Alibaba Cloud
Object Storage Service

Console User Guide

Issue: 20190220

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

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

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

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

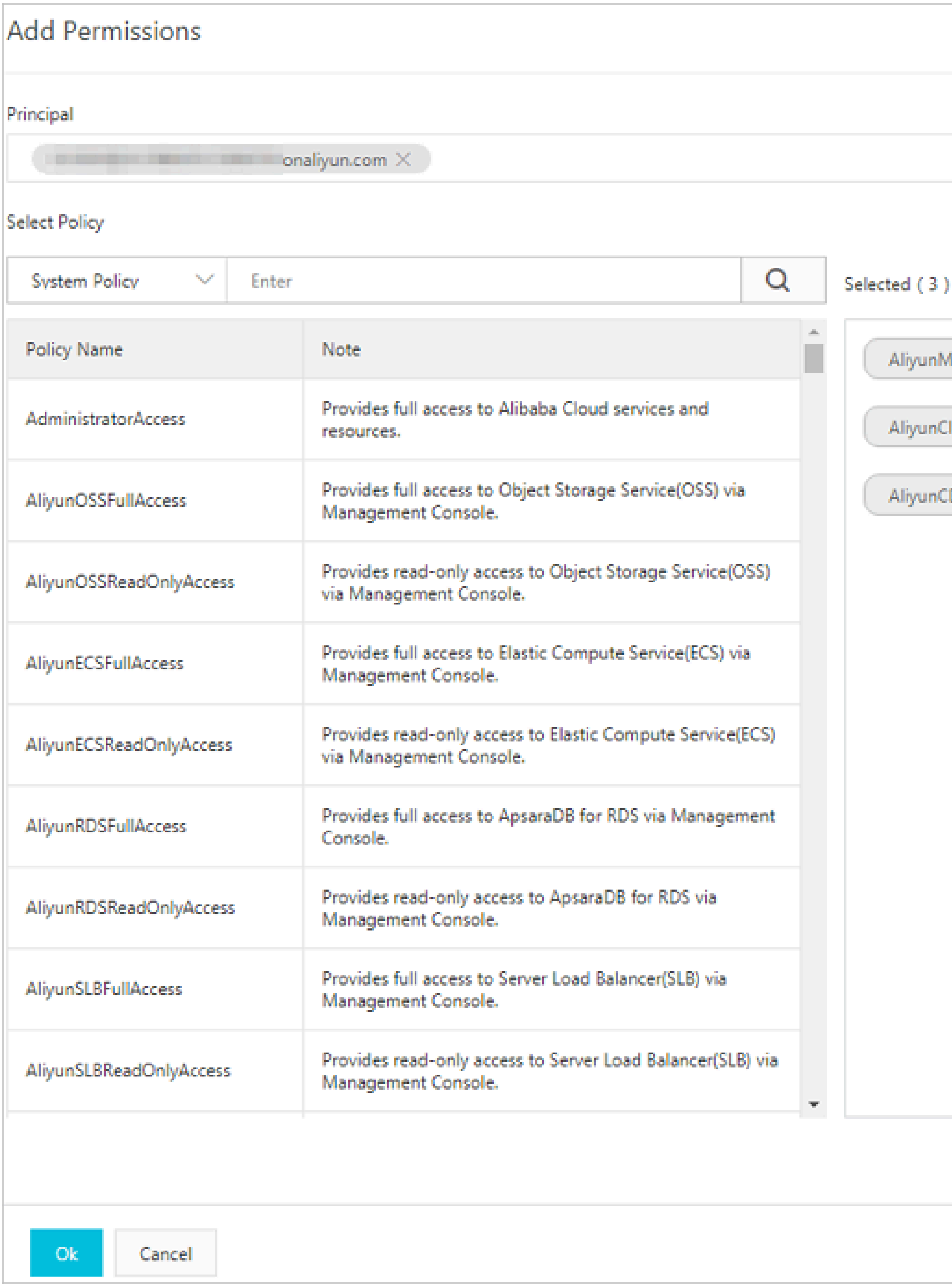
Create a RAM user

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

Authorize a sub-account

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

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



Add Permissions

Principal

[redacted]onaliyun.com ✕

Select Policy

System Policy | Enter

Selected (3)

Policy Name	Note
AdministratorAccess	Provides full access to Alibaba Cloud services and resources.
AliyunOSSFullAccess	Provides full access to Object Storage Service(OSS) via Management Console.
AliyunOSSReadOnlyAccess	Provides read-only access to Object Storage Service(OSS) via Management Console.
AliyunECSFullAccess	Provides full access to Elastic Compute Service(ECS) via Management Console.
AliyunECSReadOnlyAccess	Provides read-only access to Elastic Compute Service(ECS) via Management Console.
AliyunRDSFullAccess	Provides full access to ApsaraDB for RDS via Management Console.
AliyunRDSReadOnlyAccess	Provides read-only access to ApsaraDB for RDS via Management Console.
AliyunSLBFullAccess	Provides full access to Server Load Balancer(SLB) via Management Console.
AliyunSLBReadOnlyAccess	Provides read-only access to Server Load Balancer(SLB) via Management Console.

Log on to the console with a sub-account

Do the following to log on to the console with a sub-account:

1. Log on to the RAM console, and click User Management.
2. Select the corresponding RAM user, and click Manage to configure related information.
3. Turn on Enable Console Logon.
4. Log on to the RAM console, view your RAM user logon link, and click the link to log on.

For more information, see *RAM User Manual*.

2 Log on to OSS console

Context

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

Procedure

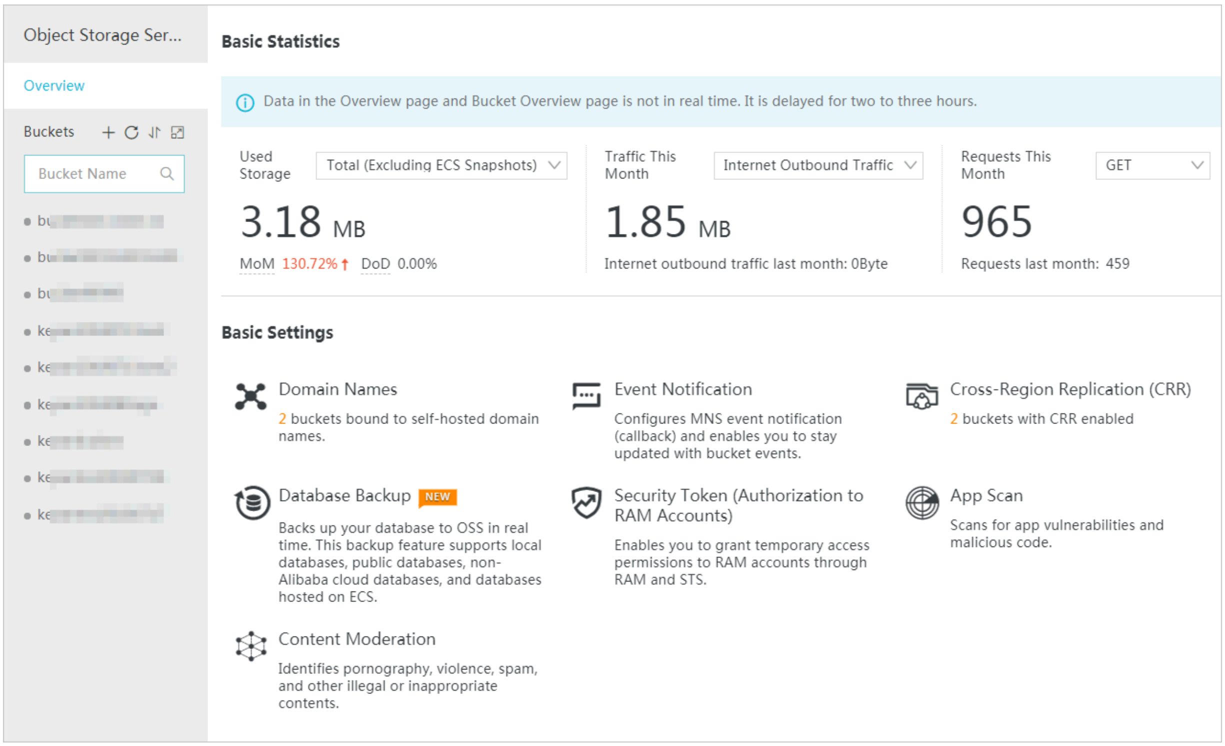
1. Log on to the *Alibaba Cloud official website*.
2. On the *OSS product detail page* click Buy now.
3. After OSS is activated, click Console to access the OSS console. You can also click Console in the upper-right menu bar on the *homepage* to open Alibaba Cloud console, and click Object Storage Service in the left-side navigation pane to access the OSS console.

3 Manage buckets

3.1 Bucket overview

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

The following picture shows the overview page of a bucket:



Basic Statistics

Data in the Overview page and Bucket Overview page is not in real time. It is delayed for two to three hours.

Used Storage: Total (Excluding ECS Snapshots)
3.18 MB
MoM 130.72% ↑ DoD 0.00%

Traffic This Month: Internet Outbound Traffic
1.85 MB
Internet outbound traffic last month: 0Byte

Requests This Month: GET
965
Requests last month: 459

Basic Settings

Domain Names
2 buckets bound to self-hosted domain names.

Event Notification
Configures MNS event notification (callback) and enables you to stay updated with bucket events.

Cross-Region Replication (CRR)
2 buckets with CRR enabled

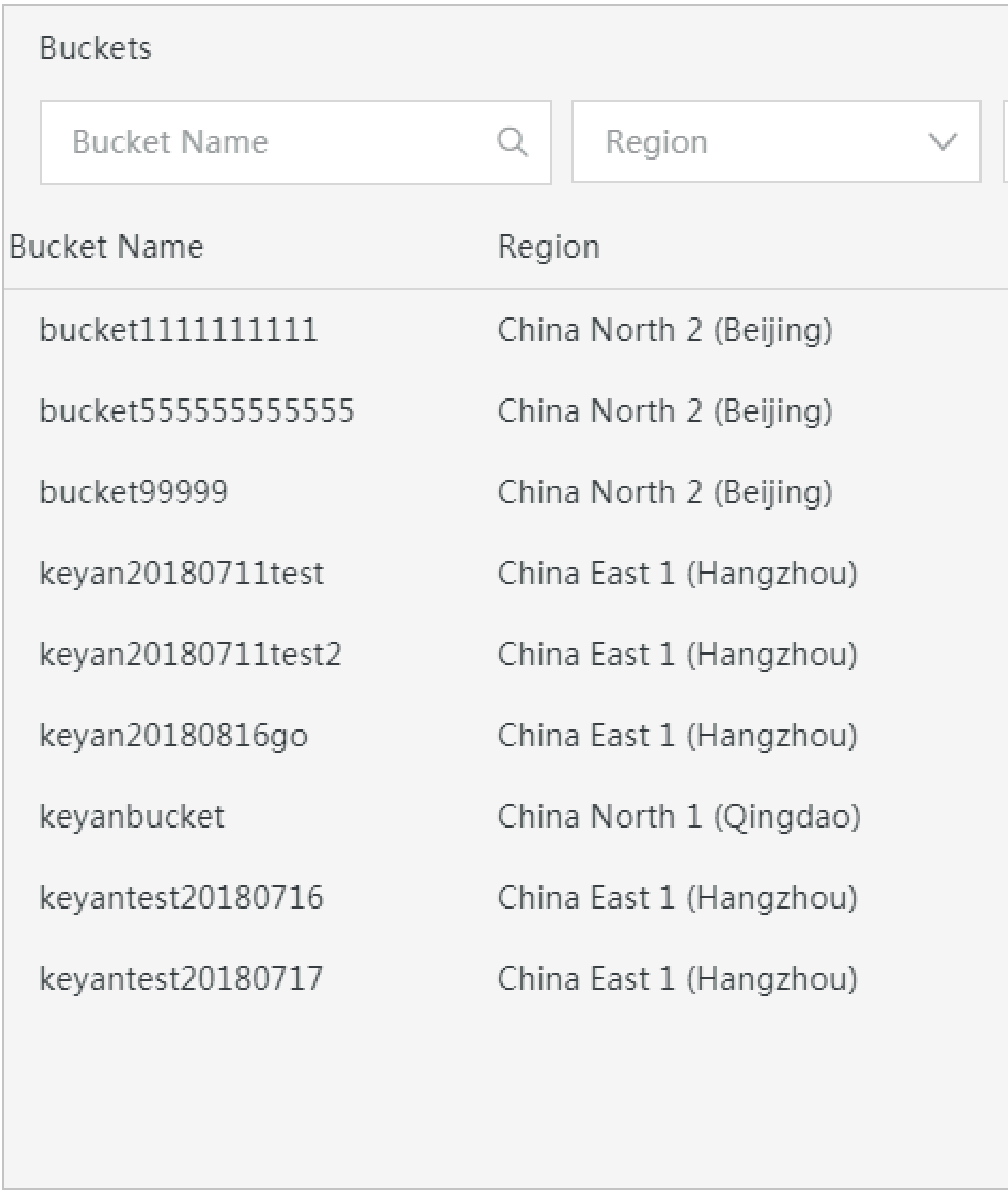
Database Backup NEW
Backs up your database to OSS in real time. This backup feature supports local databases, public databases, non-Alibaba cloud databases, and databases hosted on ECS.

