time period required for the record to take effect varies according to DNS providers. You can run the `ping` or `lookup`

command to check the status of an added CNAME. If it directs to `*.* kunlun *. com` , the CNAME has taken effect.

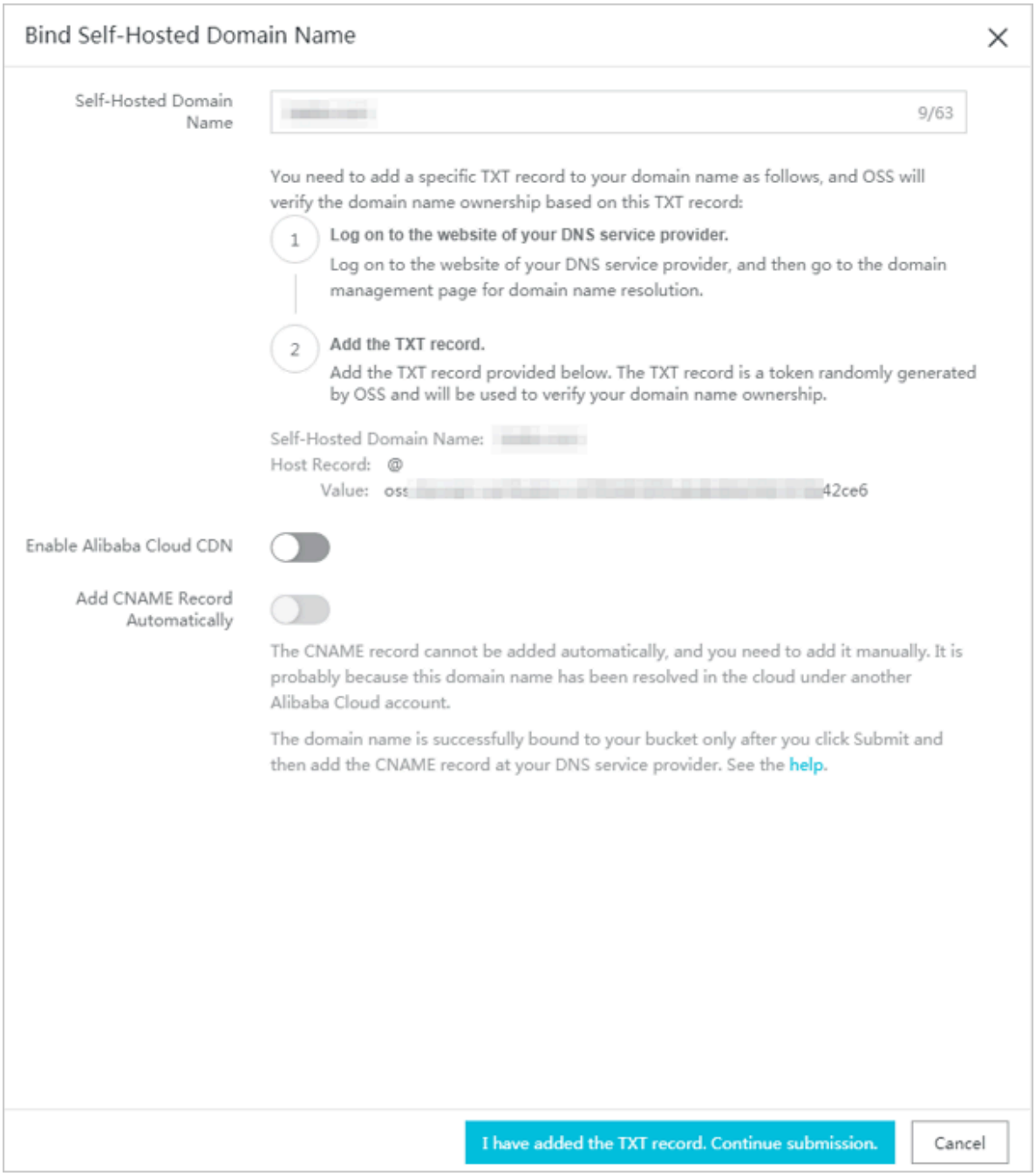


Verify domain name ownership

If your self-hosted domain name is attached to a bucket owned by another user, follow these steps to verify the ownership of the domain name and forcibly detach the domain name from the current bucket.

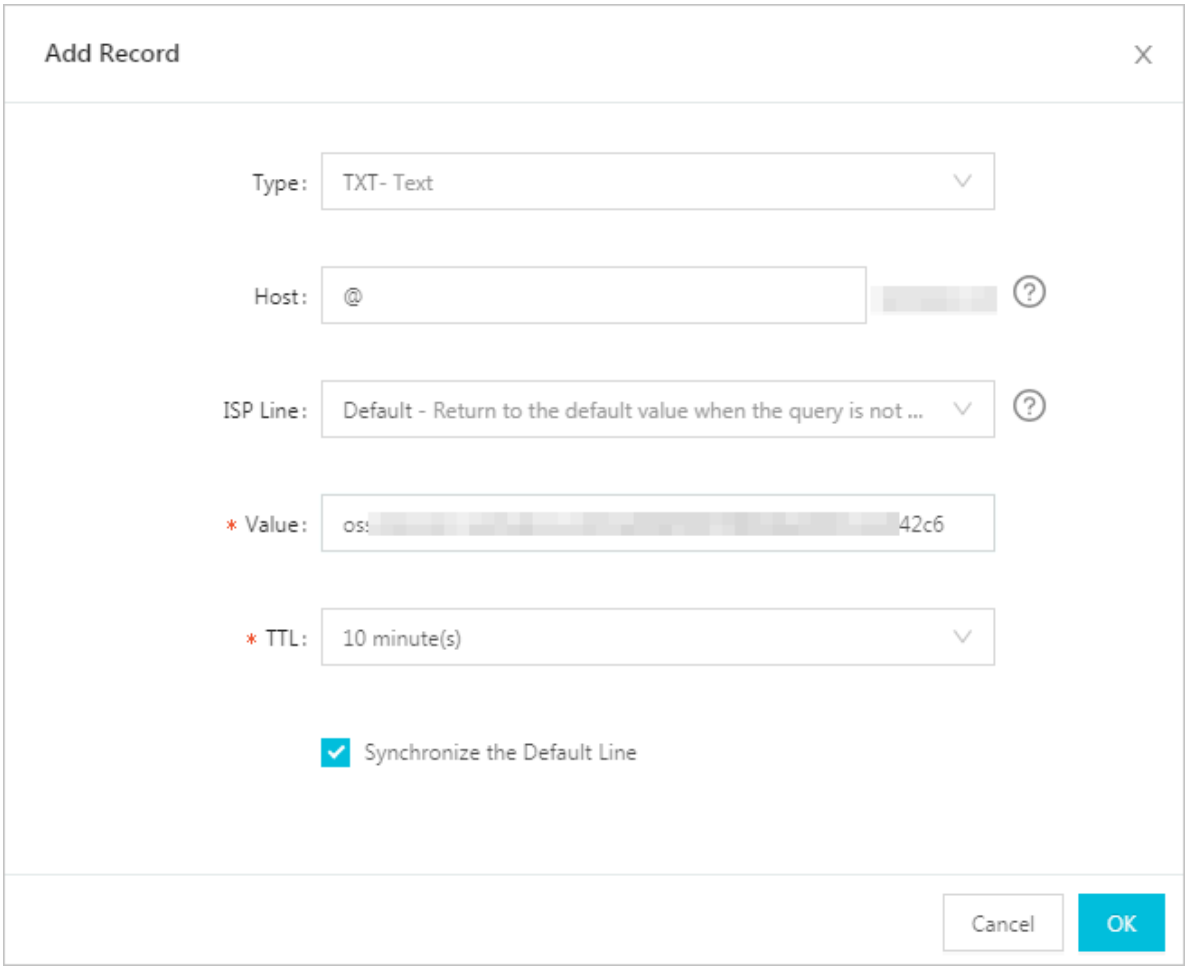
> Note:
> The following steps apply only in scenarios where a Domain name conflict message is prompted when you Attach a custom domain name.

1. Click Obtain TXT to obtain a txt record generated by the system based on your information.



2. Add the txt record to the DNS of your DNS provider. For a domain name added to Alibaba Cloud DNS, you can add a record in the Add Record page following the

procedures described in Manually add a CNAME record. Then, you can configure the parameters as follows:



- Type: Select TXT.
- Host: Enter a character "@".
- Value: Enter the value generated on the Bind Self-Hosted Domain Name page in the OSS console.
- Retain default values for other parameters.

3. On the Bind Self-Hosted Domain Name page, click I have added the TXT record, Continue submission.. If the system confirms that the information is correct, the verification is passed.

Enable auto CDN cache update

1. Log on to the OSS console.
2. In the left-side bucket list, click the name of the bucket that you want to enable the auto CDN cache update function.
3. Click the Domain Names tab.

4. Enable Auto CDN Cache Update for the record that a self-hosted domain name is attached.

After the auto CDN cache update function is enabled, modifications to an object in the bucket are automatically updated to the CDN cache.

 Note:
If you detach your self-hosted domain name from the bucket, the auto CDN cache update function is not supported in the OSS console. However, you can update the CDN cache in the Alibaba Cloud CDN console.

AccessDenied error

After attaching a self-hosted domain name to a bucket, you can access a target OSS resource using the URL that is composed of your self-hosted domain name and the path of the resource, such as `http :// mydomain . cn / test / 1 . jpg`. However, if you access OSS only with your self-hosted domain name (such as `http :// mydomain . cn`) an AccessDenied error occurs because the default page of the OSS static website is not configured. For more information about configuring the default page of an OSS static website, see Host a static website.

1.7.3 Certificate hosting

If your want to use your user domain name to access OSS services through the HTTPS protocol, you must purchase a digital certificate. You can purchase certificate

