Cloud Object Storage

Console Guide

Product Documentation
Copyright Notice

©2013-2019 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud's the prior written consent.

Trademark Notice

All trademarks associated with Tencent Cloud and its services are owned by Tencent Cloud Computing (Beijing) Company Limited and its affiliated companies. Trademarks of third parties referred to in this document are owned by their respective proprietors.

Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.
Contents

Console Guide
  Console Overview
Bucket Management
  Creating Buckets
  Deleting Buckets
  Querying Buckets
  Empty Buckets
  Setting Access Permission
  Setting Bucket Encryption
  Setting Hotlink Protection
  Setting Origin-Pull
  Setting Cross-Origin Access
  Setting Versioning
  Setting up a Static Website
  Setting Lifecycle
  Setting Log Management
  Accessing Bucket List Using a Sub-account
  Enable Inventory Feature
  Adding Bucket Policies
Domain Name Management
  Overview
    Enabling Default Accelerated Domain Names
    Enabling Custom Accelerated Domain Name
    Enabling Custom Origin Domain
    Granting the sub-account accelerated domain name configuration permission
  Setting Bucket Tags
  Setting Cross-region Replication
  Enabling Global Acceleration
Object Management
  Uploading Objects
  Downloading Objects
  Copying Objects
  Viewing Object Information
  Searching for Objects
  Direct Upload Archiving
  Modifying Storage Class
  Deleting File Fragments
  Setting Object Access Permission
Setting Object Encryption
Custom Headers
Deleting Objects
Restoring Archived Objects
Folder Management
  Creating Folder
  Deleting Folders
  View Folder Details
  Setting Folder Permissions
Data Extraction
Batch Operation
Monitoring Reports
  Querying Monitoring Reports
Picture Processing
  Turn on image processing
Console Guide

Console Overview
Last updated: 2019-09-23 16:05:15

Overview

The Cloud Object Storage (COS) Console is a tool that allows COS users to manage buckets and objects, or perform other operations without programming or running programs. The features available in the COS Console and the operation guides are listed as follows.

<table>
<thead>
<tr>
<th>COS Console Menu</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bucket Management</td>
<td>Creating Buckets</td>
</tr>
<tr>
<td></td>
<td>Deleting Buckets</td>
</tr>
<tr>
<td></td>
<td>Querying Buckets</td>
</tr>
<tr>
<td></td>
<td>Emptying a Bucket</td>
</tr>
<tr>
<td></td>
<td>Setting Access Permissions</td>
</tr>
<tr>
<td></td>
<td>Setting Hotlink Protection</td>
</tr>
<tr>
<td></td>
<td>Setting Origin-Pull</td>
</tr>
<tr>
<td></td>
<td>Setting Cross-Origin Access</td>
</tr>
<tr>
<td></td>
<td>Setting up a Static Website</td>
</tr>
<tr>
<td></td>
<td>Setting Lifecycle</td>
</tr>
<tr>
<td></td>
<td>Accessing Bucket List Using a Sub-account</td>
</tr>
<tr>
<td></td>
<td>Adding Bucket Policies</td>
</tr>
<tr>
<td></td>
<td>Enabling Inventory</td>
</tr>
<tr>
<td></td>
<td>Deleting Incomplete Multipart Uploads</td>
</tr>
<tr>
<td></td>
<td>Domain Name Management</td>
</tr>
<tr>
<td></td>
<td>Setting Bucket Tags</td>
</tr>
<tr>
<td>Object Management</td>
<td>Uploading Objects</td>
</tr>
<tr>
<td></td>
<td>Downloading Objects</td>
</tr>
<tr>
<td>Viewing Object Information</td>
<td>Monitoring Report</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Searching for Objects</td>
<td>Querying Monitoring Reports</td>
</tr>
<tr>
<td>Modifying Storage Class</td>
<td></td>
</tr>
<tr>
<td>Setting Access Permissions for Objects</td>
<td></td>
</tr>
<tr>
<td>Setting Object Encryption</td>
<td></td>
</tr>
<tr>
<td>Customizing Headers</td>
<td></td>
</tr>
<tr>
<td>Deleting Objects</td>
<td></td>
</tr>
<tr>
<td>Recovering Archived Objects</td>
<td></td>
</tr>
<tr>
<td>Creating Folders</td>
<td></td>
</tr>
<tr>
<td>Deleting Folders</td>
<td></td>
</tr>
<tr>
<td>Viewing Folder Details</td>
<td></td>
</tr>
</tbody>
</table>
Bucket Management
Creating Buckets

Overview

You can create buckets on the Bucket List page on the COS Console. For more information on buckets, see Bucket Overview.

Up to 200 buckets are allowed under the same user account (regardless of region).