Security Token (Authorization to RAM Accounts)
Enables you to grant temporary access permissions to RAM accounts through RAM and STS.

App Scan
Scans for app vulnerabilities and malicious code.

Content Moderation
Identifies pornography, violence, spam, and other illegal or inappropriate contents.

You can click the Expand Bucket List icon on the right of Bucket to view the bucket list and related information, including the region, storage class, capacity, Internet traffic of the current month, and the visits of the current month, as shown in the following picture:



Bucket Name	Region
bucket111111111	China North 2 (Beijing)
bucket55555555555	China North 2 (Beijing)
bucket99999	China North 2 (Beijing)
keyan20180711test	China East 1 (Hangzhou)
keyan20180711test2	China East 1 (Hangzhou)
keyan20180816go	China East 1 (Hangzhou)
keyanbucket	China North 1 (Qingdao)
keyantest20180716	China East 1 (Hangzhou)
keyantest20180717	China East 1 (Hangzhou)

3.2 Create a bucket

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

Procedure

1. Log on to the *OSS console*.
2. Click Create Bucket to open the Create Bucket dialog box.
3. In the Bucket Name field, enter the bucket name.
   - The bucket name must comply with the naming conventions.
   - The bucket name must be unique across all existing bucket names in OSS.
   - The bucket name cannot be changed after the bucket is created.
   - For more information about bucket naming, see *Basic concepts*.
4. In the Region drop-down box, select the data center of the bucket.

   The region cannot be changed after the subscription. To access the OSS over the intranet of the ECS, select the same region with your ECS instance. For more information, see *Endpoints*.
5. For Storage Class, select the storage type as needed.
   - `Standard storage`: provides highly reliable, highly available, and high-performance object storage services that support frequent data accesses.
   - `Infrequent access`: suitable for data that is stored for a long term and infrequently accessed. Its unit price is lower than that of the standard type. This storage class requires a minimum storage duration for the files. Charges are incurred if you delete files that are stored for less than 30 days. This storage class requires a minimum billable size for files. Files smaller than 64 KB are charged for 64 KB and data retrieval may cause a certain cost.
   - `Archive storage`: suitable for storing archival data that requires long-term persistence (more than half a year). The data is infrequently accessed during the storage period and restoring the data to a readable state may take one minute. It is suitable for storing archival data, medical images, scientific materials, and video footages for long-term persistence.
6. For ACL, select the expected permission for the bucket.

- `Private`: Only the owner of the bucket and the authorized users can perform read, write, and delete operations on the objects in the bucket. Other users cannot access objects in the bucket.
- `Public Read`: Only the owner of the bucket and the authorized users can perform write and delete operations on the objects in the bucket. Anyone (including anonymous access) can read the objects in the bucket.
- `Public Read/Write`: Anyone (including anonymous access) can read, write, and delete the objects in the bucket.

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

7. Click OK.

3.3 Delete a bucket

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

Prerequisite

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

> Note:
>
> - If you want to delete all objects in a bucket, we recommend that you use *Set lifecycle*.
> - For detailed procedures on how to delete parts, see *Manage fragments*.

Procedure

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

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

3.4 Change bucket ACL

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

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.

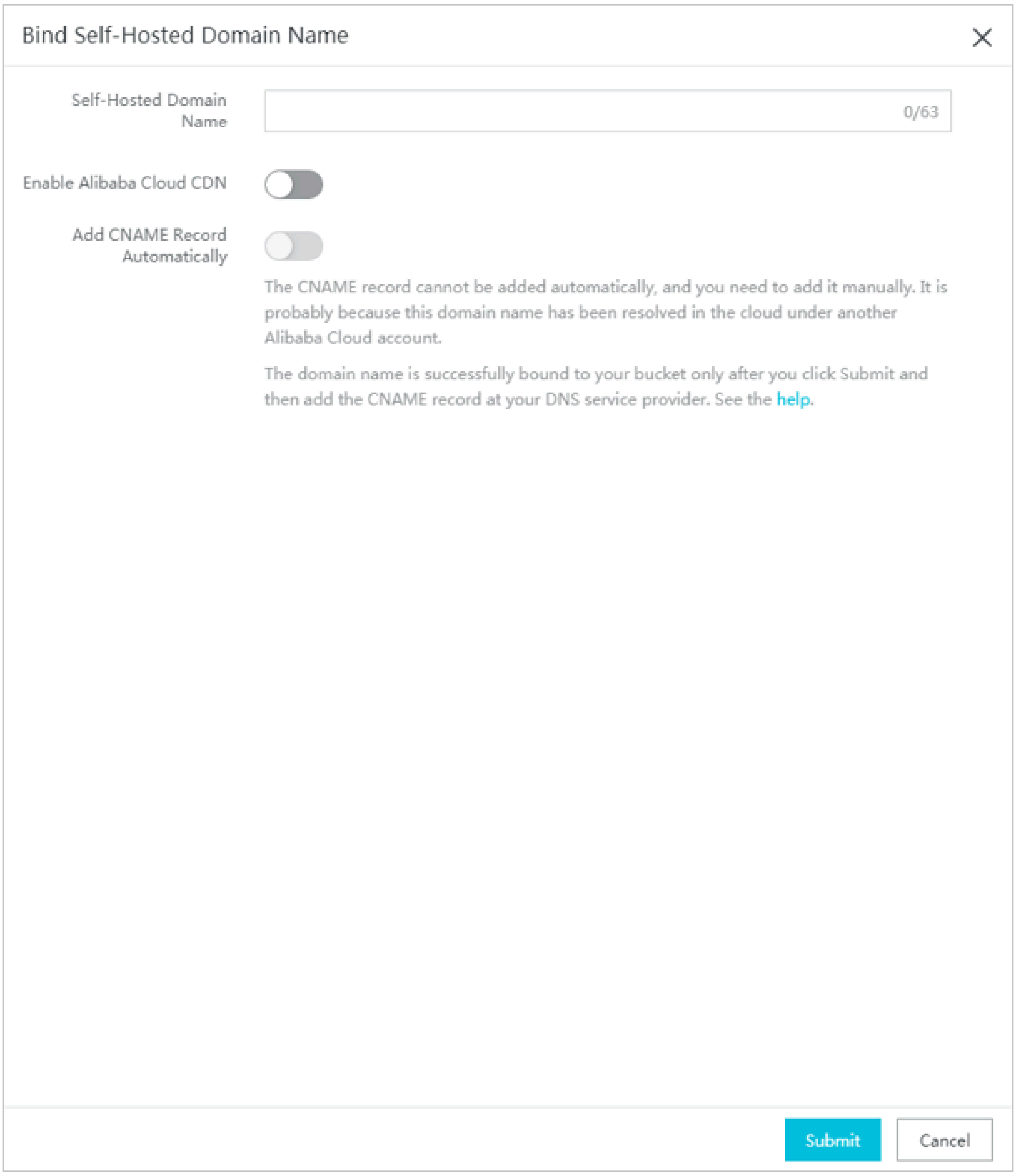
3.5 Manage a domain

3.5.1 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:



Bind Self-Hosted Domain Name

Self-Hosted Domain Name: 0/63

Enable Alibaba Cloud CDN

Add CNAME Record Automatically

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

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

- 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.

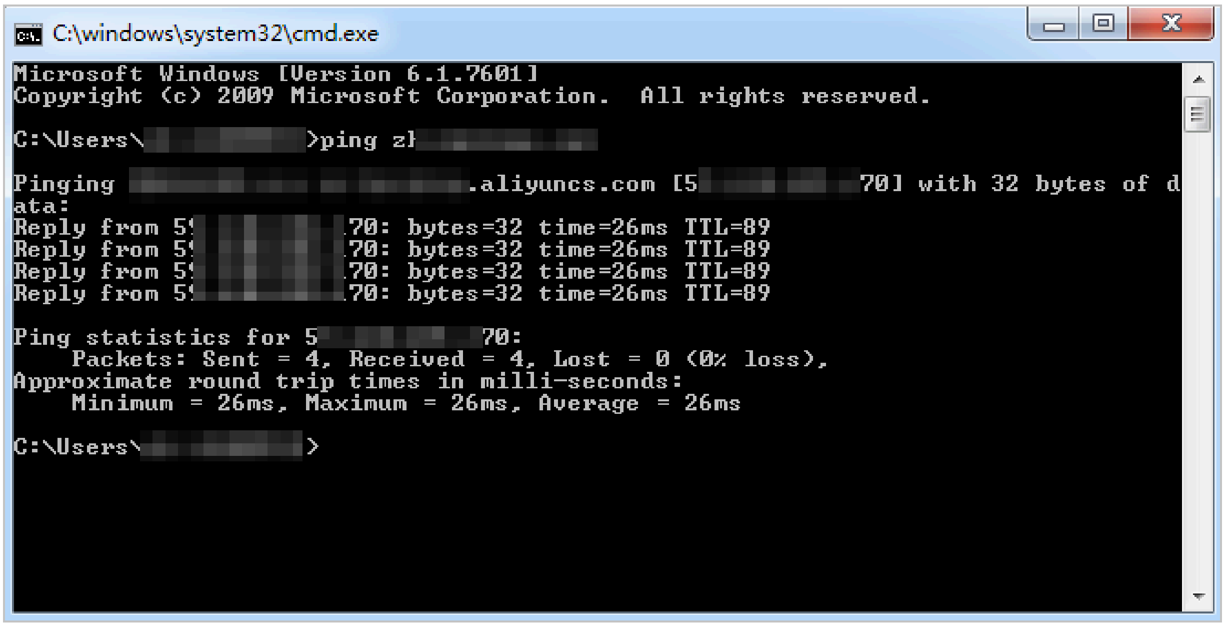
4. ClickOK.

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.