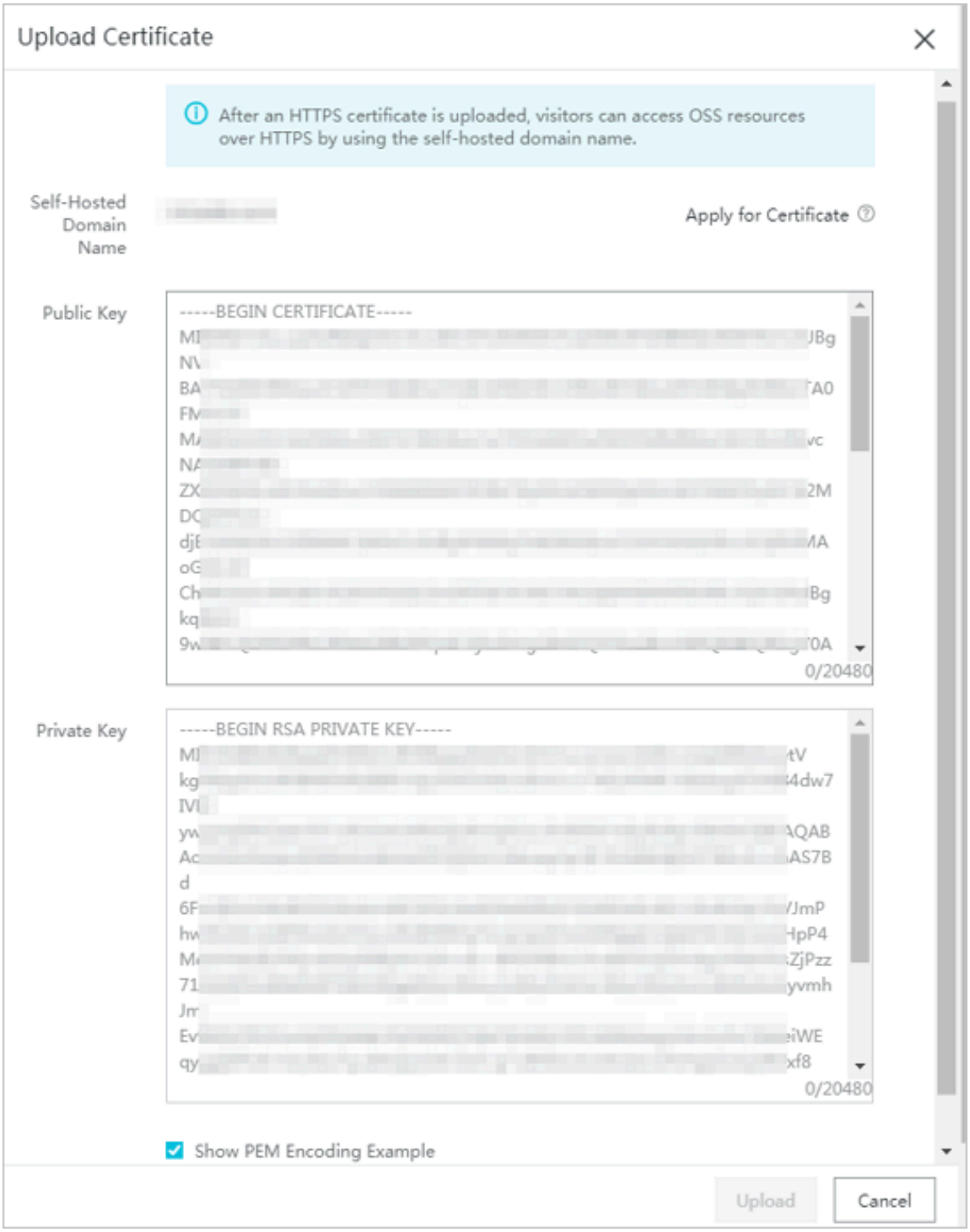
services from any certificate authority (CA) or purchase a certificate from Alibaba Cloud SSL Certificates Service and host your certificate on OSS.

Procedure

- Alibaba Cloud CDN is not enabled

  After you Attach a custom domain name, follow these steps to host your certificate in the OSS console.

  1. Log on to the OSS console. In the left-side bucket list, click the bucket attached with the host name that you want to host your certificate.
  2. Click the Domain Names tab.
  3. Click Upload Certificate on the right of the domain name that you want to host your certificate.
  4. On the Upload Certificate page, enter the public key and private key in your certificate, and then click Upload.



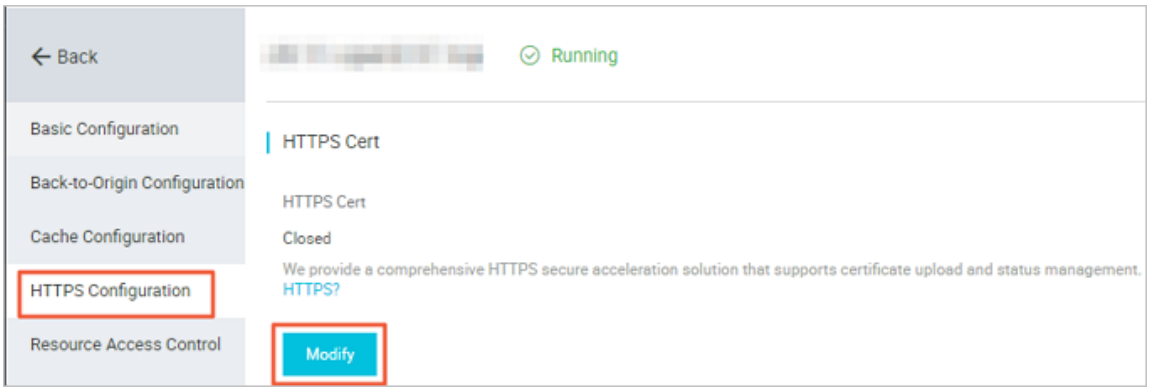
Note:

You can select Show PEM Encoding Example to view public key and private key examples. For more information about the certificate format, see Certificate format.

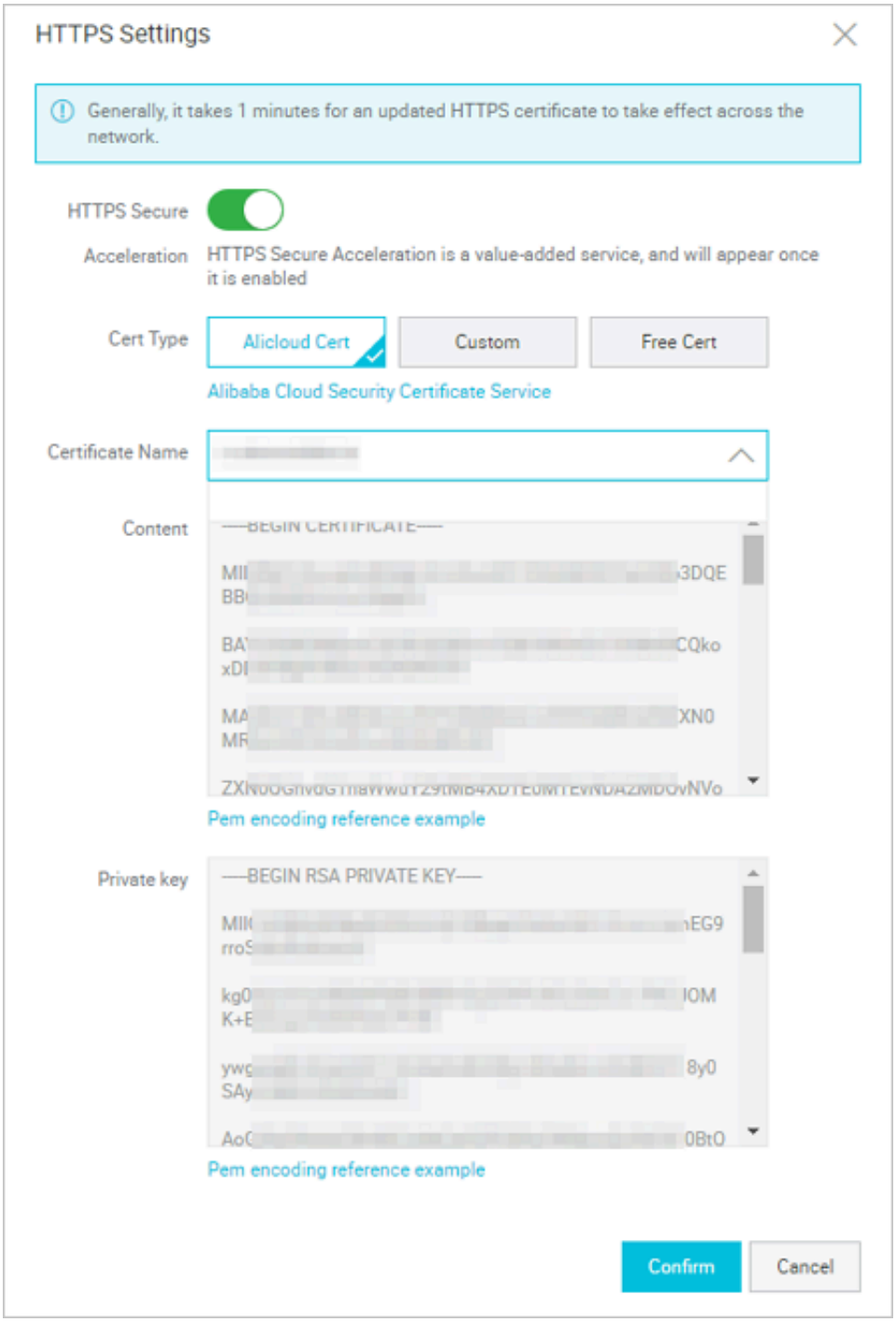
- Alibaba Cloud CDN is enabled

  After you Attach a CDN acceleration domain name, you can manage HTTPS certificates in the CDN console.

  1. Log on to the CDN console.
  2. Click Domain Names. Select the domain name that you want to host your certificate and click Manage.
  3. Click HTTPS configuration > Modify.



  4. In the HTTPS Settings dialog box, enable HTTPS HTTPS Secure .
  5. Select a certificate. You can select the following certificate types: Alicloud CertCustom, and Free Cert. Only the `PEM` certificate format is supported.



- Alicloud Cert: Select your SSL certificate.
- Custom: You must upload the certificate and the private key after configuring the certificate name. The uploaded certificate is stored in Alibaba Cloud SSL Certificates Service. You can view the certificate in SSL Certificates.
- You can also select a free certificate, that is, a free Digicert DV SSL certificat e provided by Alibaba Cloud. However, a free CDN certificate only applies to the HTTPS Secure Acceleration service of CDN. Therefore, you cannot configure a free certificate in the Alibaba Cloud SSL Certificates console and

cannot view the public key and the private key of a free certificate. A free certificate takes up to 10 minutes to take effect.

6. A purchased certificate takes about one hour to take effect. After the certificate takes effect, you can access OSS resources through the HTTPS protocol. If a green HTTPS mark is displayed, it indicates that the HTTPS Secure Acceleration service has taken effect.

1.8 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.

Note:

When you use an OSS endpoint in Mainland China regions or the China (Hong Kong) region to access a web file through the Internet , the Content-Disposition: 'attachment=filename;' is automatically added to the Response Header, and the web file is downloaded as an attachment. If you access OSS with a user domain, the Content-Disposition: 'attachment=filename;' will not be added to the Response Header. For more information about using the user domain to access OSS, see Bind a custom domain name.

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.

1.9 Set anti-leech

OSS is a Pay-As-You-Go service. To reduce extra fees caused in case your data on OSS is used by unauthorized users, OSS supports the anti-leech function based on the Referer header field in HTTP or HTTPS requests. You can configure a Referer whitelist for a bucket and configure whether to allow access requests with an empty Referer field in the OSS console.

Procedure

1. Log on to the OSS console.
2. In the left-side the bucket list, click the bucket that you want to set anti-leech for.
3. In the overview page of the bucket, click the Basic Settings tab, and then click Configure in the Anti-Leech area.
4. Enter the following information:
   - Referer Whitelist: Add one or more Referers into the whitelist and separate them with line breaks. Referers are usually URLs and support asterisks (*) and question marks (?) as wildcards.

     If you set the Referer whitelist for a bucket named *test-1-001* to *http :// www . aliyun . com* , only requests in which the Referer field is `http :// www . aliyun . com` can access the objects in the bucket *test-1-001*.
   - Allow Empty Referer: Configure whether to allow access requests in which the Referer field is empty. If you does not allow empty referer, only HTTP or HTTPs request which include the Referer header can access the objects in the bucket.
5. Click Save.

Reference

- For more information about the anti-leech function, see Set anti-leech.
- For more information about the principle of anti-leech, see Anti-leech.
- For FAQs and troubleshooting for anti-leech, see Referer.