Steps

1. Log into the COS Console.
2. On the left sidebar, click Bucket List to enter the bucket list, and then click Create Bucket.

3. In the pop-up Create Bucket dialog box, configure the following information:
   - **Name**: Enter a custom bucket name, which cannot be modified once configured. For naming instructions, see Naming Conventions.
   - **Region**: Select the COS region corresponding to your physical zones where your business (or number of users) is concentrated. This cannot be modified once configured. For more information on regions, see Regions and Access Domain Names.
   - **Access Permissions**: Three access permissions are available for buckets by default: "Private Read/Write", "Public Read/Private Write" and "Public Read/Write". The permission can be modified after configured. For more information, see Setting Access Permission.
   - **Bucket Tag**: Bucket tag is used as an identifier to manage buckets. For more information, see Setting Bucket Tags.
   - **Server-Side Encryption**: Currently, the supported bucket encryption method is SSE-COS encryption (i.e., server encryption using COS-managed keys). For more information on server encryption, see Server
Encryption Overview.

4. Verify all the information entered is correct, and then click **OK** to create a bucket. On Bucket List page, you can view the newly created bucket.
Deleting Buckets

Overview

You can delete buckets on the Bucket List page on the COS console. For more information on buckets, see Bucket Overview.

To delete a bucket, first make sure to delete all objects in the bucket and all fragments in Incomplete Upload.

Directions

1. Log in to the COS console, click Bucket List to enter the bucket detail page and then click Delete on the right of the target bucket.

2. In the Delete Bucket confirmation popup box, click OK to delete the bucket.
Querying Buckets

Overview

You can query created buckets quickly using the Cloud Object Storage (COS) Console.

- Before you can access a bucket list with a sub-account, the sub-account must be authorized by the root account. For more information, see Accessing Bucket List Using a Sub-Account.
- List Bucket is independent of bucket permission restrictions. Restricting a sub-account's query to some specific buckets is not supported.

Directions

1. Log in to the COS Console. On the left sidebar, click Bucket List to open the Bucket List page, which contains all created buckets.

<table>
<thead>
<tr>
<th>Bucket Name</th>
<th>Monitoring</th>
<th>Region</th>
<th>Time Created</th>
</tr>
</thead>
<tbody>
<tr>
<td>examplebucket-125444</td>
<td></td>
<td>Chengdu (China) (ap-chengdu)</td>
<td>2019-03-20 15:29:59</td>
</tr>
</tbody>
</table>

2. In the search box on the right, you can enter a bucket name or a prefix of a bucket name to search for the desired bucket.

3. When the access permission for the bucket is Public Read/Write or Public Read/Private Write, a Public status is indicated next to the bucket name to alert you to the security risk.
<table>
<thead>
<tr>
<th>Bucket Name</th>
<th>Monitor Status</th>
<th>Region</th>
</tr>
</thead>
<tbody>
<tr>
<td>eu-frankfurt-1256</td>
<td>Read</td>
<td>Frankfurt, German federal state (Europe) (eu-frankfurt)</td>
</tr>
<tr>
<td>examplebucket-1256</td>
<td></td>
<td>Chengdu (China) (ap-chengdu)</td>
</tr>
<tr>
<td>examplebucket-oversea</td>
<td></td>
<td>Tokyo, Japan (Asia-Pacific) (ap-tokyo)</td>
</tr>
</tbody>
</table>

Bucket public access status: The objects in this bucket can be accessed by any anonymous users, thus data security risks may exist. This may be because you have set bucket permissions to public (read/write) or public read & private write, or because you have configured any anonymous user access in the bucket policy. Please use these configurations with caution.
Empty Buckets

Last updated: 2019-09-30 11:31:54

Overview

You can empty the specified bucket in the COS Console. For more information about buckets, see Bucket Overview.

Emptying a bucket will delete all files and file fragments in it permanently. Please do so with cautions.

Steps

1. Log in to the COS Console and click Bucket List in the left sidebar to enter the bucket list page.
2. Click the name of the bucket you want to empty to enter its File List page.
3. On the file list page, click Clear Buckets.
4. On the confirmation page, enter the name of the bucket you want to delete and click Yes.

5. At this point, you can see that the bucket has been emptied.
Setting Access Permission

Overview

You can set or modify bucket access permissions using the COS Console or APIs. COS supports two permission types:

- **Public Permissions**: Private Read/Write, Public Read/Private Write, and Public Read/Write. For more information, see Type of Access in the "Bucket Overview".
- **User Permissions**: The root account has all the permissions (full control) for buckets by default. In addition, you can add sub-accounts that are granted permissions to read/write data and read/write permissions, and even full access to buckets.

You can modify the access permissions for a bucket in Permission Management.