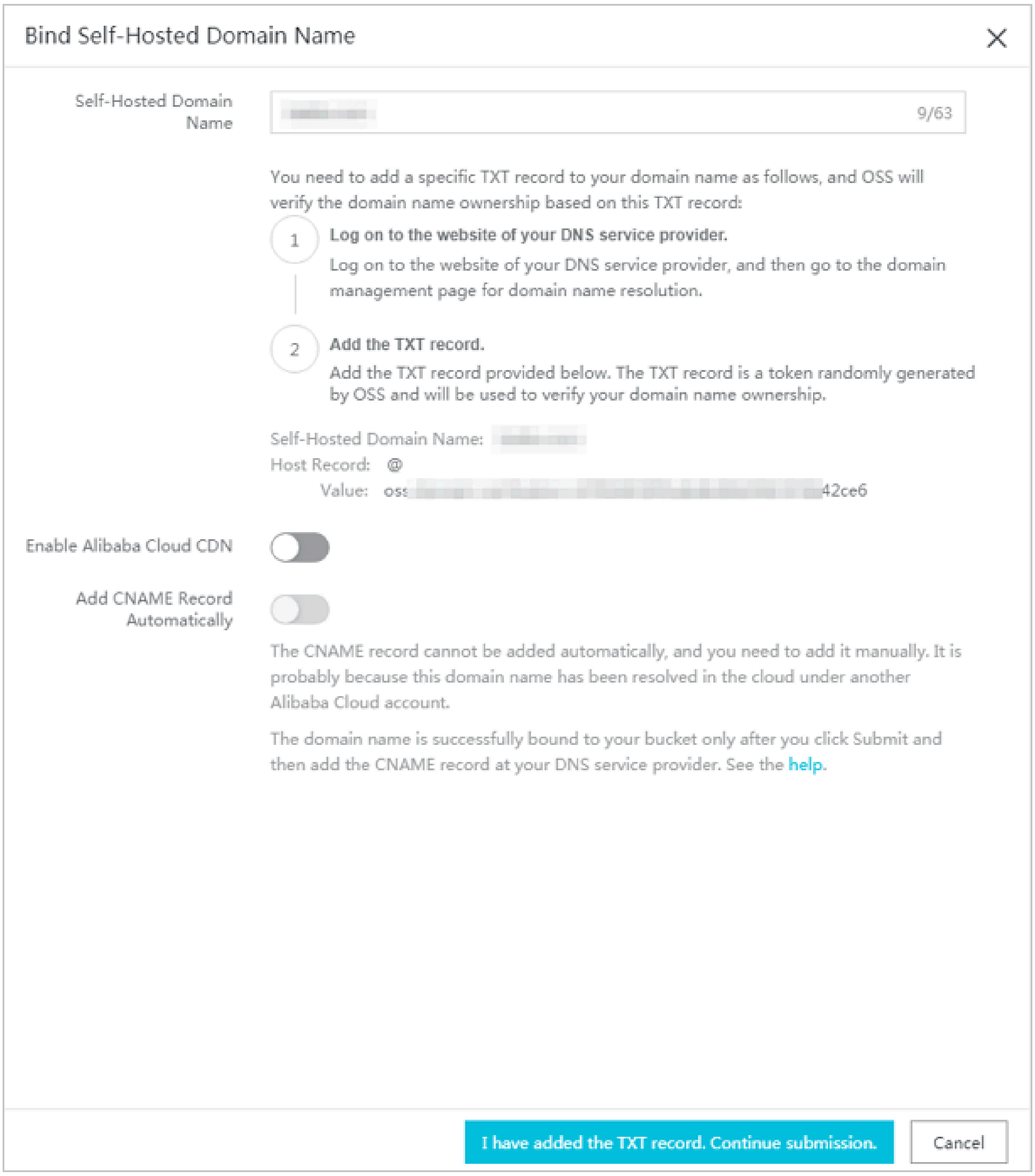
```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\[redacted]>ping z[redacted]

Pinging [redacted].aliyuncs.com [5[redacted]70] with 32 bytes of d
ata:
Reply from 5[redacted].70: bytes=32 time=26ms TTL=89
Reply from 5[redacted].70: bytes=32 time=26ms TTL=89
Reply from 5[redacted].70: bytes=32 time=26ms TTL=89
Reply from 5[redacted].70: bytes=32 time=26ms TTL=89

Ping statistics for 5[redacted]70:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 26ms, Maximum = 26ms, Average = 26ms

C:\Users\[redacted]>
```

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.



Bind Self-Hosted Domain Name

Self-Hosted Domain Name: [redacted] 9/63

You need to add a specific TXT record to your domain name as follows, and OSS will verify the domain name ownership based on this TXT record:

1. **Log on to the website of your DNS service provider.**
   Log on to the website of your DNS service provider, and then go to the domain management page for domain name resolution.
2. **Add the TXT record.**
   Add the TXT record provided below. The TXT record is a token randomly generated by OSS and will be used to verify your domain name ownership.

Self-Hosted Domain Name: [redacted]
Host Record: @
Value: oss[redacted]42ce6

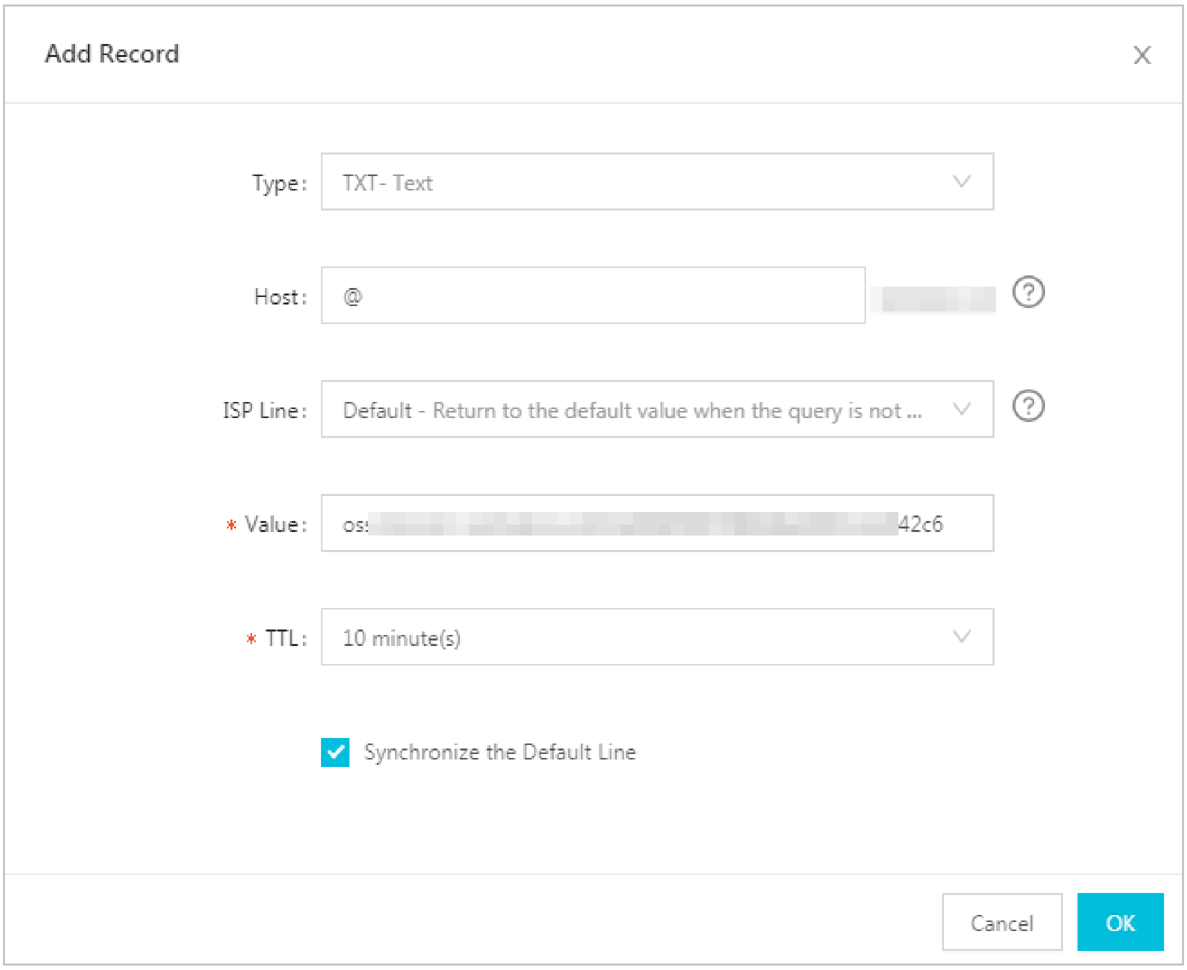
Enable Alibaba Cloud CDN

Add CNAME Record Automatically

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

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

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:



Add Record

Type: TXT- Text

Host: @ [redacted]

ISP Line: Default - Return to the default value when the query is not ...

* Value: os[redacted]42c6

* TTL: 10 minute(s)

☑ Synchronize the Default Line

- 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.

3.5.2 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.

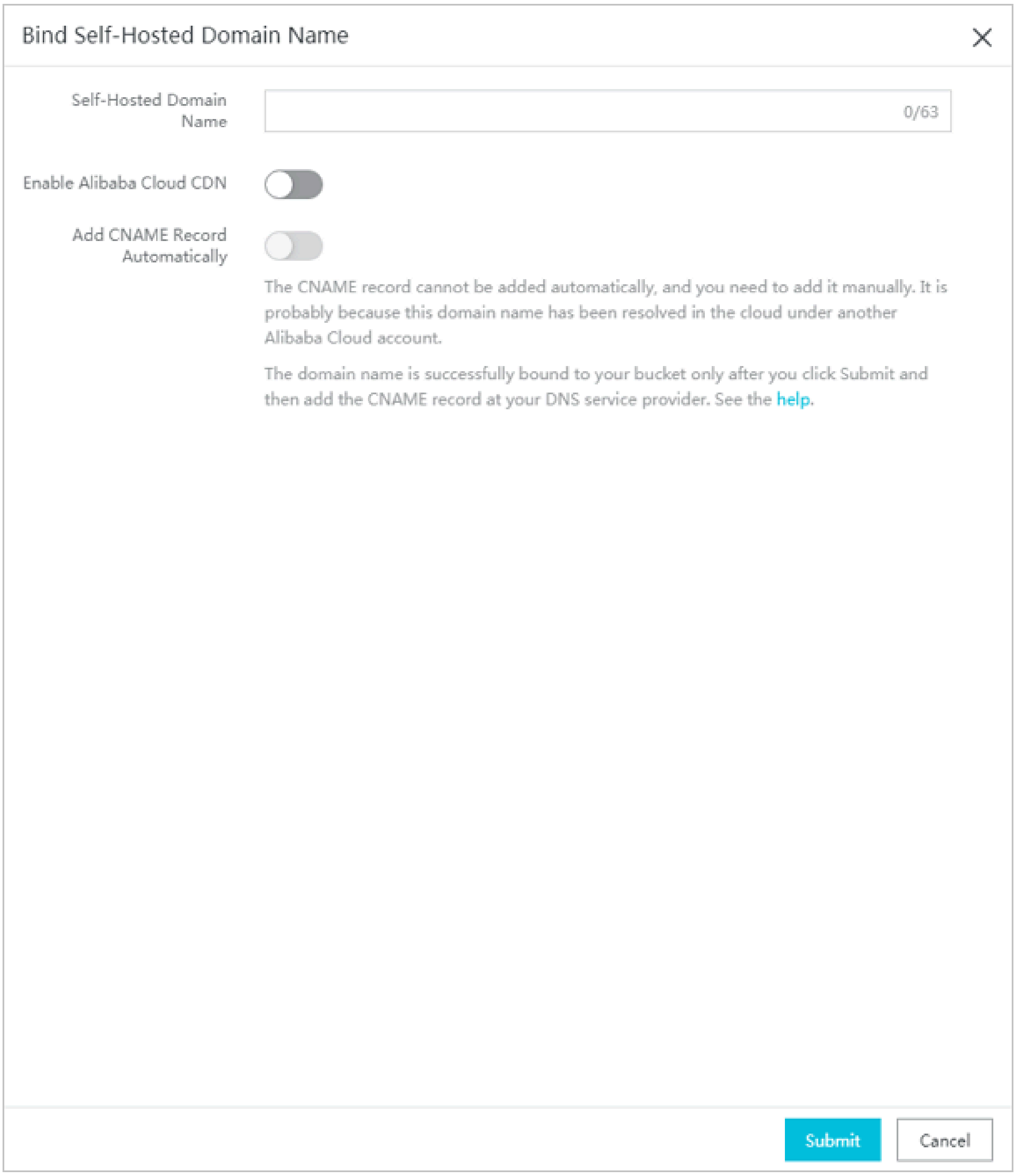
To enable the Alibaba Cloud CDN-based acceleration service, you must direct your self-hosted domain name to a CDN acceleration domain name assigned by Alibaba Cloud CDN. Afterwards, all requests for your self-hosted domain name are redirected to the CDN edge nodes.

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:



Bind Self-Hosted Domain Name

Self-Hosted Domain Name: 0/63

Enable Alibaba Cloud CDN

Add CNAME Record Automatically

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

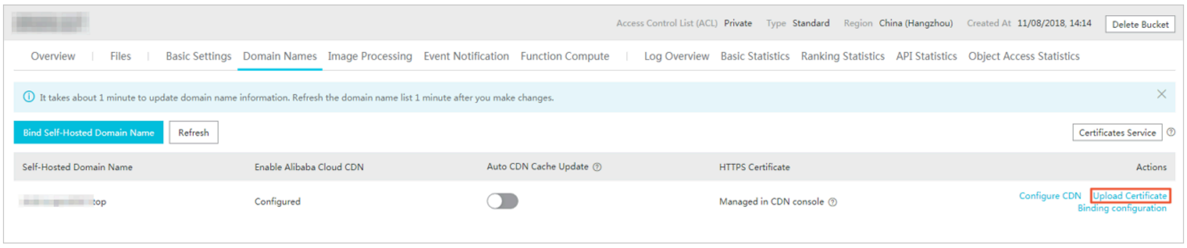
The domain name is successfully bound to your bucket only after you click Submit and then add the CNAME record at your DNS service provider. See the help.