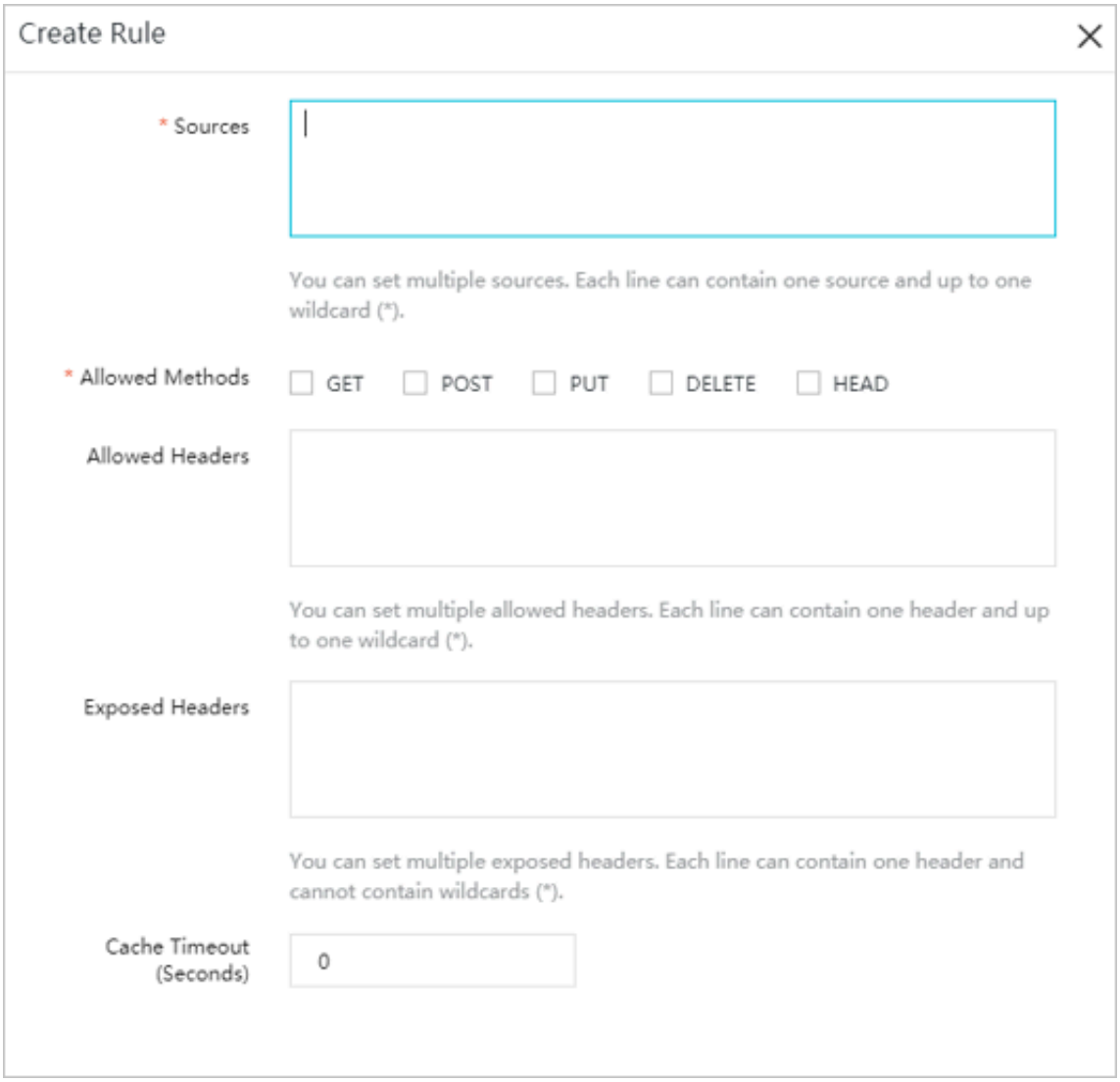
1.10 Configure CORS rules

OSS provides Cross-Origin Resource Sharing (CORS) in the HTML5 protocol to help users achieve cross-origin access. When OSS receives a cross-origin access request (or OPTIONS request) for a bucket, it reads the CORS rules for the bucket and then checks relevant permissions. OSS matches the rules with the request in sequence , uses the first rule that matches to allow the request, and returns the correspond ing header. If none of the rules match the request, no CORS header is carried in the returned result.

Procedure

1. Log on to the OSS console.
2. In the left-side bucket list, click the name of the bucket that you want to configure CORS rules.
3. Click the Basic Settings tab. In the Cross-Origin Resource Sharing (CORS) area, click Configure.

4. Click Create Rule. In the CORS Rule dialog box, set the following parameters:



Parameter	Required	Description
Source	Yes	Specifies the sources of allowed CORS requests. You can configure multiple matching rules for the source. Multiple rules must be configured in separate lines. Up to one asterisk (*) wildcard can be used in a rule. If a rule includes only an asterisk (*) wildcard, it allows CORS requests from all sources.
Allowed Methods	Yes	Specifies the allowed CORS request methods.

Parameter	Required	Description
Allowed Headers	No	Specifies the response headers for the allowed CORS requests. You can configure multiple matching rules for the allowed headers. Multiple rules must be configured in separate lines. Up to one asterisk (*) wildcard can be used in a rule. Set this parameter to * if there is no special business requirements.
Exposed Headers	No	Specifies the response headers that users are allowed to access from an application (for example, a Javascript XMLHttpRequest object). Asterisks (*) cannot be used in exposed headers.
Cache Timeout	No	Specifies the cache time for the returned results of browser prefetch (OPTIONS) requests to a specific resource.

Note:

You can configure up to 10 CORS rules for a bucket.

5. Click OK.

Note:

You can also edit or delete an existing rule.

1.11 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 Ruleto 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

        Note:
       For the billing information about objects whose storage classes are converted, see Manage object lifecycle.
     - 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.

1.12 Configure cross-region replication

Cross-region replication is used to automatically and asynchronously copy objects across buckets in different regions. Any changes (creation, replacement, and deletion) to objects in the source bucket will be synchronized to the target bucket.

 Note:

· Currently, the cross-region replication feature is only supported between different regions in Mainland China and between the US West 1 (Silicon Valley) and US East 1 (Virginia) regions.

· The cross-region replication function is in the beta testing phase and is free currently. The function is charged after it is officially released.

Procedure

1. Log on to the OSS console.
2. In the left-side bucket list, click the name of the bucket that you want to configure cross-region replication.
3. Click the Basic Settings tab and find the Cross-Region Replication (CRR) region.
4. Click Enable to open the Cross-Region Replication (CRR) dialog box.
5. Select the region and the name of the target bucket.

   Note:

   - The source bucket and target bucket in synchronization must be in different regions.
   - Two buckets with cross-region replication enabled cannot be synchronized to other buckets.
6. Select from the following two options for Applied To.
   - All Files in Source Bucket: Synchronizes all objects in the bucket to the target bucket.
   - Files with Specified Prefix: Synchronizes the objects with specified prefixes in the bucket to the target bucket. For example, you have a folder named `management` in the root directory of a bucket and a folder named `abc` under `management`. If you want to synchronize objects in the `abc` folder, add the `management / abc` as the prefix. You can add a maximum of five prefixes.
7. Select from the following options for Operations:
   - Add/Delete/Change: Synchronizes all data in the bucket (including the add, change, and delete operations) to the target bucket.
   - Add/Change: Synchronizes only added or changed data in the bucket to the target bucket.
8. Select whether to Replicate Historical Data.

   Note:
   If you enable Replicate Historical Data, objects replicated from the source bucket may overwrite the objects with the same names in the target bucket. Therefore, ensure the data in the source and target buckets is consistent 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. Information related to synchronization is displayed after the source bucket is synchronized.
- In cross-region replication, data is replicated asynchronously. Therefore, it usually takes several minutes or hours to replicate data to the target bucket according to the data size.

1.13 Set back-to-origin rules

This topic describes how to set back-to-origin rules.

If you access data that does not exist on OSS, a 404 Not Found error is return. However, if you set back-to-origin rules and set the correct URL for the data, you can obtain the data correctly through the back-to-origin rules. Two kinds of back-to-origin rules can be set: mirroring rules and redirection rules, which can meet the requirements of frequently accessed (hot) data migration and specific request redirection requirements. You can set a maximum of 5 back-to-origin rules, which are compared with access requests in a sequence that they are set. For more information, see Manage back-to-origin settings.

Note:
The back-to-origin function does not support intranet endpoints. Internet traffic generated by the function are charged at normal rate.

Procedure

1. Log on to the OSS console.
2. In the left-side bucket list, click the bucket that you want to set back-to-origin rules for.
3. In the overview page of the bucket, click the Basic Settings tab, locate the Back-to-Origin area, and click Configure.
4. Click Create Rule.

5. In the Create Rule dialog box, configure parameters as follows to create a back-to-origin rule.

Parameter	Required	Description
Mode	Yes	Select Mirroring or Redirection. · In the Mirroringmode, if the object requested by the user does not exist in OSS, OSS obtains the object from the origin site and returns the object to the user. · In the Redirection mode, requests that meet the response requirement are redirected to specified URLs using the HTTP redirection method. Browsers or clients obtain the request data from the origin site through the URLs.

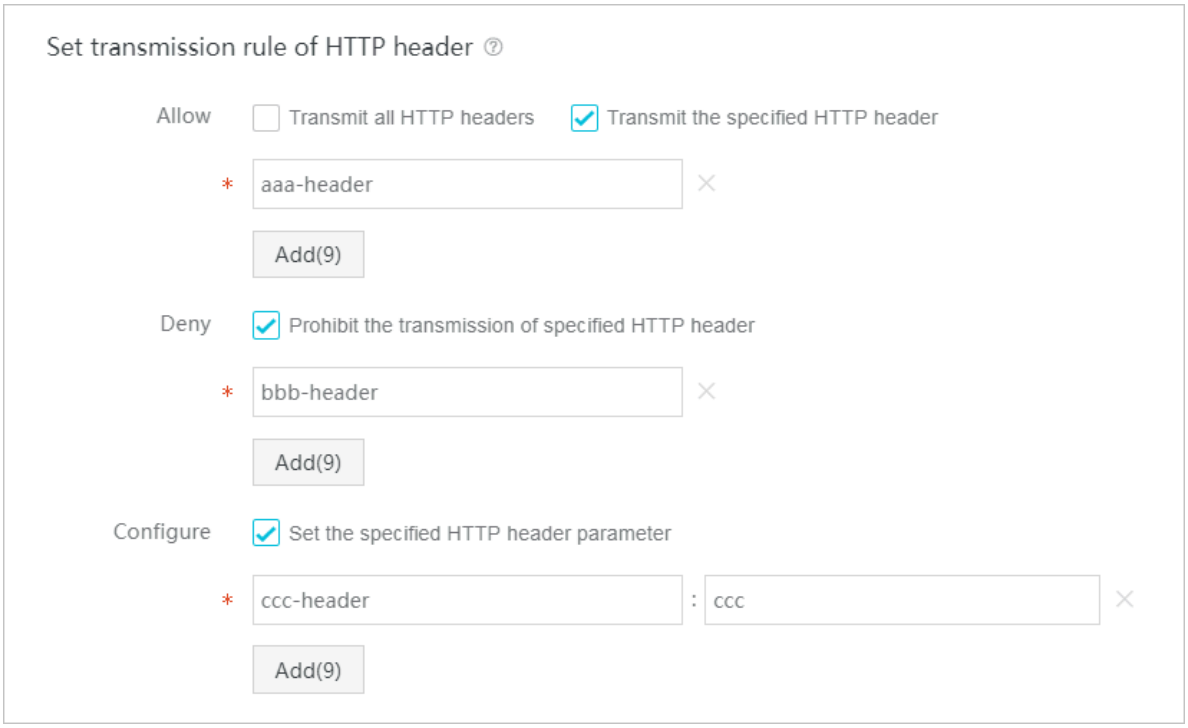
Parameter	Required	Description
Prerequisite	Yes	Set the conditions that trigger the back-to-origin rule. A rule is triggered only when all the conditions are met. · HTTP Status Code: The back-to-origin rule is triggered when the specified HTTP status code is returned. The default HTTP status code is 404, that is, the rule is triggered when the requested object does not exist in OSS and a 404 HTTP status code is returned. This condition is selected by default and cannot be configured when you select the Mirroring mode, and is optional when you select the Redirction mode. · File Name Prefix: The back-to-origin rule is triggered when objects with the specified prefix are accessed. For example, if you set the prefix to *abc /*, the rule is triggered when the `http :// bucketname . oss - endpoint . com / abc / image . jpg` object is accessed. Note: This condition is optional when you create a single back-to-origin rule. When creating multiple back-to-origin rules, you must set different prefixes for different rules.