Directions

1. Log in to the COS Console. On the left sidebar, click Bucket List to open the Bucket List page.
2. Locate the bucket for which you want to set or modify access permissions, and then click the bucket name.

<table>
<thead>
<tr>
<th>Bucket Name</th>
<th>Monitoring</th>
<th>Region</th>
<th>Time Created</th>
</tr>
</thead>
<tbody>
<tr>
<td>examplebucket-125688888888</td>
<td><img src="monitoring.png" alt="monitoring" /></td>
<td>Chengdu (China) (ap-chengdu)</td>
<td>2019-03-20 15:29:59</td>
</tr>
</tbody>
</table>

3. In the Bucket Configuration page, click Permission Management to set Public Permissions and User Permissions for the bucket (for example, add a sub-account).
4. Click **Save** to apply the access permissions.
Setting Bucket Encryption

Overview

You can set server-side encryption for a bucket in the COS Console, so that new objects uploaded to the bucket can be encrypted by default. For more information on bucket encryption, please see Bucket Encryption Overview.

Currently, the supported bucket encryption method is SSE-COS encryption (i.e., server-side encryption using COS-managed encryption keys). For more information on server-side encryption, please see Server-side Encryption Overview.

Directions

Setting encryption when creating a bucket
You can configure bucket encryption when creating a bucket, as shown below:

```
Create Bucket

Name: examplebucket
Region: China
Server-Side Encryption: None

Access Permissions
- Private Read/Write
- Public Read/Private Write
- Public Read/Write

Endpoint: examplebucket-1256285578.cos.ap-chengdu.myqcloud.com

Bucket Tag
- Enter a tag key
- Enter a tag value

OK  Cancel
```

**Setting encryption for an existing bucket**

If you do not set encryption when creating a bucket, you can follow the steps below to set configuration subsequently.

1. On the Bucket List page, click the name of the bucket for which to set encryption to enter the bucket configuration page.
2. Click Basic Configuration on the left to enter the basic configuration page of the bucket.
3. Scroll down to Bucket Encryption, click Edit, and change the current status to "Enabled".
4. Select the specified encryption method and click **Save**.
Setting Hotlink Protection

Overview

Tencent Cloud COS provides hotlink protection support for users to avoid unnecessary losses caused by malicious programs' cheating for public network traffic using resource URLs or stealing of resources by malicious means. It is recommended that you configure the blacklist/whitelist in Hotlink Protection Settings in the console for security protection.

Procedure

1. Log in to the COS Console and then select the Bucket List in the left pane to go to the Bucket List page. Click the bucket (such as examplebucket-1250000000) for which you want to set hotlink protection to enter the bucket.

2. Find the Bucket for which you want to set up Hotlink protection Prevent hotlinking, click its name, and go to the Bucket management page.

3. Click Basic Configuration, find Hotlink Protection Settings, and click Edit.
4. Modify the current status to Enabled, select a list type (blacklist or whitelist), enter applicable domain names, and then click Save.
   - Blacklist: Domain names on this list are not allowed to access the default access address of the bucket. 403 is returned if any domain name on the list accesses such address.
   - Whitelist: Only domain names on this list are allowed to access the default access address of the bucket. 403 is returned if any domain name not on the list accesses such address.
   - In HTTP requests, the header referer can be left empty. (An HTTP request header without the field of referer is allowed or the referer field is empty.)
   - Referer: Support setting up to 10 domain names with the same prefix matching, each line, multiple lines, please wrap; domain name, IP and wildcard characters are supported * And other forms of address. Example:
     - If `www.example.com` is specified, `www.example.com/123`, `www.example.com.cn`, and other addresses with the prefix of `www.example.com` will also be included in the list; Domain names and IPs with ports are supported, such as `www.example.com:8080` And `10.10.10.10:8080` .
     - If `*.example.com` is specified, such addresses as `a.b.example.com/123` And `a.example.com` are also included.

If accelerated access is implemented via CDN domain name, CDN hotlink protection rules will be executed before COS hotlink protection rules.

**Samples**
A user with the APPID of 1250000000 creates a bucket named examplebucket-1250000000 and places an image picture.jpg in the root directory, and COS generates the following default access address according to
the rules:

```
http://examplebucket-1250000000.file.myqcloud.com/picture.jpg
```

User A owns a website:

```
www.example.com
```

And embeds the image into the homepage index.html.

Webmaster B manages a website:

```
www.fake.com
```

And wants to put this image on `www.fake.com`. But he doesn’t want to pay for traffic costs. He creates a direct link to `picture.jpg` through the following address and places it into the homepage index.html on `www.fake.com`.

```
http://examplebucket-1250000000.file.myqcloud.com/picture.jpg
```

To avoid losses of User A in such cases, we provide the following two methods to enable hotlink protection.