- 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 acceleration*service.
- 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.

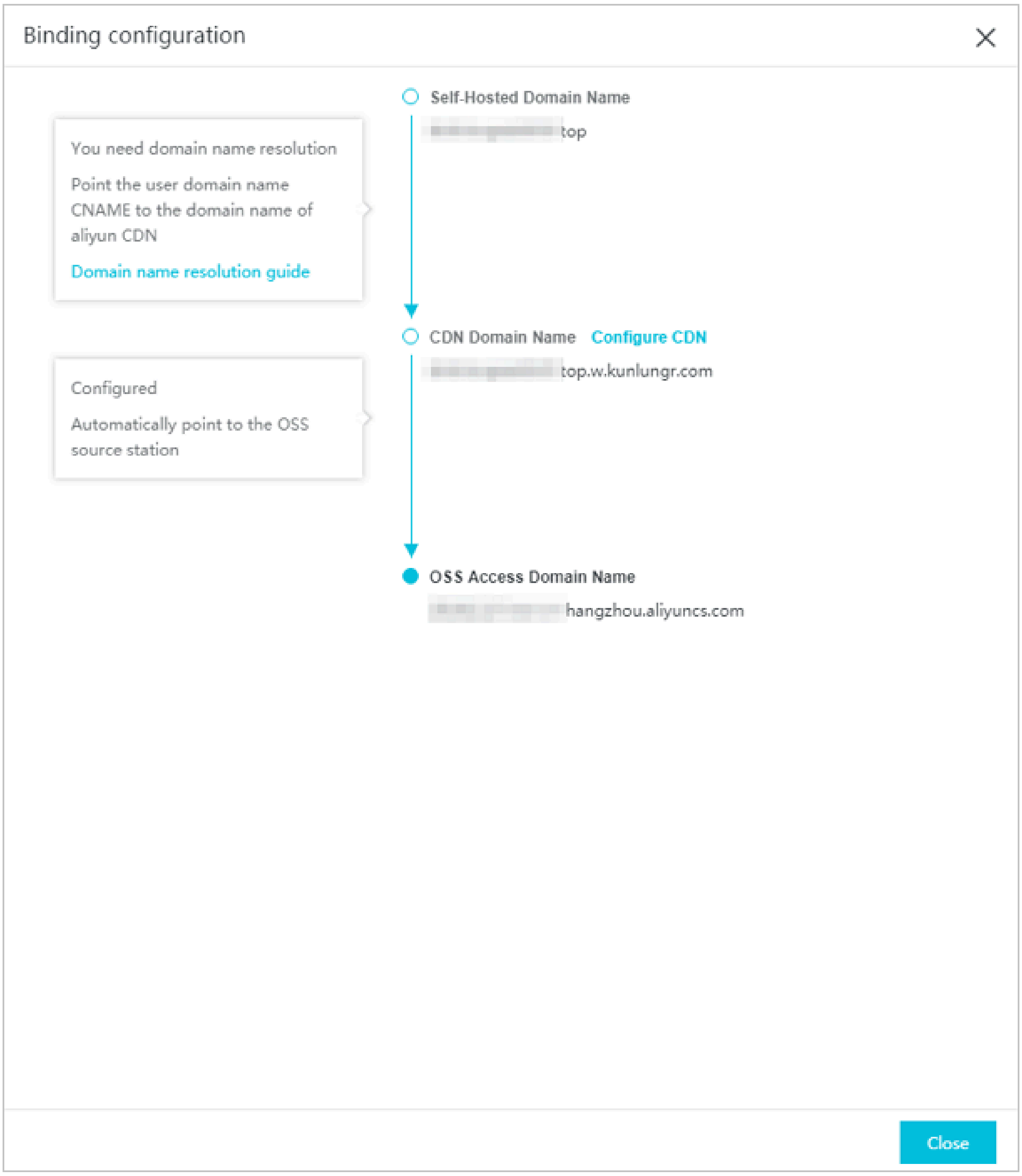


[redacted]

Access Control List (ACL) Private Type Standard Region China (Hangzhou) Created At 11/08/2018, 14:14

It takes about 1 minute to update domain name information. Refresh the domain name list 1 minute after you make changes.

Self-Hosted Domain Name	Enable Alibaba Cloud CDN	Auto CDN Cache Update	HTTPS Certificate	Actions
[redacted]top	Configured	○	Managed in CDN console	Configure CDN Upload Certificate Binding configuration



Binding configuration

You need domain name resolution

Point the user domain name CNAME to the domain name of aliyun CDN

Domain name resolution guide

Configured

Automatically point to the OSS source station

Self-Hosted Domain Name

top

CDN Domain Name Configure CDN

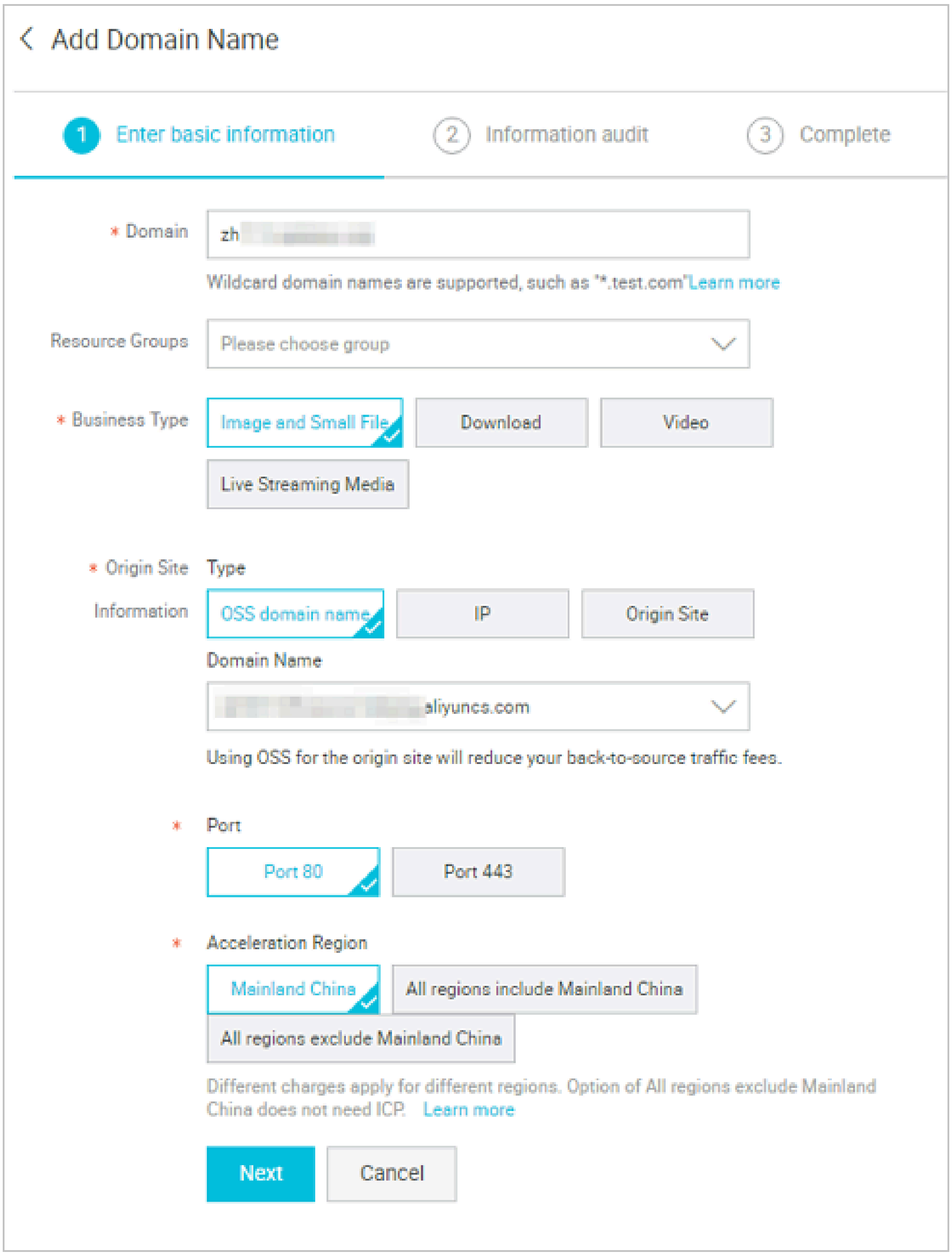
top.w.kunlungr.com

OSS Access Domain Name

hangzhou.aliyuncs.com

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.



Add Domain Name

1 Enter basic information 2 Information audit 3 Complete

* Domain zh[redacted]

Wildcard domain names are supported, such as "*.test.com"Learn more

Resource Groups Please choose group

* Business Type ☑ Image and Small File □ Download □ Video □ Live Streaming Media

* Origin Site Information

Type ☑ OSS domain name □ IP □ Origin Site

Domain Name [redacted]aliyuncs.com

Using OSS for the origin site will reduce your back-to-source traffic fees.

* Port ☑ Port 80 □ Port 443

* Acceleration Region ☑ Mainland China □ All regions include Mainland China □ All regions exclude Mainland China

Different charges apply for different regions. Option of All regions exclude Mainland China does not need ICP. Learn more

Next Cancel

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

Parameter	Description
Port	Select the access port as needed.
Acceleration Region	Select the region in which you want to use the acceleration service.

4. Click Next.

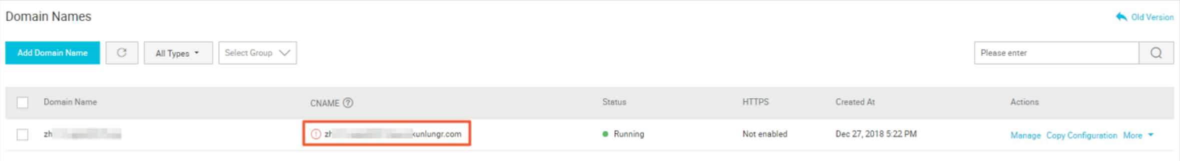
   After you add a CDN acceleration domain name, a CNAME record is generated. You must add the CNAME record to the DNS of your DNS provider to enable the CDN-based acceleration service. For more information, see *Manually add a CNAME record*.

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.

Domain Name	CNAME	Status	HTTPS	Created At	Actions
zh[redacted]	zh[redacted]kunlungr.com	Running	Not enabled	Dec 27, 2018 5:22 PM	Manage Copy Configuration More

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.

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 CNAME record that you copied in *Step 2*.
TTL	Select the update period of the record. In this example, select the default value.

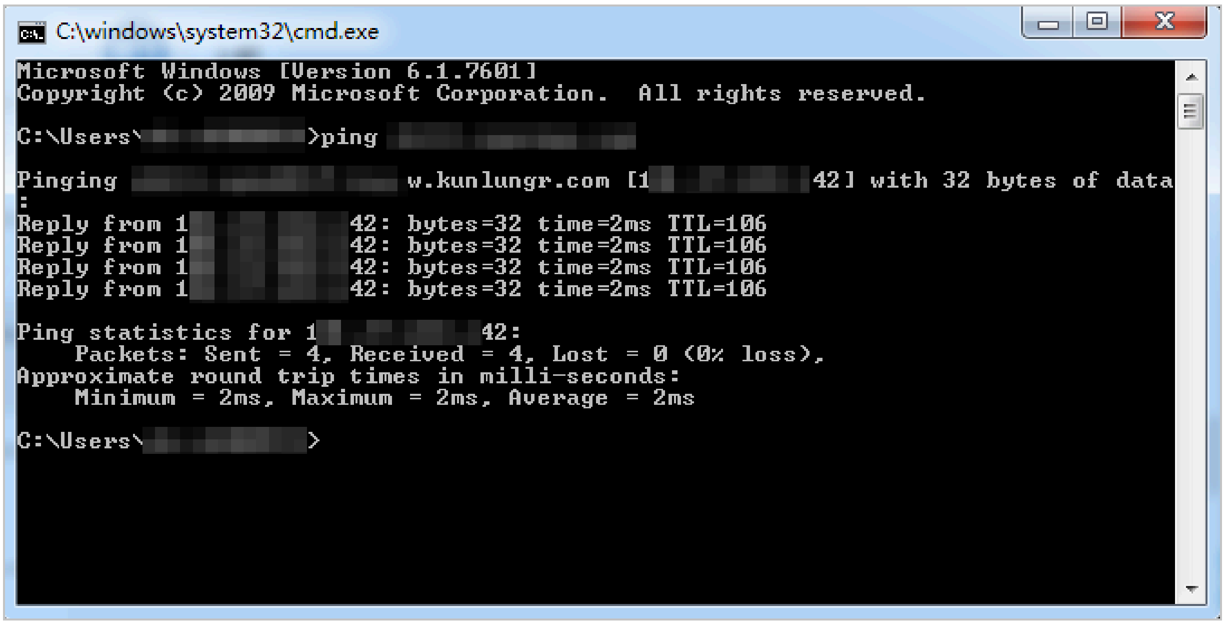
6. Click OK.