Parameter	Required	Description
Origin URL	Yes	Sets the origin URL. Directories with multiple levels must be separated by slashes (/). If you select the Redirection mode, a directory must end with a slash (/), and asterisks (*) are not supported. · If you select the Mirroring mode, configure the origin URL as follows: - First column:Select http or https based on the type of the origin site. - Second column: Input the domain name or IP address of the origin site.  Note: Input the IP address only when the origin site can be directly accessed through the IP address. - Third column: Input the directory where the requested object is stored. For example, *abc / 123* . · If you select the Redirection mode, you must set the processing rule for the origin URL. The configurations of the first and second column are similar to those when you select the Mirroring mode. - Add Prefix or Suffix: Adds a prefix or suffix to the redirected URL, in which the prefix is configured in the third column and the suffix is configured in the fourth column. You can select this option to configure correct information for the redirected URL when the URL of the requested data does not have a prefix or suffix. For example, if you set the prefix to `123 /` and the suffix to `. jpg` , access to `http :// bucketname . oss - endpoint . com / image` is automatically redirected to `http :// xx . com / 123 / image . jpg` . - Redirect to Fixed URL: Access to the

Parameter	Required	Description
Other parameters	No (only applies for the Mirroring mode)	Transfer queryString: The queryString included in the request to OSS is transferred to the origin site.
3xx Response	No (only applies for the Mirroring mode)	Follow the source station to redirect request: The requested data is obtained through the 3xx redirection request sent to the origin site and stored in OSS by default. If you do not select this option, OSS passes through the 3xx response and does not obtain the data.
Set transmission rule of HTTP header	No (only applies for the Mirroring mode)	You can set transmission rule for HTTP headers to customize transmission actions, such as passthrough, filtering, or modifying. For more information, see the following examples of setting transmission rules for HTTP headers.

Parameter	Required	Description
Redirection Code	Yes (only applies for the Redirection mode)	You can select the redirection code. Source from Alibaba Cloud CDN: Select this option if the origin site is from Alibaba Cloud CDN.

Examples of setting transmission rules for HTTP headers are listed as follows:



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 site is as follows:

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

Note:

Transmission rules do not support the following HTTP headers:

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

6. Click OK.

Note:
After a back-to-origin rule is saved, you can view the configured rule in the rule list and perform Edit or Clear operations.

1.14 Configure bucket tagging

OSS allows you to configure bucket tagging to classify and manage buckets. For example, you can configure this feature to list only buckets that have specific tags. This topic describes how to configure bucket tagging in the OSS console.

Context

Bucket tagging uses a key-value pair to identify buckets. You can manage multiple buckets that have the same tag.

- Only the bucket owner can configure tagging for the bucket. If other users attempt to configure tagging for the bucket, 403 Forbidden is returned with error code AccessDenied.
- You can configure a maximum of 20 tags for a bucket.
- The tag key is required. The tag key can be a maximum of 64 characters in length and cannot start with `http://`, `https://`, or `Aliyun`.
- The tag value is optional. The tag value can be a maximum of 128 characters in length.
- The key and value of the tag must be encoded in UTF-8.

For more information about bucket tagging, see Bucket tagging.

Procedure

1. Log on to the OSS console.
2. On the left-side bucket list, click the target bucket to open the overview page of the bucket.
3. Click the Basic Settings tab, find the Bucket Tag section.
4. Click Configure and add tags.
5. Click Save.

1.15 Delete a bucket

You can delete a bucket that is no longer need to save storage cost.

Prerequisites

Before deleting a bucket, ensure that all objects (including fragments generated in multipart upload tasks) in the bucket are deleted. Otherwise, the bucket cannot be deleted.

Note:

- If you want to delete all objects in a bucket, we recommend that you Set lifecycle for the bucket.
- For more information about how to delete fragments, see Manage fragments.

Procedure

1. Log on to the OSS console.
2. In the left-side bucket list, click the bucket that you want to delete, and then click the Basic Settings tab.
3. In the Bucket Management area, click Delete Bucket.
4. In the displayed dialog box, click OK.

Warning:
Delete a bucket with caution because a deleted bucket cannot be restored.

2 Upload、download and manage objects

2.1 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.

2.2 Upload objects

After creating a bucket, you can upload objects of any type to the bucket.

Before you begin:

You must create a bucket before uploading objects to it. For more information, see Create a bucket.

About this task:

You can upload objects in the following methods:

- Upload objects smaller than 5 GB in the OSS console.
- Upload objects larger than 5 GB in the multipart upload method by using OSS SDK or API. For more information, see Multipart upload.
- Use the graphical tool ossbrowser to upload objects. For more information, see ossbrowser.

Procedure

1. Log on to the OSS console.
2. In the left-side bucket list, click the bucket that you want to upload objects to.

3. In the overview page of the bucket, click the Files tab.
4. Click Upload.

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 Upload dialog box, set the folder where you want to upload objects to in Upload To.
   - Current: Objects are uploaded to the current folder.
   - Specified: Objects are uploaded to the specified folder. You must enter the name of the specified folder. OSS automatically creates the specified folder and uploads the object to it automatically

Note:

For more information about folders, see Create a folder.

6. Select the ACL for the object to be uploaded in File ACL. You can select one of the following four ACLs, in which Inherited from Bucket is the default ACL.
   - Inherited from Bucket: The ACL for the object is the same as the ACL for the bucket.
   - Private: Only authorized users can access the object.
   - Public Read: All users (including anonymous users) can read the object. Only authorized users can write the object.
   - Public Read/Write: All users can read and write the object.

   For more information about ACL, see Change object ACL.
7. Drag one or multiple objects that you want to upload to the Upload area, or click click here to upload to select the objects that you want to upload.

Note:

- If the name of the object that you want to upload is the same as that of an existing object, the existing object is overwritten.
- Do not refresh or close the upload page when objects are being uploaded. Otherwise, the upload tasks are interrupted and the upload object list is cleared .

2.3 Create a folder

Alibaba Cloud OSS does not has 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.

2.4 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.

2.5 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 #unique_69.
- 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

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.

2.6 Modify the storage class of an object

OSS provides three storage classes: Standard, Infrequent Access (IA), and Archive. Each storage class has different access modes, billing items, and billing methods. You can select a storage class as needed. This topic describes how to modify the storage class of an object in the OSS console.

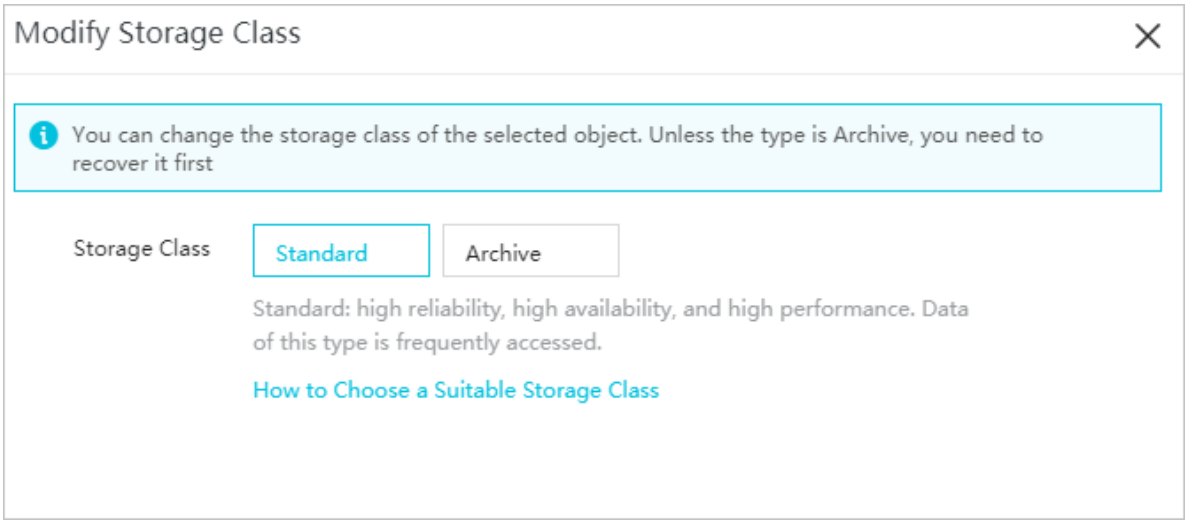
Prerequisites

- When you modify the storage class of an object in the OSS console, the object size cannot exceed 5 GB. We recommend that you use ossutil to modify objects that are greater than 5 GB.
- You can modify the storage class of an Archive object only after the object is restored.

Procedure

1. Log on to the OSS console.
2. In the left-side bucket list, click the name of the bucket in which the object to be modified is stored.
3. In the overview page of the bucket, click the Files tab.
4. Move the pointer over More in the Actions column corresponding to the object and select Modify Storage Class from the drop-down list.

5. Select the storage class you want to switch to, and click OK.



Notice:
When you modify the storage class of an object, the original object is replaced with a new object that has the selected storage class. Therefore, early deletion fees are incurred if the modified objects are of the IA or Archive storage class and are stored for less than a specified number of days. For more information, see Billing items.

2.7 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 policy, bucket policies can be directly configured by the bucket owner on 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 efficientl y.

Authorize RAM users of other accounts to access your OSS resources

1. Log on to the OSS console.
2. In the left-side bucket list, 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. For Accounts, select from the following options:
   - Sub Account: Select a RAM user under the current account from the drop-down list to grant bucket access permission to it. To select this option, you must log on to the console with your Alibaba Cloud account or as a RAM user that has the management permission on the bucket and the `ListUsers` permission on the RAM console.
   - Other Account: If you want to grant the bucket access permission to another account or your account does not have the `ListUsers` permission, enter the UID of the account to which you want to grant the permission.
   - Anonymous Account (*): If you want to grant permissions to all users, you can select Anonymous Account (*).

Note:

To grant the `ListUsers` permission to a RAM user, see

- Authorize RAM users.

- The following code template can be used to grant the `ListUsers` permission to a RAM user.

```
{
    " Version ": " 1 ",
    " Statement ": [
        {
            " Effect ": " Allow ",
            " Action ": [
                " ram : ListUsers "
            ],
            " Resource ": [
                "*"
            ],
            " Condition ": {}
        }
    ]
}
```

7. Configure `Authorized Operation` .
   - `Read - Only` : Authorized users can view, list, and download 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 for 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 left-side bucket list, 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 view, list, and download 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 some users, the users' access is determined by the combination of these policies. However, the users cannot perform any operation if the authorized operation is configured to `None` (Deny) in any of the policies. For example, if the authorized operation for some users is configured to `Read Only` in a bucket policy and `Read/Write` in another, the users have the `Read/Write` access which is the combination of the `Read Only` and `Read/Write` access. If the authorized operation of the users is configured to `None` (Deny) in another policy, the users only have 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.

2.8 Download an object

After uploading an object to a bucket, you can obtain the URL of the object to download it or share it with other users.

Prerequisites

The object has been uploaded to the bucket. For more information, see Upload an object.