**Method 1**

Configure the **Blacklist** By entering the domain name `*.fake.com`, and save.

**Method 2**

Configure the **Whitelist** By entering the domain name `*.example.com`, and save.

**Before enabled**

The image is displayed normally when `http://www.example.com/index.html` is accessed.
The image is also displayed normally when `http://www.fake.com/index.html` is accessed.

**After enabled**

The image is displayed normally when `http://www.example.com/index.html` is accessed.
The image cannot be displayed when `http://www.fake.com/index.html` is accessed.

**Mini Program's related instructions**

1. The referer of Mini Program's network request is not allowed, and the format is fixed as `https://servicewechat.com/{appid}/{version}/page-frame.html` For more information, please see [Mini Program development document](#).

2. To access the COS resources of WeChat Mini Programs and Access, please configure Hotlink protection Prevent hotlinking whitelist on the COS console: [servicewechat.com](#).
Setting Origin-Pull

Overview

You can configure origin-pull rules for buckets on COS Console. If the object you request does not exist in the bucket, or a specific request needs to be redirected, you can configure origin-pull rules to access corresponding data via COS. Origin-pull configurations are mainly used for data hot migration, redirection of specific requests, and other scenarios.

The success rate of data origin-pull depends on network environment.

Steps

1. Log into the COS Console, select Bucket List in the left pane to enter the Bucket List page. Click the bucket for which you want to configure CORS to enter the bucket details page.
2. Click **Basic Configuration** on the left to enter the basic configuration page of the bucket.

3. Scroll down to find the [Origin-Pull Configurations] item, change the current status to On, and enter the origin-pull address. The configuration items are described as follows:
   - **Origin-Pull Address**: Enter the domain name or IP address without the `http://` or `https` prefix. You can also add the port number after the domain name or IP address.
   - **Origin-Pull Protocol**: The HTTP protocol when COS accesses the origin server you have specified. The options are Force HTTPS, Force HTTP, and Follow Request Protocol.
     - If you select Force HTTPS/HTTP, COS will access your origin server using HTTPS/HTTP protocol.
     - If you select Follow Request Protocol, COS will access your origin server with the protocol you use to request COS.
   - **Origin-Pull Parameter**: Specify whether to pass in request parameters used when accessing the COS to the origin server.
   - **3xx Following Policy**: When the origin server returns a 3XX redirect status code, COS by default will follow 3XX to pull data from another origin server again. If you select Off, resources will not be pulled.
   - **Add Origin-Pull Header**: When COS accesses your origin server, it can carry the newly added header you have specified for access. Currently, up to 10 new custom headers can be added.

Example of a correct address:

```
abc.example.com
abc.example.com:8080
10.10.10.10
10.10.10.10:8080
```

5. Click **Save**.

**Samples**

**Background**

A user whose APPID is 1250000000 created a bucket named “examplebucket-1250000000”, and enabled CDN accelerated domain name:

```
examplebucket-1250000000.file.myqcloud.com
```

Configure the origin-pull address of the bucket to:

```
abc.example.com
```
Store the image picture.jpg at the origin server http://abc.example.com.

**Initial access from the client:**

http://examplebucket-1250000000.file.myqcloud.com/picture.jpg

When COS finds that the object cannot be hit, it returns the HTTP status code 302 to the client and is redirected to the following address:

http://abc.example.com/picture.jpg

The origin server then provides the object to the client to ensure access, and COS copies picture.jpg from the origin server and saves it to the root directory of the bucket "example".

**The second access:**

http://examplebucket-1250000000.file.myqcloud.com/picture.jpg

COS directly hits the picture.jpg object in the root directory and returns it to the client.
Setting Cross-Origin Access

Overview

You can set Cross Origin Resource Sharing (CORS) for objects in buckets through the COS Console. COS supports configuring multiple rules to respond to OPTIONS requests. CORS is a mechanism that allows resources at one origin to be requested from another origin through HTTP requests. Origins are deemed different from each other as long as their protocols, domain names or ports are different.

COS supports response to OPTIONS requests for CORS, and returns specific rules set by developers to browsers, but the server does not verify whether subsequent cross-origin requests conform to the rules. For more information, see Cross-Origin Resource Sharing.

Procedure

1. Log in to the COS Console, and then select the Bucket List in the left pane to go to the Bucket List page. Click the bucket of the object for which you want to set CORS to enter the bucket.

2. Click Basic Configuration to go to the Basic Configuration page of the bucket, find CORS Settings, and click Add Rule.