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.



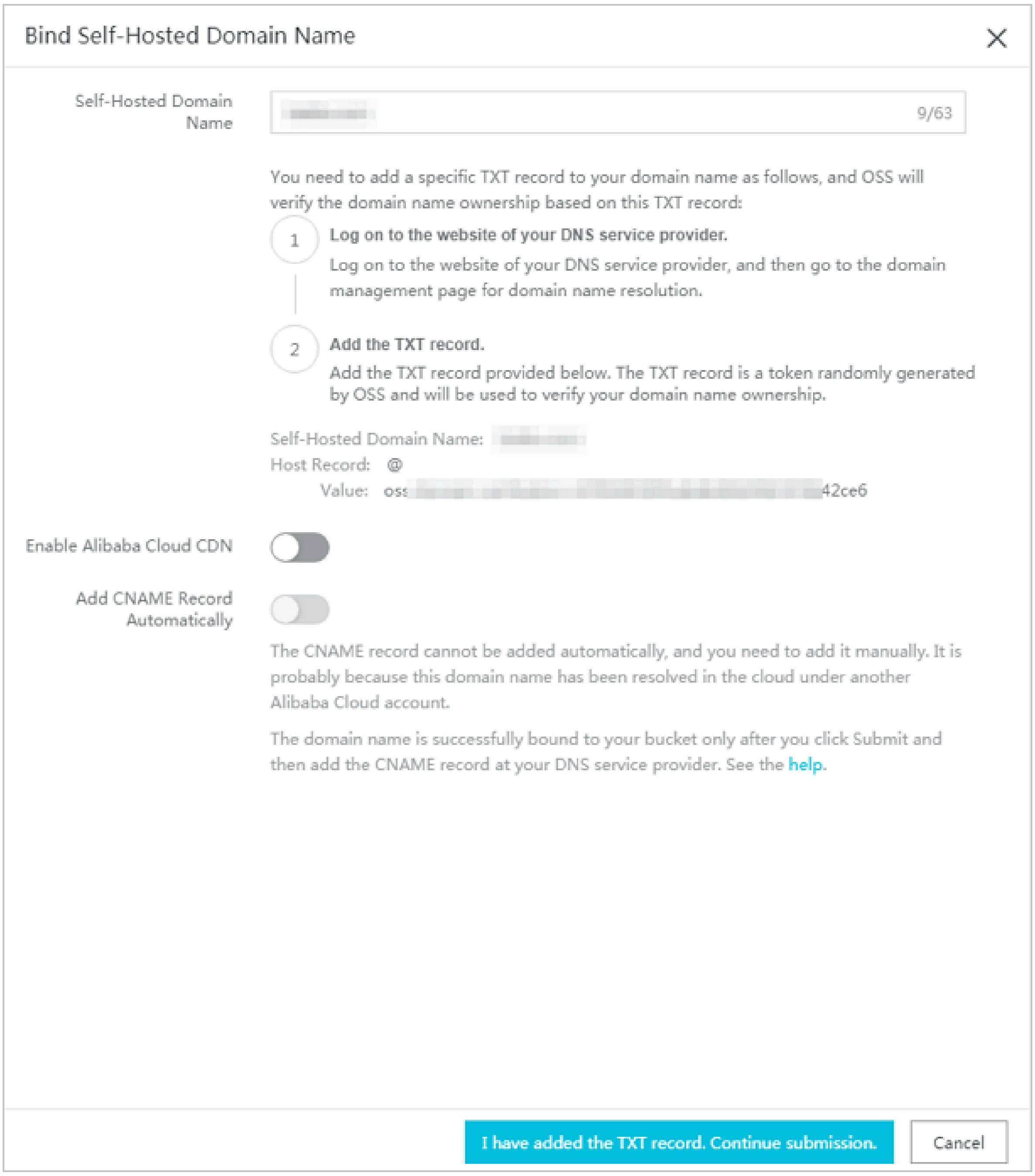
```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\[redacted]>ping [redacted]

Pinging [redacted]w.kunlungr.com [1[redacted]42] with 32 bytes of data
:
Reply from 1[redacted]42: bytes=32 time=2ms TTL=106
Reply from 1[redacted]42: bytes=32 time=2ms TTL=106
Reply from 1[redacted]42: bytes=32 time=2ms TTL=106
Reply from 1[redacted]42: bytes=32 time=2ms TTL=106

Ping statistics for 1[redacted]42:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 2ms, Average = 2ms

C:\Users\[redacted]>
```

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.



Bind Self-Hosted Domain Name

Self-Hosted Domain Name [redacted] 9/63

You need to add a specific TXT record to your domain name as follows, and OSS will verify the domain name ownership based on this TXT record:

1 Log on to the website of your DNS service provider.

Log on to the website of your DNS service provider, and then go to the domain management page for domain name resolution.

2 Add the TXT record.

Add the TXT record provided below. The TXT record is a token randomly generated by OSS and will be used to verify your domain name ownership.

Self-Hosted Domain Name: [redacted]

Host Record: @

Value: oss[redacted]42ce6

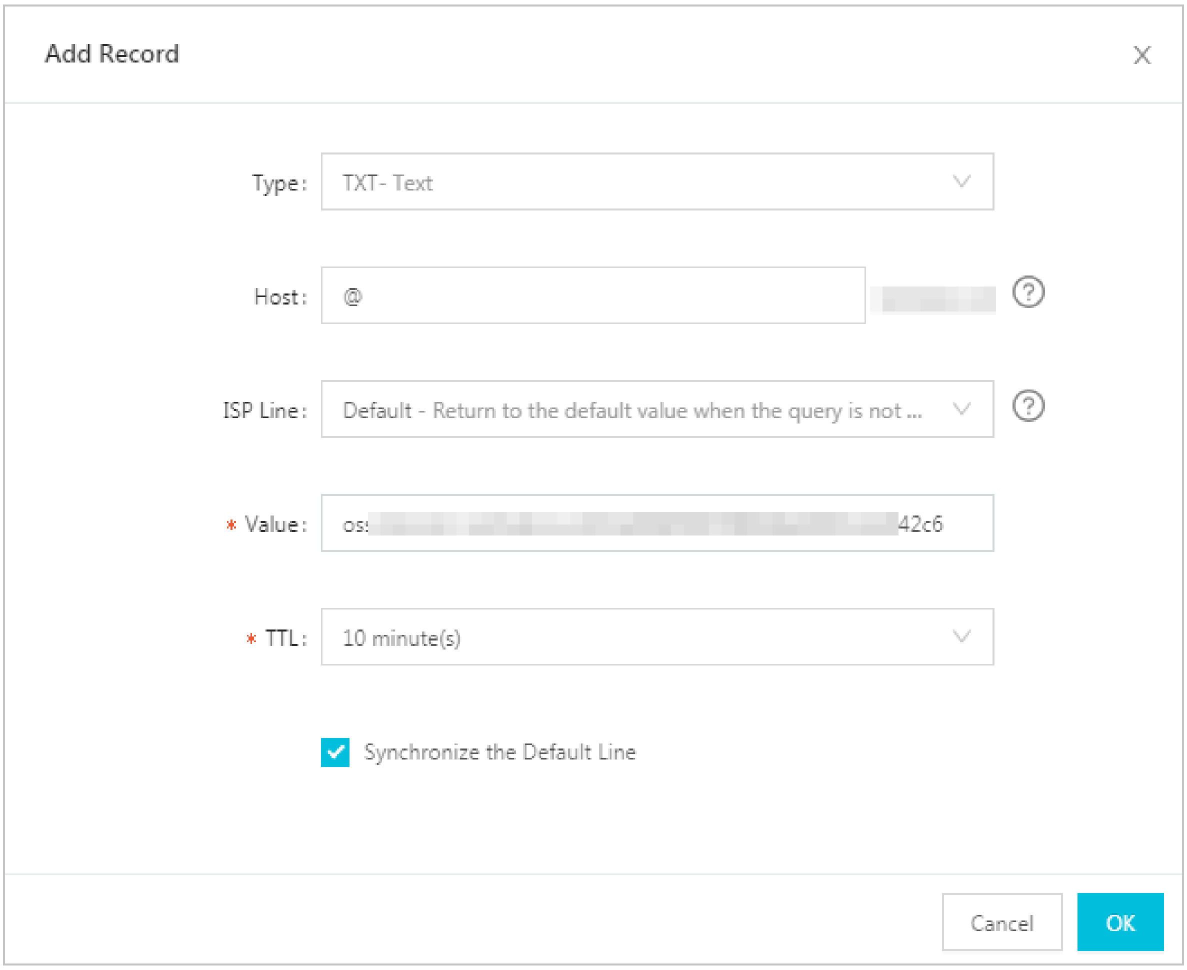
Enable Alibaba Cloud CDN

Add CNAME Record Automatically

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

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

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:



Add Record

Type: TXT- Text

Host: @ [redacted]

ISP Line: Default - Return to the default value when the query is not ...

* Value: os[redacted]42c6

* TTL: 10 minute(s)

☑ Synchronize the Default Line

- 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*.

3.5.3 Certificate hosting

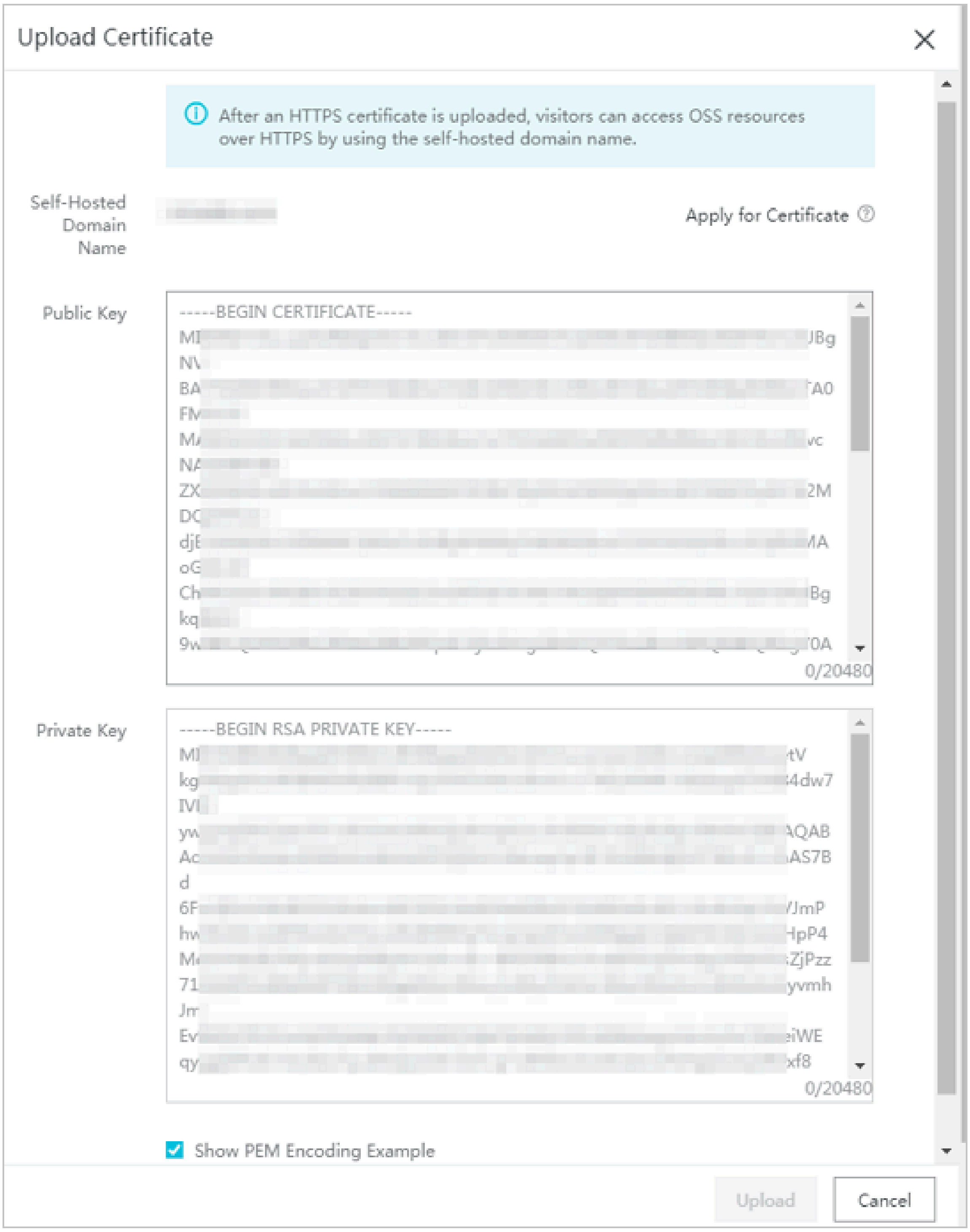
If your want to use your user domain name to access OSS services through the HTTPS protocol, you must purchase a digital certificate. You can purchase certificate services from any certificate authority (CA) or purchase a certificate from *Alibaba Cloud SSL Certificates Service* and host your certificate 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.