Procedure

1. Log on to the OSS console.

2. In the left-side bucket list, click the name of the bucket that you created.
3. In the overview page of the bucket, click the Files tab.
4. Click the name of the object that you want to download or share, or click Preview on the right of the object. In the Preview page, you can see the following options:

   · Download: Download the object to your local storage device.

   Depending on how many objects you require, you can also download objects by using the following methods:

   - Download multiple objects: On the Files tab page, select multiple objects, and then choose Batch operation > Download.
   - Download a single object: On the Files tab page, select an object, and then choose More > Download.

   · Open File URL: View an object in a browser. The object that cannot be viewed in a browser (such as Excel files) is downloaded when the URL is opened.

    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.

   · Copy File URL: Copy the URL of the object and share it with other users, so that they can use the URL to view or download the object.

   You can also obtain the URL of an object in the following methods:

   - Obtain the URL of one or more objects: On the Files page, select one or more objects, and then select Batch operation > Export URL List.
   - Obtain the URL of a single object: On the Files page, select More > Copy File URL.

   If you want to share the URL of an object whose ACL is Private, you must set the Validity Period on the Preview page when you want to obtain the URL of an object. The default value of the validity period is 3,600 seconds, and the maximum value is 64,800 seconds.

    Note:

   - The validity period of a signed URL is calculated based on NTP. You can share the signed URL of an object to other users so that they can use the URL to access the object within the validity period. If your objects ACL is Private, a

signature is added to the URL of the objects stored in the bucket. For more information, see #unique_69.

- For more information about how to change buckets and objects ACL, see Change bucket ACLand Change object ACL.

· Copy File Path: Copy the path of the object. You can use the path when searching for the object or adding watermarks to the object (if it is a picture).

2.9 Set an HTTP header

HTTP header is used to define the policy of HTTP requests, such as cache policy or download policy. You can set an HTTP header for up to 1,000 files using the batch process in the OSS console.

Note:
If you want to set an HTTP header for more than 1,000 files, see the Java SDK document Manage Object Meta.

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.

2.10 Delete an object

You can delete a single object or multiple objects (up to 1,000 at a time) in the OSS console. If you want to select and delete objects in a more flexible manner or delete more than 1,000 objects at a time, see Delete an object in the OSS Developer Guide.

Warning:
A deleted object cannot be recovered. Exercise caution when performing this action.

Procedure

1. Log on to the OSS console.
2. In the left-side bucket list, click the name of the target bucket.
3. On the overview page of the bucket, click the Files tab.
4. Select one or more objects, and then select Batch operation > Delete. You can also select More > Delete on the right of the object you want to delete.
5. In the displayed dialog box, click OK.

2.11 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.

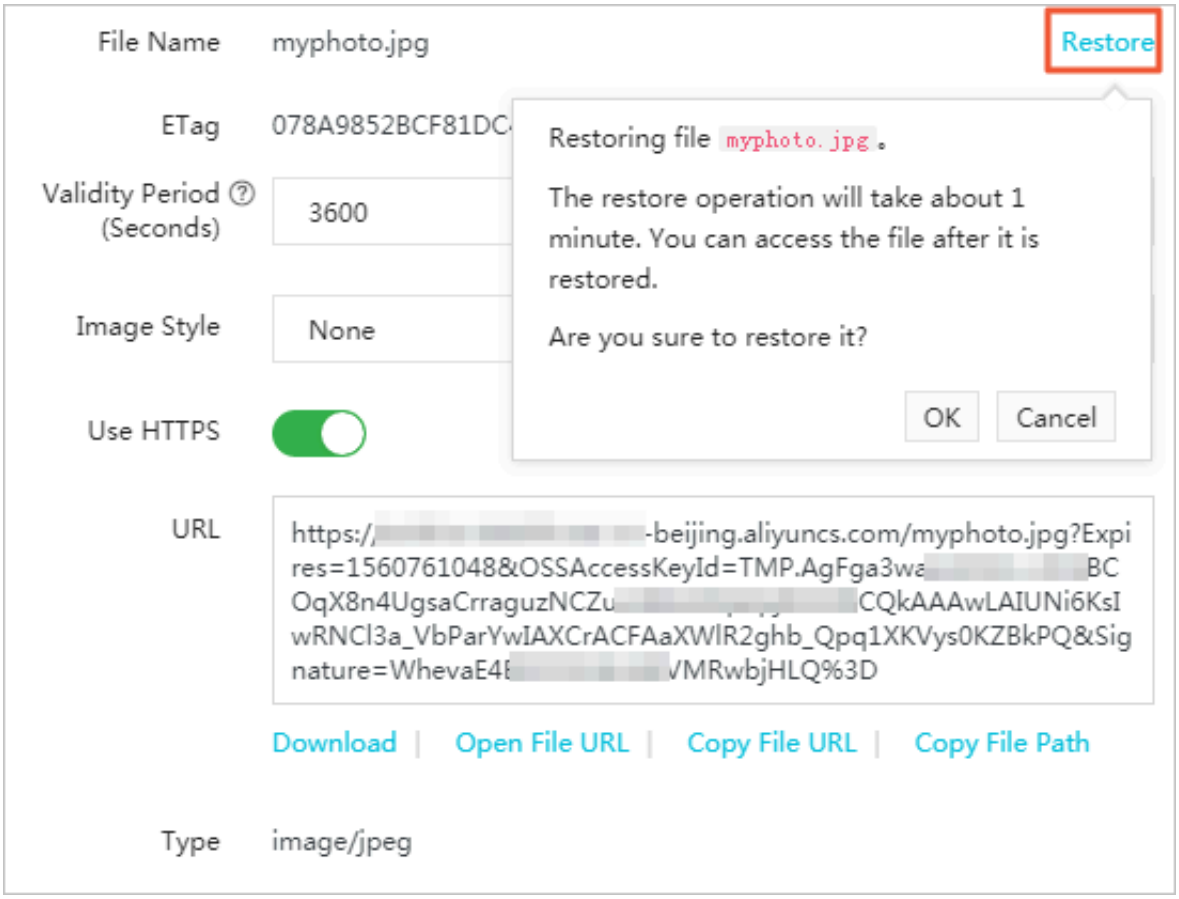
5. Click OK to delete the folder.

2.12 Restore an Archive object

This topic describes how to restore an Archive object in the OSS console.

Procedure

1. Log on to the OSS console.
2. In the left-side bucket list, click the name of the bucket in which the object to be restored is stored.
3. In the overview page of the bucket, click the Files tab.
4. Move the pointer over More in the Actions column corresponding to the object and select Restore from the drop-down list. You can also click the object name. On the View Details page that appears, click Restore > OK.



Note:

- The restoration takes about one minute. Then, the object is in the restored state .

- The object remains in the restored state for one day by default. You can use ossutil or SDK to prolong this period to a maximum of seven days. When this period expires, the object returns to the frozen state.
- Data retrieval fees are incurred when you restore an Archive object. For more information, see Billing items.
- For more information about the Archive storage class, see #unique_88/unique_88_Connect_42_section_v3z_lxt_tdb.

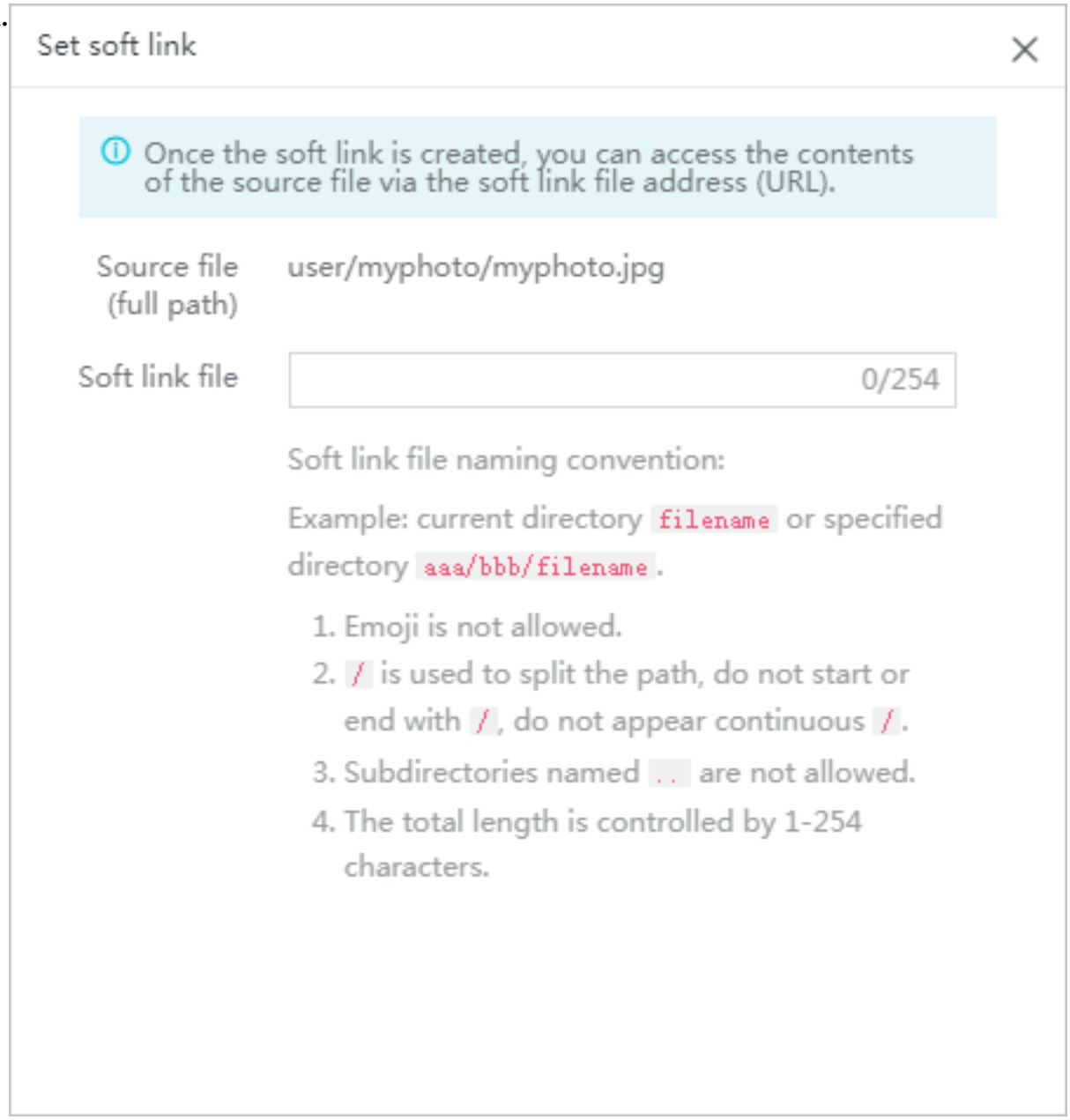
2.13 Set a symbolic link

You can set a symbolic link to point to a frequently accessed object in the target bucket for easier object retrieval. After setting a symbolic link for an object, you can use the symbolic link to quickly access the object. A symbolic link works in a similar manner as the shortcut in Windows.

Procedure

1. Log on to the OSS console.
2. In the left-side bucket list, click the name of the bucket where the target object is stored, and then click the Files tab.
3. Find the object for which you want to set a symbolic link, and then select More > Set soft link on the right of the object.