3. Add rule information (Fields with * are required). Configuration items are as follows:

   **Source Origin**: The domain names allowed for cross-origin requests.
More than one domain name can be specified, with one domain name per line. wildcard * is supported, which means all domain names are allowed. Not recommended. A single specific domain name is supported, such as http://www.abc.com. Second-level wildcard domain names are supported, such as http://*.abc.com. Only one second-level wildcard domain name with only one * in it is allowed per line. Do not omit protocol name HTTP or HTTPS, and specify the port if the port is not default 80.

**Operating Methods**: GET, PUT, POST, DELETE, and HEAD are supported. Enumeration of one or more methods is allowed for a cross-domain request.

**Allow-Headers**: Allow-Header is used to notify the server about which custom HTTP request headers are allowed for subsequent requests when an OPTIONS request is sent, such as x-cos-meta-md5. More than one header can be specified, with one header per line. Header is easy to be omitted, so it is recommended to set this field to * to indicate that all headers are allowed if there is no special requirement. Uppercase and lowercase letters [a-z, A-Z] are supported, and no underscores (_) are allowed. Each header specified in Access-Control-Request-Headers must also be provided in Allowed-Header.

**Expose-Headers**: Expose-Header returns a common header for COS. For more information, see the Common Request Headers. The configuration should be specific to the requirements of application. Etag is recommended. Wildcard is not allowed. Headers are case insensitive, with one header per line.

**Timeout Max-Age**: Sets the validity period (in seconds) of the results obtained by OPTIONS. The value must be a positive integer, such as 600.
4. After configuration, click **Submit** and you will see the CORS rules added. To modify it, click the **Modify** button.
Setting Versioning

Overview

With versioning, you can store multiple versions of an object in a bucket and retrieve, delete, or restore a specified version. This can help you recover from data loss caused by accidental deletion or application failure.

- Once versioning is enabled for the bucket, it cannot be disabled. However, you can suspend versioning to stop object versioning.
- After versioning is enabled, newly uploaded objects will generate multiple versions and take up storage space, so these versions of the object will also charge for storage.

Directions

1. Log in to the COS Console and click Bucket List in the left sidebar to enter the bucket list page.
2. Click the bucket to be configured to enter the bucket details page.
3. Click Advanced Configuration on the left to enter the advanced configuration page of the bucket, scroll down to Versioning, and click Edit on the right.
4. Click Enable in “Status” and save the change. In the pop-up window, click OK to enable versioning. When you no longer need versioning, you can simply click Disable to disable it.
Are you sure you want to enable versioning?

You can not close versioning after you open it, if you do not need it, you can disable it.

Versioning documents

OK  Cancel
Setting up a Static Website

Overview

You can configure a bucket to host a static website in the COS Console and access the static website at the bucket's access domain name. For more information on static websites, see Static Website Hosting.

To use buckets to host static websites, you first need to set the access permission to the buckets to Public Read/Private Write.

Prerequisites

A bucket has been created. For more information, see Creating a Bucket.

Directions

1. Log in to the COS Console, select Bucket List on the left sidebar, and click the bucket to host a static website to enter the bucket details page.

<table>
<thead>
<tr>
<th>Bucket Name</th>
<th>Monitoring</th>
<th>Region</th>
<th>Time Created</th>
</tr>
</thead>
<tbody>
<tr>
<td>examplebucket-1250288222</td>
<td></td>
<td>Chengdu (China) (ap-chengdu)</td>
<td>2019-03-20 15:29:59</td>
</tr>
</tbody>
</table>

2. Click Permission Management on the left and find Bucket ACL. Select Public Read & Private Write in the Public Permissions configuration item.
3. Click **Basic Configuration** on the left and find the **Static Website** configuration item. Click **Edit**, toggle on the **Status** switch, and set the static website configuration items, as shown below:

**Force HTTPS (optional):** After Force HTTPS is enabled, when an end user accesses your static website, the access node of the static website will forcibly enable the HTTPS protocol.

**Index Document (required):** An index document (i.e., the homepage of the static website) is a page returned when the root directory or any subdirectory of a website is requested, which is usually named index.html.

If folders are created in the bucket, the index document needs to be added at each folder level.

**Error Document (optional):** An error document is a page returned after an error occurs in accessing a static website. This configuration item allows you to define an error document. When the static website cannot respond to end user requests, the specified custom error page will be returned. For example, when an HTTP error occurs in accessing, if an error document named error.html is configured, the error.html page will be returned for easy troubleshooting. However, if it is not configured, the default error message will be returned.

Only a file in the bucket root directory can be configured as an error document. A file that is recognizable by browsers should be used, such as an `.html` or `.htm` file. Most browsers will display "inaccessible" or "access request denied" if an unrecognizable file such as a `.zip` file is used.