Upload Certificate

After an HTTPS certificate is uploaded, visitors can access OSS resources over HTTPS by using the self-hosted domain name.

Self-Hosted Domain Name: [redacted]

Public Key

```
-----BEGIN CERTIFICATE-----
MI[redacted]JBg
NV[redacted]
BA[redacted]A0
FM[redacted]
MA[redacted]vc
NA[redacted]
ZX[redacted]2M
DC[redacted]
djE[redacted]MA
oG[redacted]
Ch[redacted]Bg
kq[redacted]
9w[redacted]0A
0/20480
```

Private Key

```
-----BEGIN RSA PRIVATE KEY-----
MI[redacted]tV
kg[redacted]4dw7
IVI[redacted]
yw[redacted]AQAB
Ac[redacted]AS7B
d
6F[redacted]/JmP
hw[redacted]HpP4
Mc[redacted]ZjPzz
71[redacted]yvmh
Jm[redacted]
Ev[redacted]iWE
qy[redacted]xf8
0/20480
```

☑ Show PEM Encoding Example

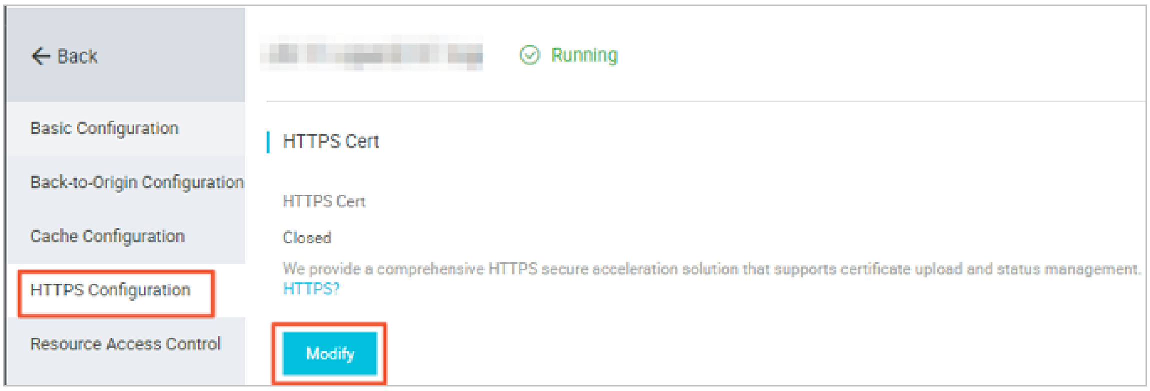
Note:

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.

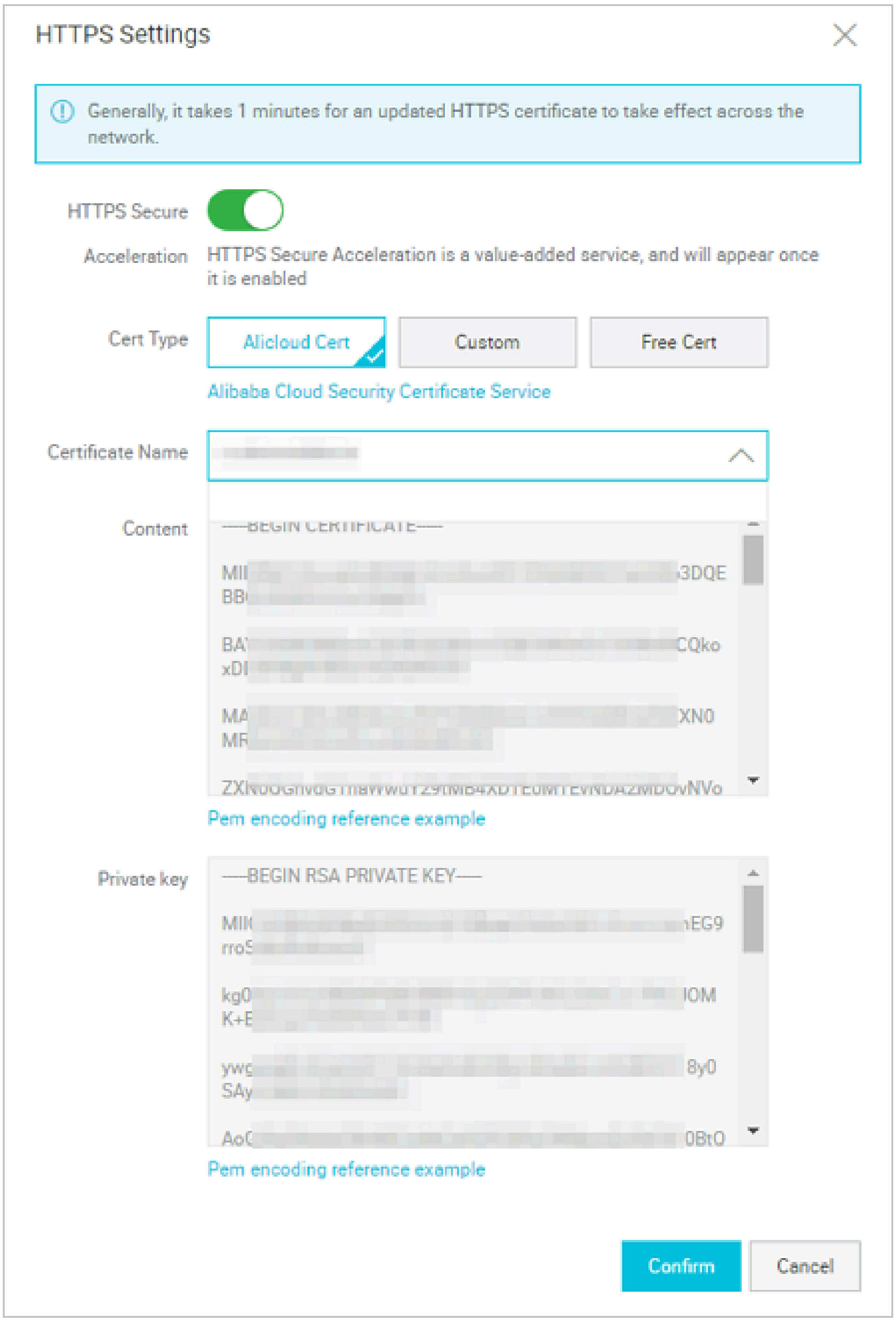


HTTPS Cert

Closed

We provide a comprehensive HTTPS secure acceleration solution that supports certificate upload and status management. HTTPS?

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.



HTTPS Settings

Generally, it takes 1 minutes for an updated HTTPS certificate to take effect across the network.

HTTPS Secure Acceleration: ● HTTPS Secure Acceleration is a value-added service, and will appear once it is enabled

Cert Type: [✓ Alicloud Cert] Custom Free Cert

Alibaba Cloud Security Certificate Service

Certificate Name: [redacted]

Content:

```
-----BEGIN CERTIFICATE-----
MI[redacted]3DQE
BB[redacted]
BA[redacted]CQko
xD[redacted]
MA[redacted]XN0
MR[redacted]
ZXNuUGFivdGTmawwuYz9tMB4XDTEUMTEVNDAZMDOvNVo
```

Pem encoding reference example

Private key:

```
-----BEGIN RSA PRIVATE KEY-----
MII[redacted]EG9
rroS[redacted]
kg0[redacted]IOM
K+E[redacted]
ywc[redacted]8y0
SAy[redacted]
AoC[redacted]0BtO
```

Pem encoding reference example

Confirm Cancel

- 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.

3.6 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 Hongkong 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.

3.7 Set anti-leech

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

Procedure

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

Example

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

3.8 Set a retention strategy

A retention strategy is used to specify the protection period of objects in a bucket. No one can modify or delete a protected object during the protection period. For more information, see *Set a retention strategy*. Currently, you can set a retention strategy only for a bucket in the China South 1 (Shenzhen) region.

Procedure

1. Log on to the *OSS console*.
2. In the bucket list on the left, click the name of the target bucket.
3. Click the Basic Settings tab, locate the Retention Strategy area, and click Configure.
4. Click Create Strategy to open the Create Strategy dialog box.
5. Set the Retention period for the retention strategy.

   The value range of Retention period is 1 day to 70 years.
6. Click OK.

   > Note:
   >
   > After a retention strategy is created, it is in the IN_PROGRESS state. You can Lock or Delete a retention strategy in this state.
7. Click Lock.

   > Note:
   >
   > You cannot delete a locked retention strategy or shorten the retention period of it. Therefore, set a retention strategy with caution.
8. Confirm the retention strategy and click OK.

   > Note:
   >
   > After this step, the strategy is in the LOCKED state. You can click Edit to extend the retention period.

3.9 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 corresponding 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.
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.
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.

3.10 Set lifecycle

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

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

Procedure

1. Log on to the *OSS console*.
2. In the left-side bucket list, click the name of the target bucket to open the overview page of the bucket.
3. Click the Basic Settings tab, locate the Lifecycle area, and then click Edit.
4. Click Create 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.

3.11 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.

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.

3.12 Set back-to-origin rules

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

Note:

Back-to-origin does not support intranet endpoint.