4. In the Set soft link dialog box, enter a name for the symbolic link file and click OK.



- Source file (full path): The full path of the current object is displayed here.
- Soft link file: Enter a name for the symbolic link that conforms to the symbolic link naming conventions. You can use a slash (/) to add a file path when entering the symbolic link file name.
  - If you do not add the file path, you can directly enter a customized symbolic link file name. For example: If the complete source file path is `user / myphoto / myphoto . jpg` , you can name the symbolic link file as

`myphoto` or `myphoto.jpg`. Then, the symbolic link file is stored in the root directory.

- If you add a file path, you can use a slash (/) to add the file path when entering the name of a symbolic link file. For example: If the complete source file path is `user/myphoto/myphoto.jpg`, you can name the symbolic link file as `shortcut/myphoto` or `shortcut/myphoto.jpg`. Then, the symbolic link file is stored in the `shortcut` directory.

> **Notice:**
> If the symbolic link file does not include a suffix that indicates the file type, for example, the symbolic link file name of the source file `myphoto.jpg` is named as `myphoto`, you can open the symbolic link file in the console or by accessing its URL. However, if you want to download the symbolic link file, a suffix that indicates the file type must be added in the file name.

2.14 Configure object tagging

OSS allows you to configure object tagging to classify objects. Object tagging uses a key-value pair to identify objects. You can perform operations on multiple objects that have the same tag. For example, you can configure lifecycle rules for objects that have the same tag.

Context

Object tagging uses a key-value pair to identify objects. You can manage multiple objects that have the same tag. For example, you can configure lifecycle rules for objects that have the same tag and authorize RAM users to access objects that have the same tag. For more information, see Object tagging.

- A maximum of 10 tags can be set for each object. Tags associated with an object must have unique tag keys.
- A tag key can be a maximum of 128 bytes in length. Each tag value can be a maximum of 256 bytes in length.
- Keys and values are case-sensitive.
- The key and value of the tag can contain letters, digits, spaces, and special characters such as

  + - = . _ : /

- Only the bucket owner and authorized users have the read and write permissions on object tags. These permissions are independent of object ACLs.
- During cross-region replication, object tags are also replicated to the destination bucket.

Procedure

1. Log on to the OSS console.
2. In the left-side bucket list, click the name of a bucket to go to the Overview tab.
3. Click the Files tab.
4. Move the pointer over More in the Actions column corresponding to an object and choose Tagging from the drop-down list.
5. In the Tagging dialog box that appears, configure tags.
6. Click OK.

3 Manage logs

3.1 Set logging

A large number of access logs are generated when you access OSS. After you enable the logging function for a bucket, OSS automatically records the access logs for the bucket on the hour, write the logs into an object that follows the specified naming convention, and store the object in the target bucket that you specify. For more information, see Access logging in the OSS developer guide.

Note:

To ensure that this function works properly, make sure that at least a pair of enabled AccessKey is available under your account.

Procedure

1. Log on to the OSS console.
2. In the left-side bucket list, click the name of the bucket that you want to set the logging unction.
3. Click the Basic Settings tab and find the Log area.
4. Click Configure and then set Destination Bucket and Log Prefix.
   - Destination Bucket: In the drop-down list, select the name of the bucket used to store logs. You can only select buckets owned by you and in the same region as the bucket for which the logging function is enabled.
   - Log Prefix: Enter the directory where logs are stored and the prefix of the logs. For example, if you enter `log/<TargetPrefix>`, logs are stored in the *log /* directory.
5. Click Save.

Logging naming convention

The following example is used to describe the naming convention for objects that store access logs.

*<TargetPrefix><SourceBucket>*YYYY-MM-DD-HH-MM-SS-*<UniqueString>*

- *<TargetPrefix>*: Indicates the specified log prefix.

- *<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 a string generated by OSS.

For example, the name of an object used to store OSS access logs is as follows:

MyLog-OSS-example2015-09-10-04-00-00-0000

- *MyLog* is the specified log prefix.
- *oss-example* is the name of the source bucket.
- *2015-09-10-04-00-00* indicates the time the the log is created.
- *0000* is a string generated by OSS.

3.2 Real-time log query

A large number of access logs are generated when you access OSS. By integrating OSS and Log Service (SLS), the real-time log query function allows you to query OSS access logs in the OSS console so that you can monitor OSS operations, measure OSS access statistics, trace exceptions, and locate problems with ease, improving efficiency and helping you make data-based decisions.

For more information, see Real-time log query in the OSS developer guide.

Enable real-time log query

You can enable the real-time log query function using either of the following two methods:

- Method 1: Enable real-time log query when creating a bucket.
  1. Log on to the OSS console.
  2. Click Create Bucket.
  3. In the Create Bucket dialog box, configure the parameters of the bucket you want to create.

     Select Enable for Real-time Log Query. For the configuration of other parameters, see Create a bucket.
  4. Click OK.

- Method 2: Enable real-time log query in the Log Overview page.

  1. Log on to the OSS console.
  2. In the left-side bucket list, click the bucket that you want to enable real-time log query.
  3. Click Log Overview, and then click Activate Now in the displayed page.

     
     Note:
     If Log Service is not activated, you are asked to authorize Log Service so that it can access OSS. After Log Service is authorized, a Log Service activation dialog box is displayed. Click Activate Now. After activating Log Service, follow step 3 to enable real-time log query.


Notice:
By using real-time log query, you can query logs recorded in the latest seven days for free. You can click Config Log Retention Time in the upper right of the Log Overview page to modify the log storage period. If the log storage period is set to a value larger than seven days, logs generated outside the scope of the latest seven days are charged individually. Additional fees are incurred if you use Log Service through the Internet.

For more information about the fees, see Billing method.

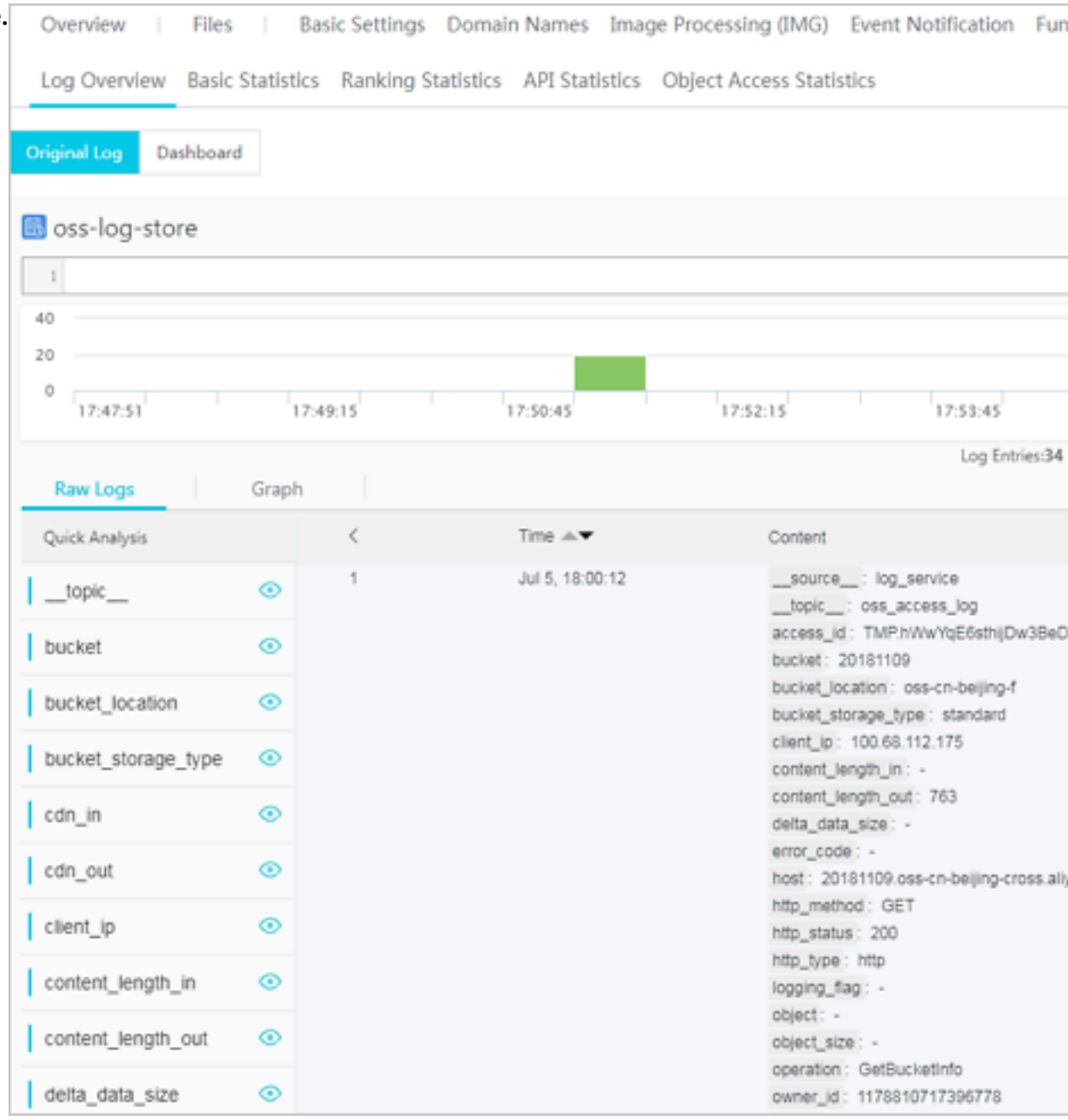
Query real-time logs

You can query real-time logs using any of the following three methods:

- Query real-time logs in the Original Log page.

  When querying real-time logs, you can specify the time range and query statements. For example, you can quickly analyze the distribution

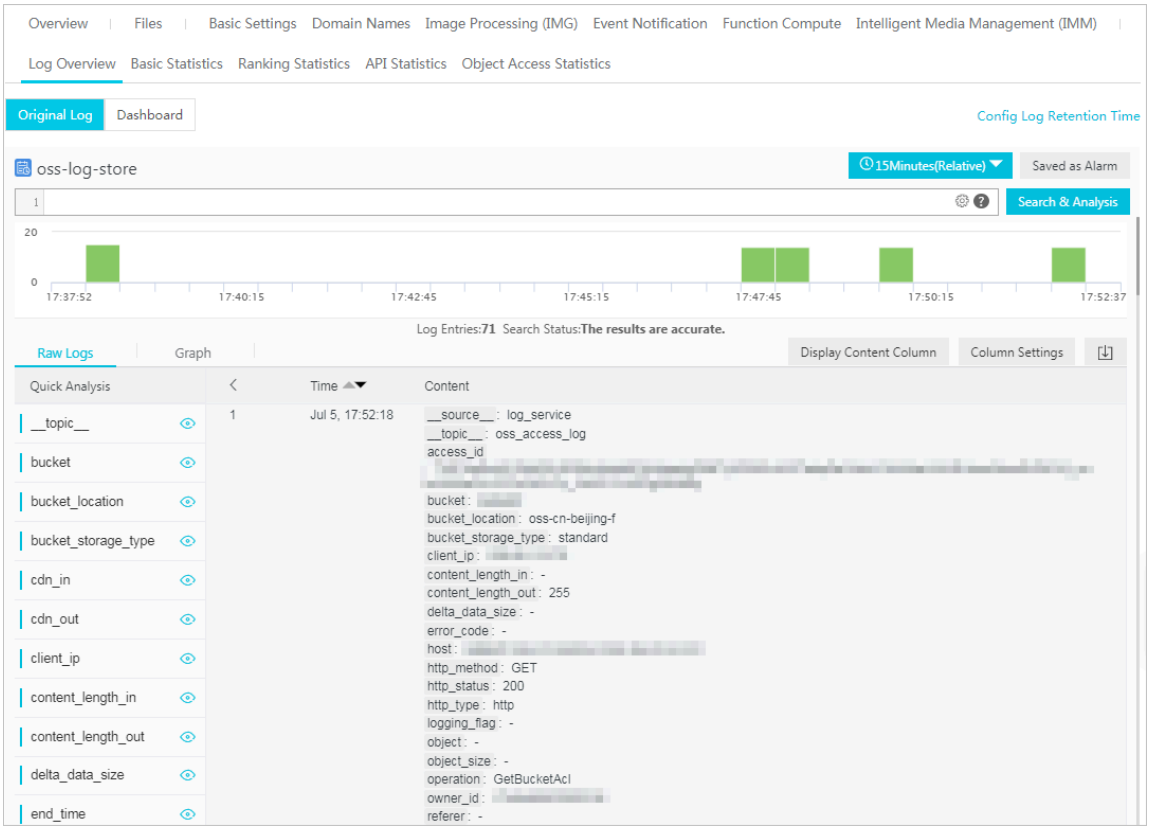
of a specified field (such as an API operation) in a specified time range.