**Redirect Rules (optional):** With redirection rules, you can redirect requests based on specific file paths, prefixes in requests, or response codes.
For example, if a file in a bucket is deleted or renamed, you can add a redirection rule to redirect requests to other files.

- **Error codes:** The redirection rules only support redirection configurations for $4xx$ error codes (e.g., 404). You can customize the error page and add troubleshooting guidelines there, so that when a corresponding HTTP error is triggered, the end user can find more useful information.
- **Prefix matching:** You can use a prefix matching rule to redirect requests to files or folders in the bucket. For more information, see [Redirection Rule Example](#).

### Static website hosting

<table>
<thead>
<tr>
<th>Status</th>
<th>[ ]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoint</td>
<td>[ ]</td>
</tr>
<tr>
<td>Force HTTPS</td>
<td>[ ]</td>
</tr>
</tbody>
</table>

- **Endpoint:** [https://examplebucket-12345.cos-window.ap-chengdu.myqcloud.com](https://examplebucket-12345.cos-window.ap-chengdu.myqcloud.com)

- **Index document:** index.html
- **Error document:** error.html

### Redirect rules

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
<th>Force HTTPS</th>
<th>Rule</th>
<th>Replace content</th>
<th>Actions</th>
</tr>
</thead>
</table>

- [Save](#) [Cancel](#)
4. After completing the configuration, click **Save**.

![Static website hosting configuration](image)

<table>
<thead>
<tr>
<th>Static website hosting</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>On</td>
</tr>
<tr>
<td>Endpoint</td>
<td><a href="https://examplebucket-125.cos-website.ap-chengdu.myqcloud.com">https://examplebucket-125.cos-website.ap-chengdu.myqcloud.com</a></td>
</tr>
<tr>
<td>Force HTTPS</td>
<td>On</td>
</tr>
<tr>
<td>Index document</td>
<td>index.html</td>
</tr>
<tr>
<td>Error document</td>
<td>error.html</td>
</tr>
<tr>
<td>Redirect rules</td>
<td><img src="image" alt="Table" /></td>
</tr>
<tr>
<td>Type</td>
<td>No data to display</td>
</tr>
<tr>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>Force HTTPS</td>
<td></td>
</tr>
<tr>
<td>Rule</td>
<td></td>
</tr>
<tr>
<td>Path</td>
<td></td>
</tr>
</tbody>
</table>
Setting Lifecycle

Overview

You can use the lifecycle management feature when you need to change the storage class or delete specified objects regularly to reduce costs. COS will automatically change the storage class or delete specified objects within the specified time frame according to the rules you set. For more information, see Lifecycle Overview.

A lifecycle can be set to a maximum of 3,650 days.

Directions

1. Log in to the COS Console.
2. On the left sidebar, click Bucket List to enter the bucket list page.
3. Locate the bucket for which you want to enable the lifecycle feature. Click the bucket name to enter its details page.

<table>
<thead>
<tr>
<th>Bucket Name</th>
<th>Monitoring</th>
<th>Region</th>
<th>Time Created</th>
</tr>
</thead>
<tbody>
<tr>
<td>examplebucket-12567890</td>
<td></td>
<td>Chengdu (China) (ap-chengdu)</td>
<td>2019-03-20 15:29:59</td>
</tr>
</tbody>
</table>

4. Click Basic Configuration on the top, scroll down to Lifecycle and then click Add Rules.

   Lifecycle
   
<table>
<thead>
<tr>
<th>Rule ID</th>
<th>Applied to</th>
<th>Rule content</th>
<th>State</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Add rule</td>
</tr>
</tbody>
</table>

   Note: Rules can be configured to periodically drop objects, delete objects, and delete fragment objects uncompleted. Due to object specification limitations for IAR (Infrequent Access) Storage and Archive Storage types, there is a minimum specification limit for settled objects and your storage usage may increase. For more information or help, please refer to Learn more.

5. Add lifecycle rules as needed. The configuration items are described as follows:
   - **Rule Name**: Enter a name for the lifecycle rule.
- **Applied to**: This lifecycle rule can be applied to the entire bucket or objects with a specific prefix in the bucket, such as examplevault. If you select **Specified Prefix**, you need to enter a prefix.

- **Prefix**: For more information on object keys (or prefixes), see **Object Overview**. For more information on the configuration rules for the lifecycle, see **Rule Description**.

- **Manage current version**: You can transition or delete objects in the current version by enabling **Manage current version**. You can transition the objects in a bucket from COS Standard to COS Infrequent Access or Archive Storage, and delete the objects upon their expiration. Storage classes include **COS Standard > COS Infrequent Access > Archive Storage** (from hot storage to cold storage). Storage classes can only be changed from hot to cold. Calculation of days is based on the modification time of files in COS.