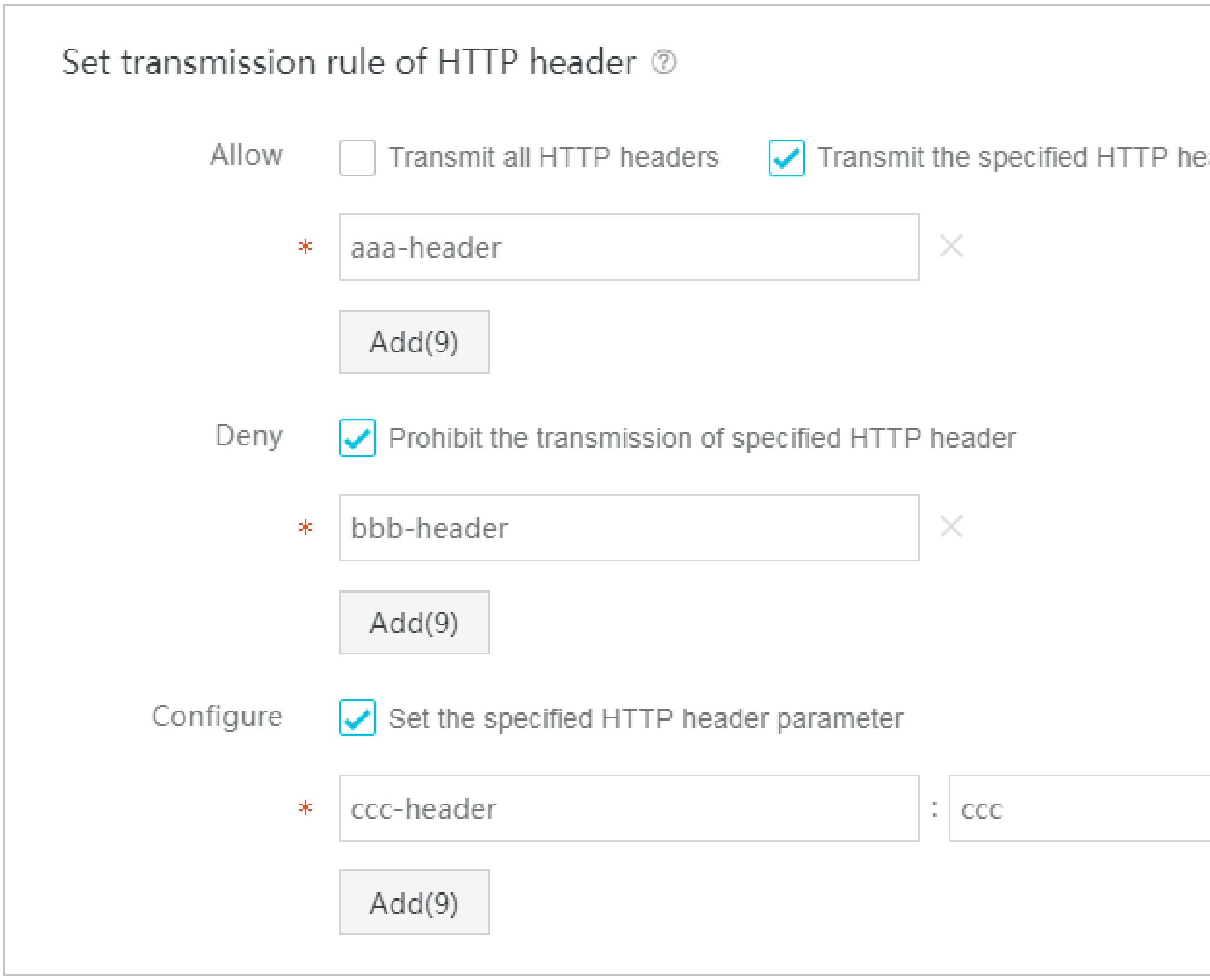
Procedure

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

- If you choose Mirroring and a requested file cannot be found on OSS, OSS will automatically fetch the file from the origin, save it locally, and return the content to the requester.
- If you choose Redirection, OSS redirects requests that meet the prerequisites to the origin URL over HTTP, and then a browser or client returns the content from the origin to the requester.

6. Set Prerequisite and Origin URL. In the Mirroring mode, you can choose to enable Transfer queryString or not. In the Redirection mode, you can set Redirection Code.
7. In the Mirroring mode, you can set the transmission rule of HTTP header.

   The configuration example is as follows:



Set transmission rule of HTTP header

Allow ☐ Transmit all HTTP headers ☑ Transmit the specified HTTP he

* aaa-header

Deny ☑ Prohibit the transmission of specified HTTP header

* bbb-header

Configure ☑ Set the specified HTTP header parameter

* ccc-header : ccc

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

```
GET /object
```

```
host : bucket.oss-cn-hangzhou.aliyuncs.com
aaa-header : aaa
bbb-header : bbb
ccc-header : 111
```

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

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

Note:

The following HTTP headers do not support transmission rules:

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

8. Click OK.

Note:

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

4 Manage objects

4.1 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.

4.2 Upload objects

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

- You can upload the object smaller than 5 GB by using the OSS console.
- You can upload the object larger than 5 GB by using SDKs or APIs. For more information, see *Introduction*.

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

Procedure

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

> Note:
> You can upload a file to a specified folder or to a default folder. You can select *Create a folder* before clicking Upload to upload the file to a specified folder. You can also directly click Upload to upload a file to a default OSS folder.

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

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

    > Note:
    > You can also create a folder manually. For more information, see *Create a folder*.

6. In the File ACL area, select the read/write permissions of the objects to be uploaded. - Inherited from Bucket: By default, the read/write permissions of the objects are inherited from the bucket which the objects are uploaded to. - Private: Only the owner of the bucket and the authorized users can perform read, write, and delete operations on the objects. Other users cannot access the objects. - Public Read: Only the owner of the bucket and the authorized users can perform write and delete operations on the objects. Anyone (including anonymous access) can read the objects. - Public Read/Write: Anyone (including anonymous access) can read, write, and delete the objects. The fees incurred by such operations are borne by the owner of the bucket. Use this permission with caution.
7. Drag one or multiple objects to be uploaded to the Upload area, or click upload them directly to select the objects to be uploaded.
8. Object names must comply with the naming conventions: - Object names must use UTF-8 encoding. - Object names must be at least 1 byte and no more than 1023 bytes in length. - Object names cannot start with a backslash (/) or a forward slash (\ ). - Object names are case sensitive.

4.3 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.

4.4 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.

4.5 Change object ACL

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

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

- Private: Only the creator of the bucket can perform read and write operations on the files in the bucket. Other users cannot access those files.
  - If the read and write permissions of the bucket are "Private", you must set a link validity period when obtaining the file access URL.
  - The validity period for URL signature links is calculated based on NTP. You can give this link to any visitor who can then use it to access the file within the validity period. If the bucket has a private permission, the obtained addresses are generated using the *Add a signature to a URL*.
- Public Read: Only the owner of the bucket can perform write operations on the files in the bucket. Anyone (including anonymous visitors) can perform read operations on the files.
- Public Read/Write: Anyone (including anonymous visitors) can perform read and write 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.

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

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

Compared with the *RAM 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 efficiently.

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.

4.7 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 *Add a signature to a URL*.
- For more information about how to change buckets and objects ACL, see *Change bucket ACL*and *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).

4.8 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.

4.9 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.

4.10 Delete a folder

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

Procedure

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

Note:

Deletion may fail if the folder contains too many files.

5. Click OK to delete the folder.

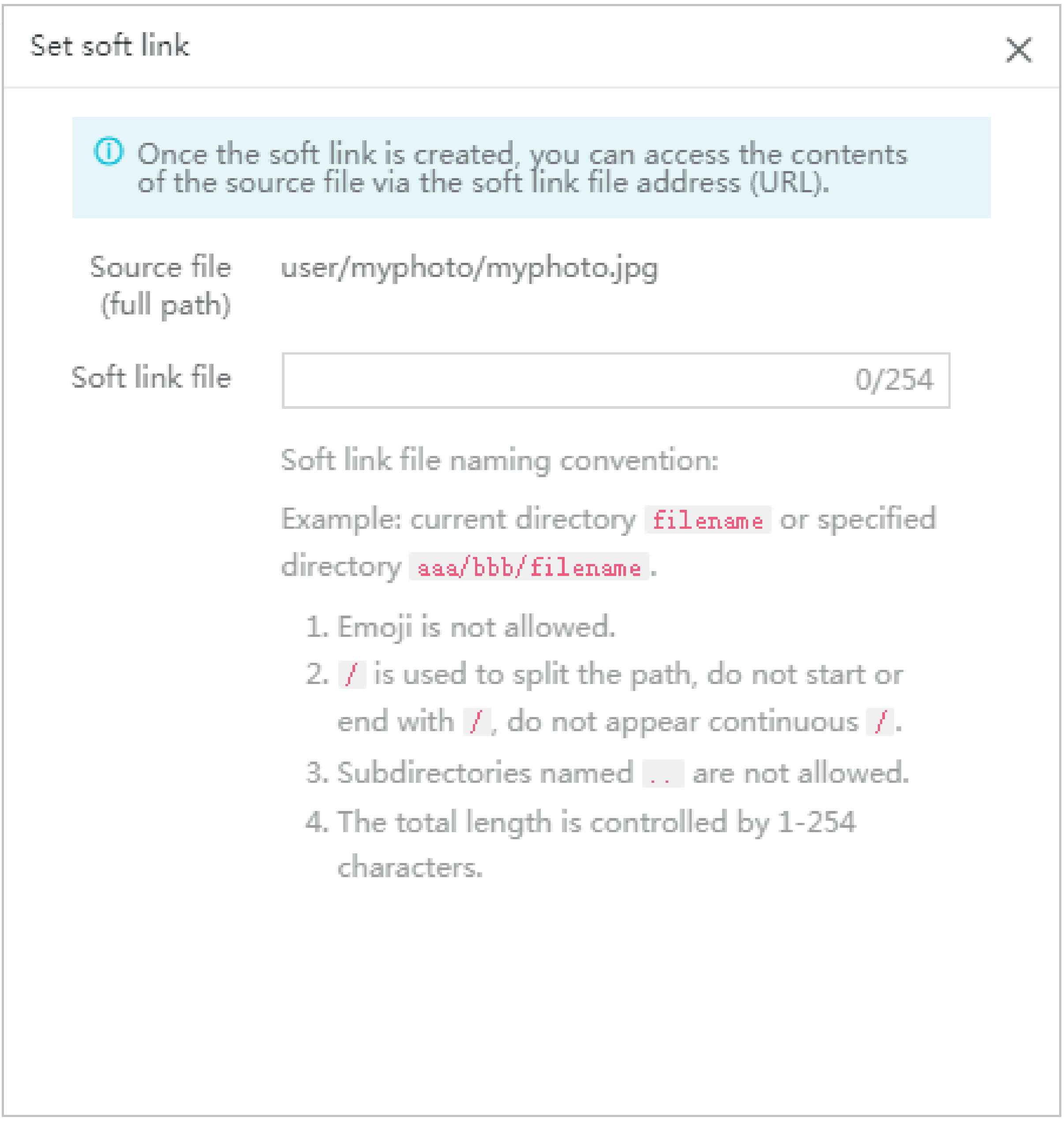
4.11 Set a symbolic link

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.



Set soft link

Once the soft link is created, you can access the contents of the source file via the soft link file address (URL).

Source file (full path): user/myphoto/myphoto.jpg

Soft link file: 0/254

Soft link file naming convention:

Example: current directory `filename` or specified directory `aaa/bbb/filename`.

1. Emoji is not allowed.
2. `/` is used to split the path, do not start or end with `/`, do not appear continuous `/`.
3. Subdirectories named `..` are not allowed.
4. The total length is controlled by 1-254 characters.

- 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.

5 Manage logs

5.1 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 日志存储 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.

5.2 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, as shown in the following figure:
    b. On the Log Analysis page, click Analyze logs.
    c. The log analysis page is displayed. You can view the log analysis result either in the database or in the dashboard.

6 Manage fragments

What are parts?

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

Note:

- You can call the CompleteMultipartUpload to combine the parts into a complete object. For more information on how to use MultipartUpload, see *Introduction*.
- You can regularly clear unnecessary parts by setting the lifecycle management. It is used to clear the parts for which the CompleteMultipartUpload is not complete for a long term in the bucket to reduce the consumption of space. For the detailed procedure, see *Set lifecycle*.
- A part cannot be read before it is combined with other parts into an object. To delete a bucket, you must delete its objects and parts first. Parts are mainly generated by Multipart Upload. For more information, see *Introduction* the API documentation.