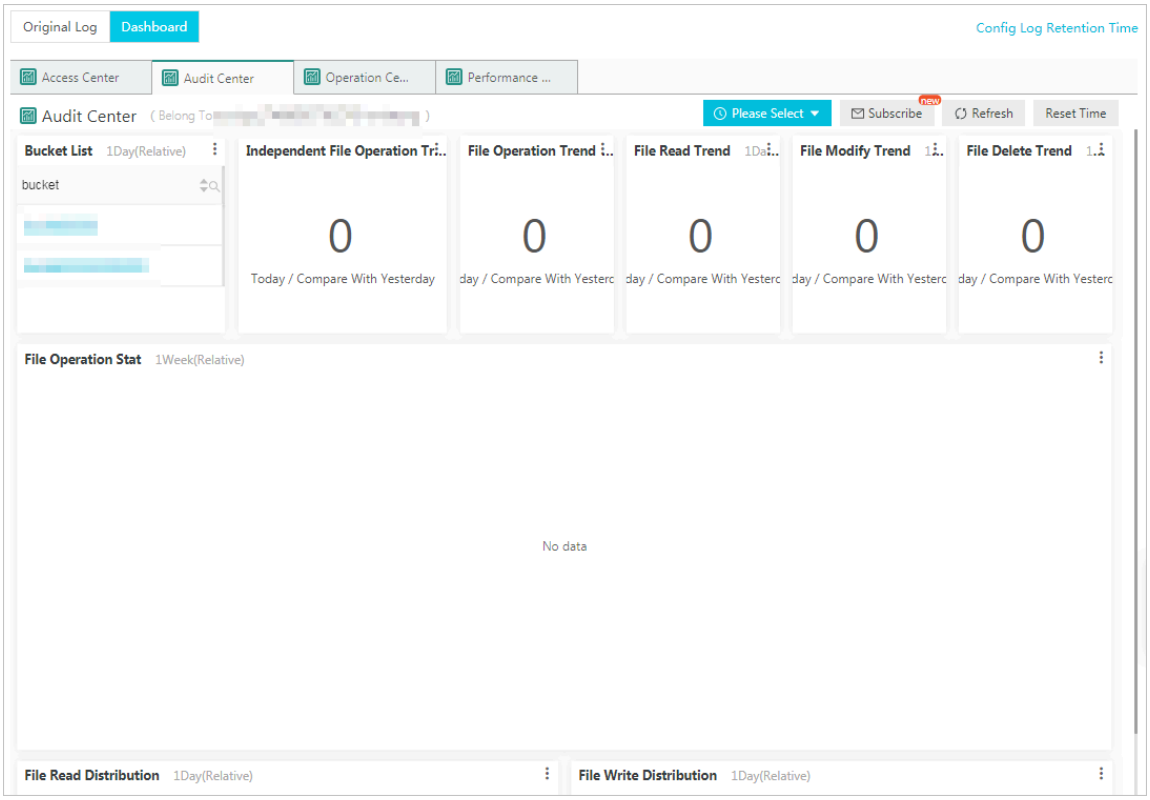
- Query real-time logs in the Dashboard page.

  In the Dashboard page, the following four system-generated reports are provided:

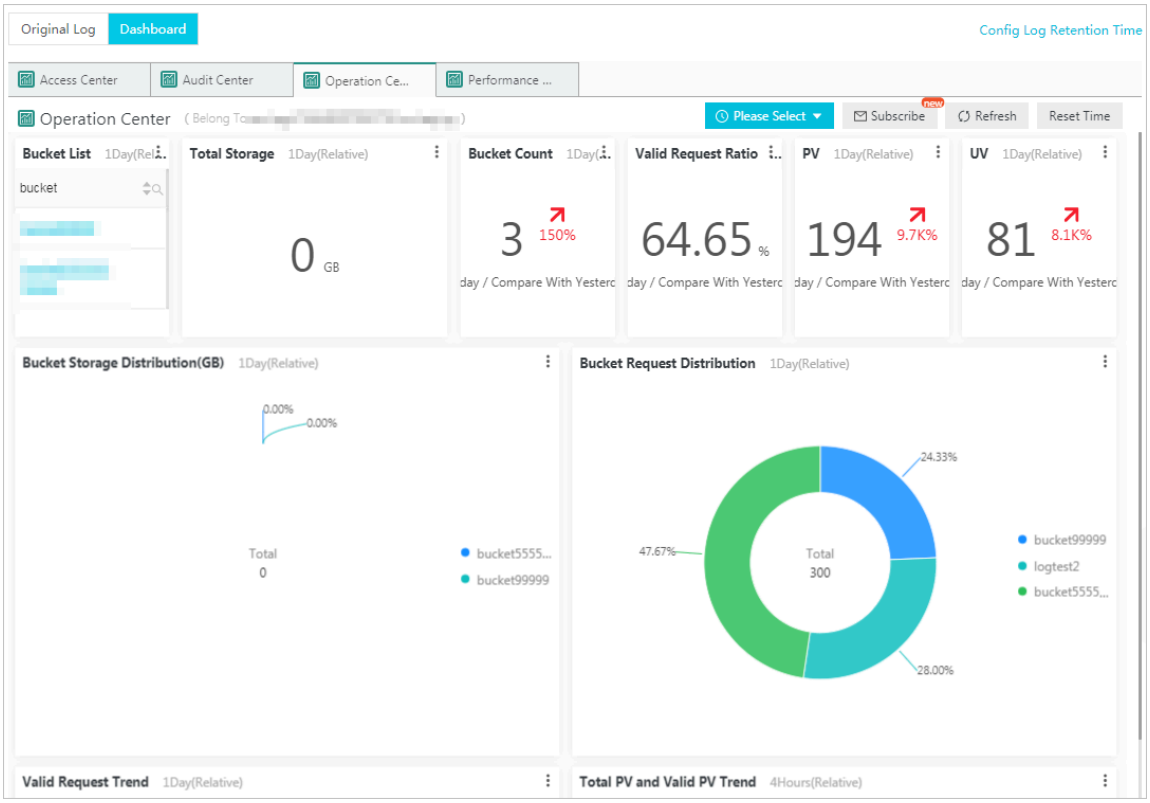
  - Access Center: displays general operation information, including PV, UV, traffics, and Internet access distribution in maps.



  - Audit Center: displays the statistics about object-related operations, including object reading, writing, and deleting.

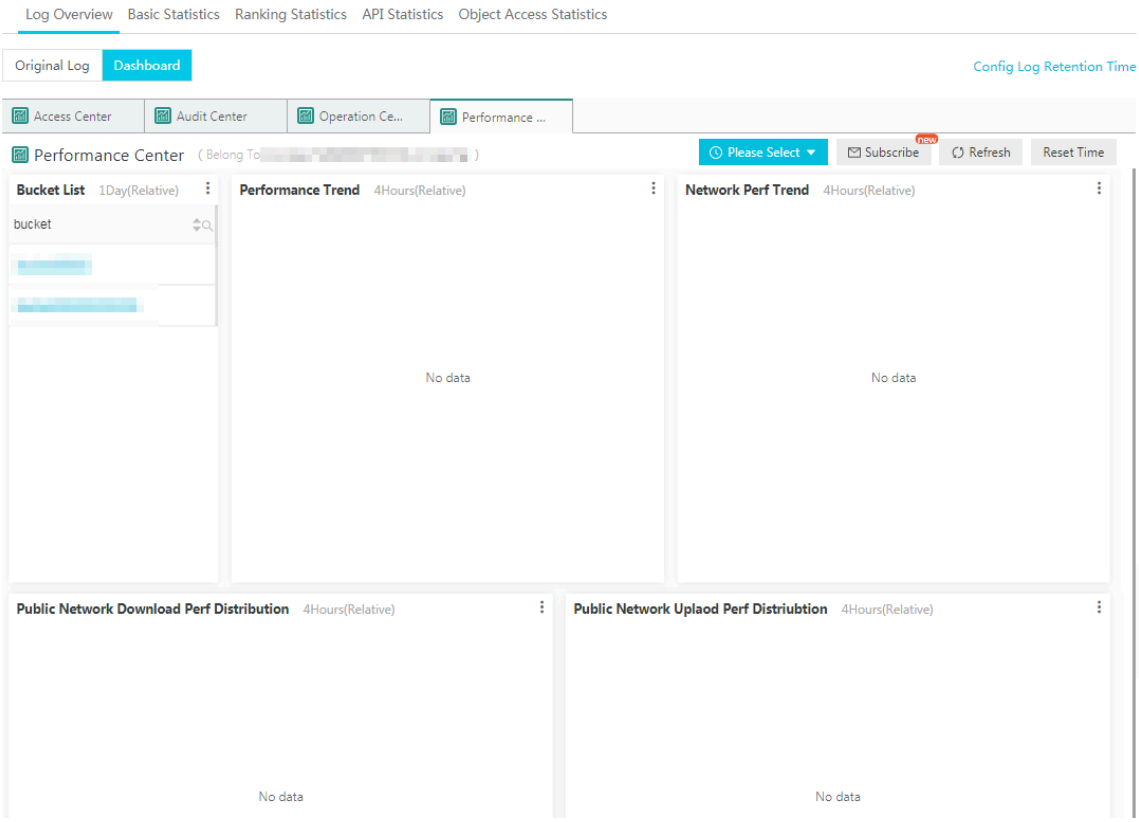


- Operation Center: displays the statistics about access logs, including the request number and the distribution of failed operations.



- Performance Center: displays the statistics about performance, including the distribution of Internet download and upload performance, transmission

performance of different networks and object sizes, and the list of download performance for different objects.



- Query real-time logs in the Log Service console.

  You can view OSS access logs in the Log Service console.

Reference

To store OSS access logs, see Set logging.

3.3 Log analysis

Before using the log analysis service, you must pay for it. For the fees of log analysis service, see Log Service Pricing.

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.

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.

4 Manage fragments

When you upload an object in the multipart upload mode, the object is divided into several parts, which are also called fragments. After you upload all the fragments to the OSS server, you can call CompleteMultipartUpload to combine the parts into a complete object.

Note:

- Fragments are also generated when you transfer objects by using OSS management tools that support multipart upload or download.
- You can call CompleteMultipartUpload to combine the fragments into a complete object. For more information on how to use MultipartUpload, see #unique_102.
- You can regularly clear unnecessary fragments by setting the lifecycle management. It is used to clear the fragments for which CompleteMultipartUpload is not complete for a long term in the bucket to reduce the consumption of space. For the detailed procedure, see #unique_55.
- A fragment cannot be read before it is combined with other fragments into an object. To delete a bucket, you must delete the objects and fragments stored in the bucket first. Fragments are mainly generated by multipart upload tasks. For more information, see #unique_102.