- **Manage previous versions**: You can transition or delete objects of previous versions by enabling **Manage historical versions**. If it is not enabled, only objects of the latest version are processed by default.

- **Clean up expired object delete markers**: If you delete certain version of an object, all previous ones of this version will expire, and the delete markers for the expired objects are retained. Although the delete markers do not incur storage costs, the removal of them can improve the performance of **LIST** operations.

- **Delete incomplete multipart uploads**: If some parts of the files fail to be uploaded due to some reasons, you can use this feature to delete the parts associated with these multipart uploads.
After the lifecycle rules are configured, click **OK** and you will see the lifecycle rules.
7. When you want to disable a lifecycle rule, click **Edit** to change the status of the rule to **Disable** or delete the lifecycle rule.

![Modify rule](image)

- If the object settles to the [IA](Infrequent Access) Storage type or the Archive Storage type, it will be limited by the object specification. If the object size is less than the minimum specification, it will be calculated according to the minimum specification.

- **State**: On / Off
Setting Log Management

Overview

You can log in to the COS Console to enable log management for a bucket, which records various requests related to **bucket operations**. Log management facilitates buckets usage and management. For more information on log management, see Log Management Overview.

- The log management feature is currently only available in four regions including Beijing, Shanghai, Guangzhou, Chengdu and Toronto.
- Currently, only the **bucket owner** has permission to set log management, and the Log Management configuration item will not be displayed to other users when they log in to the console.
- The log data is delivered every 5 minutes. COS does not guarantee 100% accuracy of the log data. It is for reference only and is not used as a basis for measurement and billing.

Directions

1. Log in to the **COS Console**, click **Bucket List** in the left sidebar, and click the source bucket that needs the log management enablement.

<table>
<thead>
<tr>
<th>Bucket Name</th>
<th>Monitoring</th>
<th>Region</th>
<th>Time Created</th>
</tr>
</thead>
<tbody>
<tr>
<td>examplebucket-125654789</td>
<td><img src="status.png" alt="Monitoring" /></td>
<td>Chengdu (China) (ap-chengdu)</td>
<td>2019-03-20 15:29:59</td>
</tr>
</tbody>
</table>

2. Click **Advanced Configuration** on the left, find the **Log Management** configuration item, and click **Edit** to enter the editable state.
3. Click Enable to the right of **Status** and click **Save**.

4. Confirm that the feature is enabled. Select the destination bucket (i.e., the bucket that stores the logs), and set the key prefix for the log object (e.g., `log/`). After confirming that the entered information is correct, click **Save**. The configuration items are as described below:

   - **Destination Bucket**: the source bucket for which log management is enabled and the destination bucket that stores the logs must be in the same region. It is not recommended to use the source bucket itself as the destination bucket.
   - **Target prefix**: enter a custom path prefix that makes it easy for you to find the logs.

**Notes**

1. To enable the log management feature, you need to create a log role in the CAM Console and grant it read/write permission to the logs of the source bucket.
2. When the log management feature is disabled, if the role is not deleted, its read/write permission to the logs of the source bucket will not be revoked.
Accessing Bucket List Using a Sub-account

Last updated: 2020-01-15 09:27:58

Overview

Sub-accounts do not have the permission to pull the bucket list by default. Therefore, if you log in to the COS Console with a sub-account, you cannot access buckets, bucket list, or statistics in Bucket List, as shown below.

You can allow a sub-account to access a bucket by adding an access path or access the bucket list by adding the preset policy QcloudCOSGetServiceAccess (i.e., the permission to obtain the bucket list) to it.

This feature is applicable to scenarios where the sub-account is logged in to the console to access the bucket.

Adding an Access Path

Sub-accounts are not granted the preset policy QcloudCOSGetServiceAccess by default and thus do not have the permission to pull the bucket list. When granted the permissions (e.g., data Read or Write permissions) to a bucket by the root account, a sub-account can then access this bucket by adding an access path.

Directions

1. Log in to the COS Console with a sub-account, enter the Access Path List page, and click Add Access Path.
2. In the **Add Access Path** pop-up window, select the bucket region and enter the access path, as shown below:
   - **Region**: Select the region of the bucket to be allowed for access.
   - **Access Path**: Enter the name of the bucket to be allowed for access (e.g., `examplebucket-1250000000`), or the path to an object in the bucket (e.g., `examplebucket-1250000000/exampleobject.txt`).

![Add access path](image)

3. After confirming that the region and the access path are correct, click **OK** to add the path to the authorized bucket or an object in it.

![Add Access Path](image)

### Adding a Preset Policy

A sub-account can access the bucket list by **adding the preset policy QcloudCOSGetServiceAccess** (i.e., the permission to obtain the bucket list) to it.