Procedures

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

7 Check resource usage

Overview

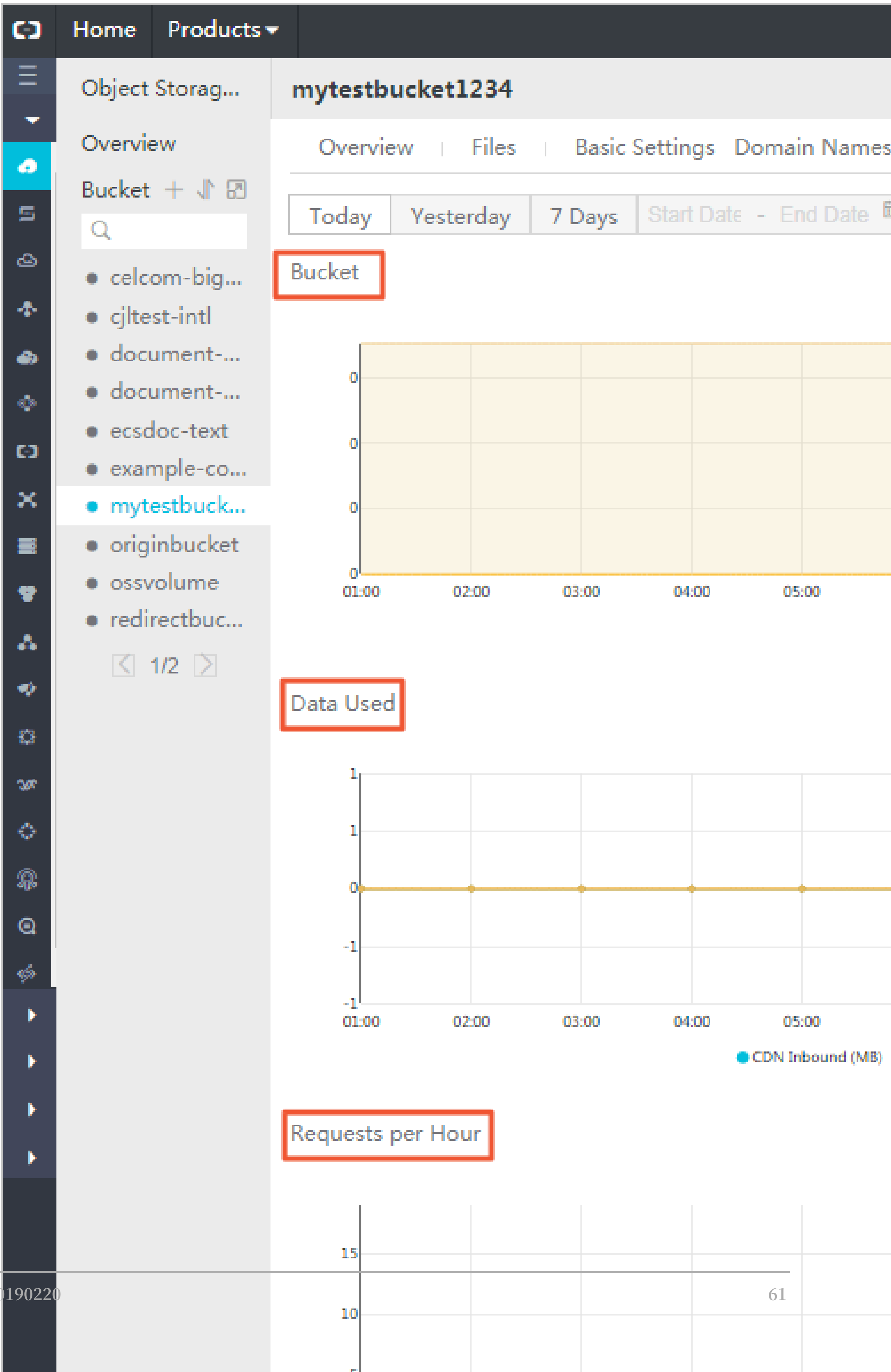
You can check the usage of the following resources on the OSS console:

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

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

Procedures

1. Log on to the *OSS console*.
2. In the bucket list on the left, click the target bucket name to open its information page.
3. Click the Basic Data tab, and diagrams of the following three kinds of basic data are displayed, as shown in the following figure:


Home
Products
Object Storag...
Overview
Bucket
celcom-big...
cjltest-intl
document-...
document-...
ecsdoc-text
example-co...
mytestbuck...
originbucket
ossvolume
redirectbuc...
1/2
mytestbucket1234
Overview
Files
Basic Settings
Domain Names
Today
Yesterday
7 Days
Start Date - End Date
Bucket
0
0
0
0
01:00
02:00
03:00
04:00
05:00
Data Used
1
1
0
-1
-1
01:00
02:00
03:00
04:00
05:00
● CDN Inbound (MB)
Requests per Hour
15
10

- Bucket
- Data Used
- Requests per Hour

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

Table 7-1: Bucket

Basic Data	Description
Standard	Size of data stored in the standard type
Archive	Size of data stored in the archive type
Infrequent Access	Size of data stored in the infrequent access type
Total	Total size of data

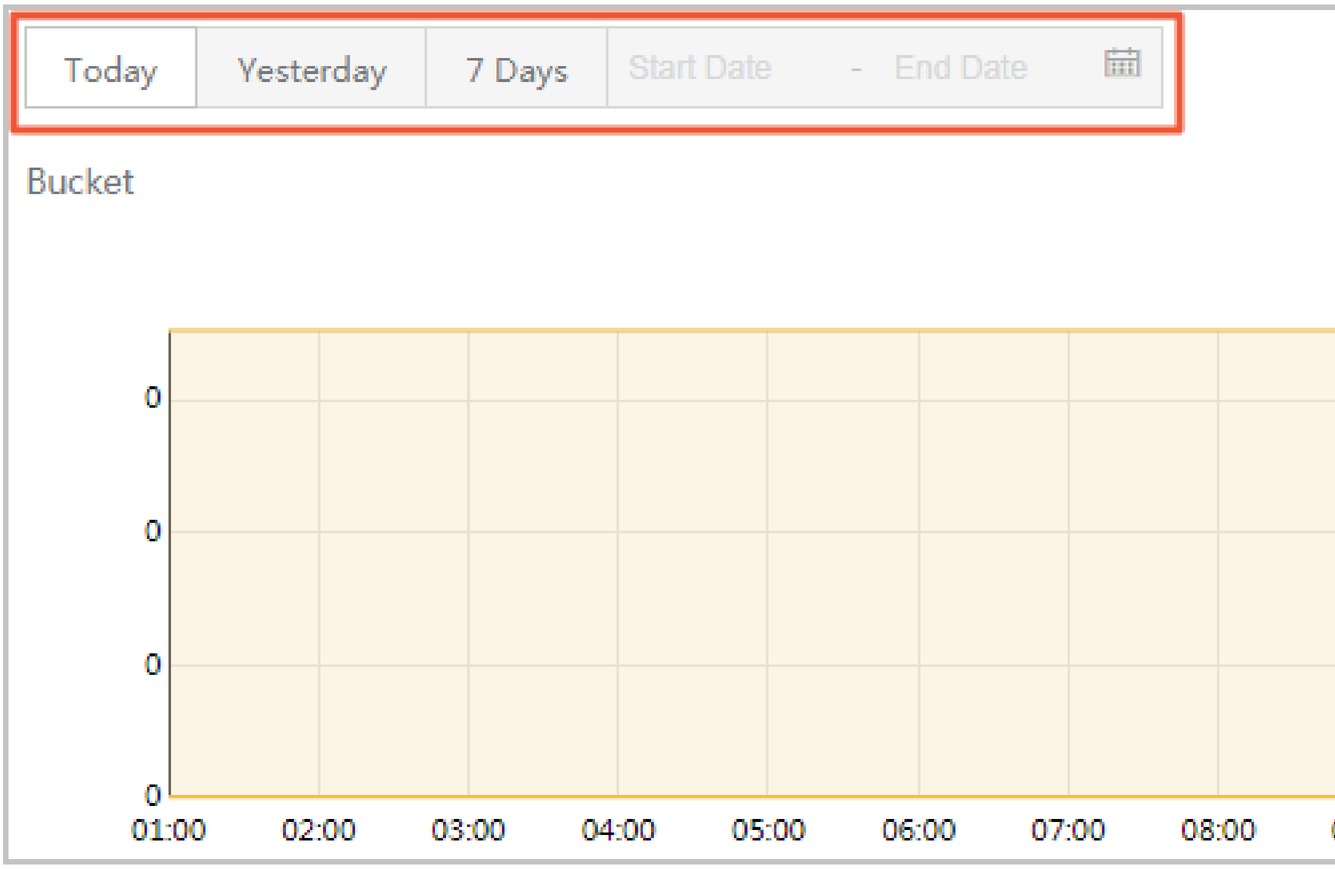
Table 7-2: Data Used

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

Table 7-3: Request per Hour

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

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

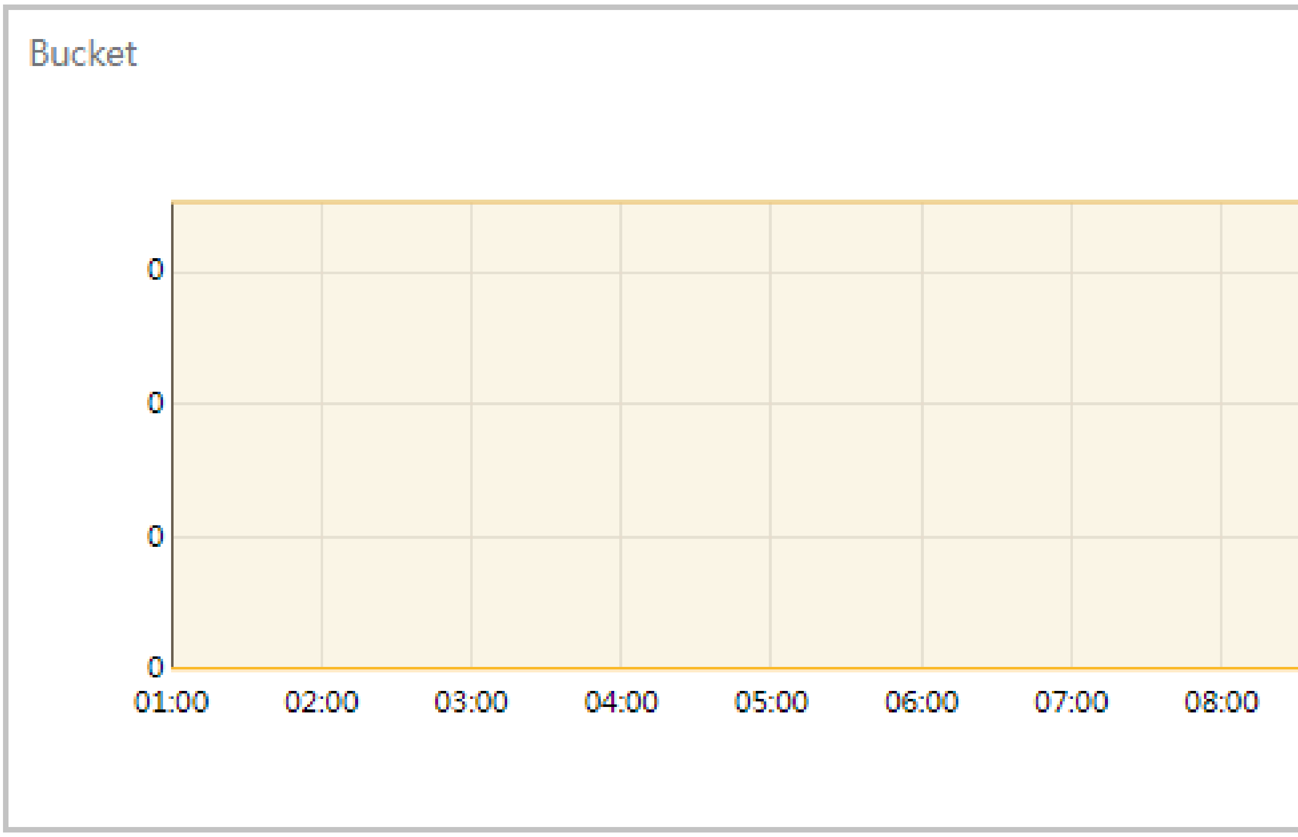


- Today: Only the data of the current day is shown in diagrams.
- Yesterday: Only the data of yesterday is shown in diagrams.
- 7 Days: Only the data of the latest seven days is shown in diagrams.
- Customized time period: You can select the Start Date and the End Date of a time period. The data in this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

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

- The display status of a basic data item is shown on the lower right of a diagram. If the circle before a basic data item is empty, the basic data item is not shown in the diagram. If the circle before a basic data item is solid, the basic data item is shown in the diagram.

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



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

- By clicking the circle before a basic data item, you can switch between the following status: 1. Show the basic data item in the diagram. 2. Do not show the basic data item in the diagram.
- By double-clicking the circle before a basic data item, you can switch between the following two status: 1. Only show this basic data item in the diagram. 2. Show all basic data items in the diagram.