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 Files tab.
4. Click the Fragments to open the Fragments page.
5. Delete the fragments.
   - To delete all the fragments in a bucket, click Delete All.
   - To delete some of the fragments in a bucket, select or search for the expected fragments and click Delete.
6. In the dialog box that appears, click OK.

5 Configure Event Notifications

The Event Notification features supported by OSS, the ability to notify you of relevant actions on the OSS resource you are concerned about in a timely manner. For example:

- New data has been uploaded from the picture content sharing platform, audio and video platform to OSS.
- Related content on OSS has been updated.
- The important files on the OSS are deleted.
- The synchronization of data on OSS has been completed.

The OSS Event Notification is asynchronous and does not affect normal OSS operations. The configuration of Event Notification consists of two parts: Rules and Message notification.

- Rules: used to describe when OSS is required for Message notification.
- Message notification: Based on the implementation of the Ali cloud messaging service MnS, various notification methods are provided.

Create method

1. Log on to the OSS console.
2. In the list of left storage spaces, click the target storage space name to open the storage space overview page.
3. Click the Event Notification tab, and then click Create rule to locate the Create rule page.
4. In the Rule name box, enter the rule name.

   Note:

   - You can create up to 10 rules in the same product under the same region, the new rule takes effect in about 10 minutes.
   - Any two rules cannot have an intersection, and any two resource descriptions cannot have an intersection.

5. In Resource descriptions area, clickAdd to add one or more resource descriptions.

   Note:

- Resource Description: can be full name, prefix, suffix, and pre-suffix, different resource descriptions cannot have intersection.
  - Full name: Enter the full name of an object to pay precise attention to this object.
  - Pre-Suffix: sets the pre-Suffix of the object to focus on all or part of the object in a bucket. For example, for a bucket named `nightbucke t` :
    - Pay attention to all of these files, the prefix and suffix are not filled in.
    - Note that all the files in the directory *`movie`* , fill in the prefix with `movie/`, but with no suffix.
    - Note that all of the *`.jpg`* images, leave the prefix empty and fill in the suffix with `.jpg`.
    - Note that mp3 format video under the *`movie`* directory, prefix the `movie/` with the suffix .mp3.
- The OSS resource includes the bucket and the object, which are connected by “/” . Take bucket (movie) and object (hello. avi) for example.
  - Full name: movie/hello.avi;
  - Prefixes and suffixes: prefix movie/, and suffix avi, it means all objects suffixes with *`.avi`* in the *`movie`* .

6. In the Event type drop-down list, select one or more events that require message notification.

   Note:

   - The event type corresponds to different operations of the OSS resource, see the list of event types below for specific types and meanings.
   - You can select multiple events that you want to trigger notifications. The same event cannot be configured multiple times on the same resource.

7. In the Receive terminal area, click Add to add one or more receive terminals.

   Note:

   - The OSS Event Notification function generates a Message description after an action rule matches, and publish the message to the topic of the MNS, and then according to the subscription on that topic, push messages to a specific receive terminal.

- For how to handle HTTP push messages for MnS and consume messages from queues, see Message Service.

List of event types

Event Type	Meaning
ObjectCreated:PutObject	Create/override files: simple upload
ObjectCreated:PostObject	Create/override files: Form upload
ObjectCreated:CopyObject	Create/override files: Copy files
ObjectCreated:InitiateMultipartUpload	Create/override file: initialize a multipart upload task
ObjectCreated:UploadPart	Create/override file: Upload multipart
Objectcreated: sealadpartcopy	Create/override file: Copy data from an existing file to upload a multipart
ObjectCreated:CompleteMultipartUpload	Creating/overwriting files: Completing multiparts upload
ObjectCreated:AppendObject	Creating/overwriting files: appending an upload
ObjectDownloaded:GetObject	Download files: simple download
ObjectRemoved:DeleteObject	Delete file: One
ObjectRemoved:DeleteObjects	Delete Files: Multiple
ObjectReplication:ObjectCreated	Synchronous files: generated
ObjectReplication:ObjectRemoved	Synchronizing files: Deleted
ObjectReplication:ObjectModified	Synchronizing files: Modified

6 Check resource usage

Overview

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

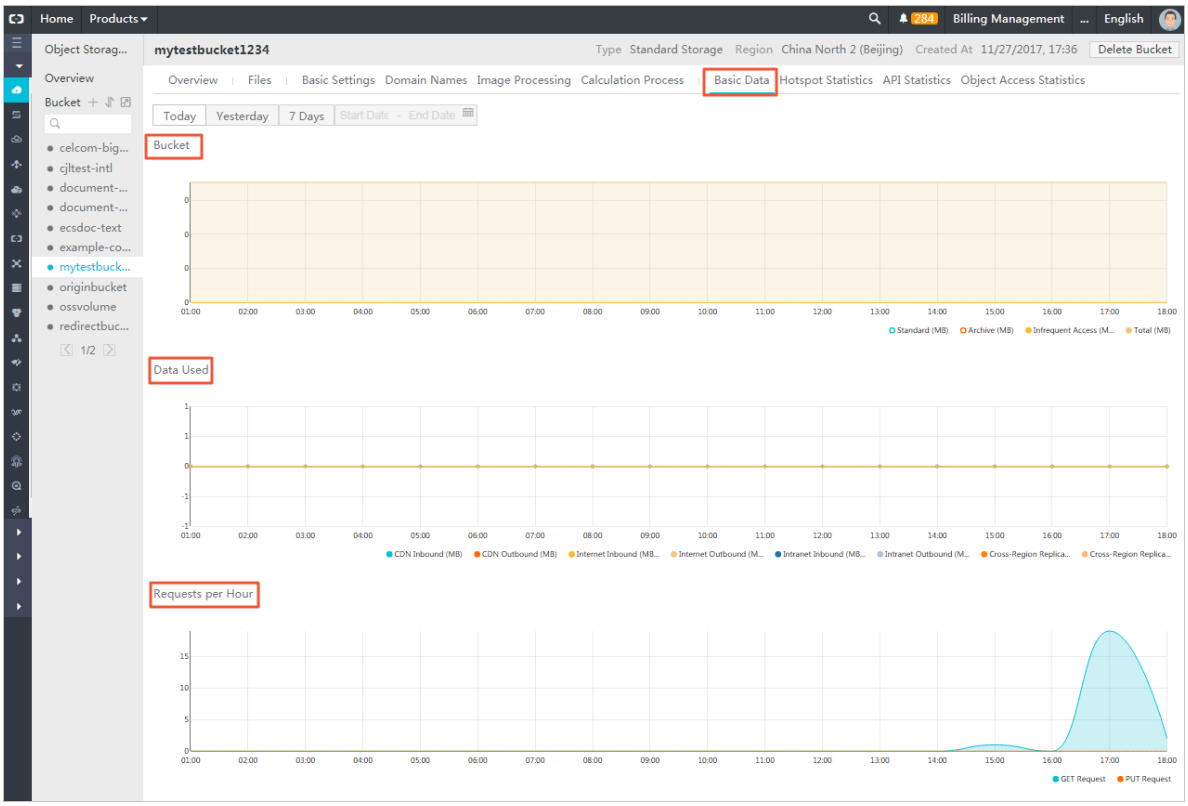
- Basic data: Including bucket, data used, and requests per hour
- Hotspot statistics: Including PV/UV, original, and hot spot
- API statistics: Including method statistics and return code
- Object access statistics: Including statistics about object access

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 6-1: 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 6-2: Data Used

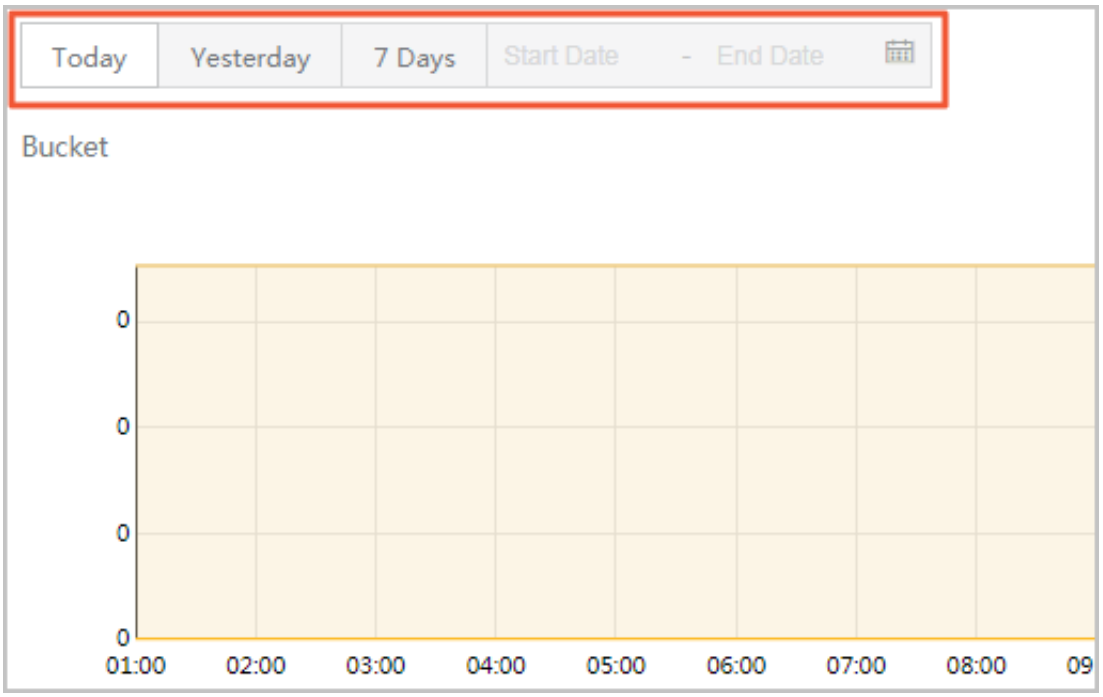
Basic Data	Description

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 6-3: 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:



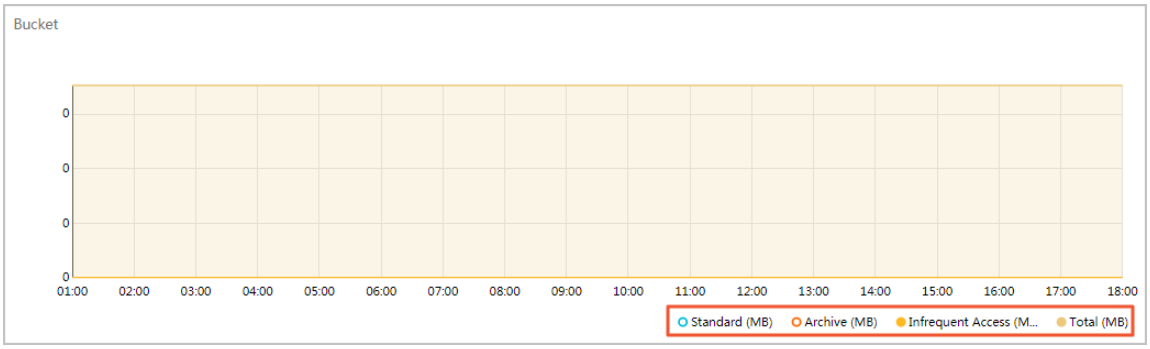
- Today: Only the data of the current day is shown in diagrams.
- Yesterday: Only the data of yesterday is shown in diagrams.
- 7 Days: Only the data of the latest seven days is shown in diagrams.
- Customized time period: You can select the Start Date and the End Date of a time period. The data in this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