- The preset policy `QcloudCOSFullAccess` or `QcloudCOSReadOnlyAccess` can also grant a sub-account access permission to the bucket list. However, due to the wide coverage of permissions granted by these two policies, **they are not recommended for security reasons**.
- The collection of statistics in the overview requires the access permission to the bucket list. When the sub-account needs to pull statistics, please make sure that the root account has added the
preset policy QcloudCOSGetServiceAccess to it; otherwise, the system will prompt that the sub-account has no access permission to the statistics.

Directions

1. Log in to the CAM Console with the root account and click the created sub-account.

2. Click Associate Policies, search for and add the preset policy QcloudCOSGetServiceAccess (i.e., the permission to access the bucket list in COS) in the policy list, and click OK to associate the policy.
3. You can view the added policies here. When you no longer need a policy, you can unbind it.

<table>
<thead>
<tr>
<th>Policy Name</th>
<th>Bind Type</th>
<th>Policy Type</th>
<th>Association Time</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>QcloudCOSGetService</td>
<td>Direct Bind</td>
<td>Preset policy</td>
<td>2019-03-21 12:01:22</td>
<td>Disassociate</td>
</tr>
</tbody>
</table>
Enable Inventory Feature

Overview

You can enable inventory for your bucket in the COS Console. The inventory feature allows you to regularly output an inventory report of object attributes and configuration details for your bucket on a daily or weekly basis. For more information about inventory, see Inventory Feature Overview. The following section will guide you through how to enable inventory for a bucket.

- You can configure multiple inventory tasks in one bucket.
- Such tasks do not directly read the object content during their execution; instead, they only scan the attribute information such as object metadata.

Steps

1. Log in to the COS Console.
2. In the left sidebar, click Bucket List and then click the bucket (source bucket) for which you want to enable inventory.
3. Click the Advanced Configuration tab, find the Inventory Settings item, and click Add an Inventory.
4. On the **Add an Inventory** page, you can configure the following items:

- **Inventory Name**: Name the output inventory report.
- **Destination Prefix (Optional)**: Enter the prefix selected for the destination bucket, which can group the inventory files in a public location. The default value is used initially.
- **Destination Bucket**: This is the bucket where the inventory is stored. The default value is the source bucket. The destination bucket must be in the same region as the source bucket.
- **Status**: You can choose to enable or disable the inventory.

![Add Inventory Form](image)

- **Output Format**: Select the output format for the inventory report. Default is CSV.
- **Object Version**: Choose to keep only the current version or include all versions.
- **Generate Lifecycle**: Select the frequency for generating the inventory report. Options are Everyday or Everyweek.
- **Filter Prefix (Optional)**: Enter a prefix to filter objects for the inventory.
- **Inventory Encryption**: Select the encryption method. Options are None or SSE-COS.
- **Inventory Information**: Select the information to include in the inventory report. Options include Size, ETag, Multipart Upload Status, Storage Class, Cross-region Replication Status, and Last Updated.

By checking the box, you agree to grant Tencent Cloud COS service access to bucket resources.

[Save] [Cancel]
- **Advanced Settings**: You can configure more inventory information in the advanced settings. If you leave them alone, all the default settings will be used:

- **Output Format**: The default value is CSV format.

- **Object Version**: Select whether to include all object versions or only the current version in the inventory. If you do not make a selection, only the current version is included by default.

- **Generation Cycle**: Select whether to export the inventory daily or weekly. If you do not make a selection, the report is exported daily by default.

- **Filter**: Add a prefix to the filter to only inventory the objects whose names begin with the same string. If you do not enter a prefix, no filter is used by default.

- **Inventory Encryption**: Select whether to encrypt the inventory on the server. Options include:
  - No encryption: The inventory is not encrypted. This is the default value.
  - SSE-COS: Encrypt the report using server-side encryption with COS-managed key. For more information, see [SSE-COS Encryption](#) in the COS Developer Guide.

- **Inventory Information**: Select the object information to be included in the inventory report. Options include object size, storage class, ETag, cross-region replication status, multipart upload status, and last modified date. If you do not make a selection, all items are selected by default.

An entity tag (ETag) is a hash of the object. It only reflects changes to the object's content but not the object's metadata. It may or may not be an MD5 digest of the object data. This depends on how the object was created and encrypted.

5. After confirming that the configuration information is correct, click **Save**.
Adding Bucket Policies

Overview

You can add a policy to a bucket in the COS Console to allow or forbid an account, IP, or IP range to access the COS resources. For more information about bucket policy and samples, see Access Policy Overview and Bucket Policy Samples. The following section will guide you through how to add a bucket policy.

For each root account, the total number of created object ACLs, bucket ACLs, and bucket policies cannot exceed 1,000.

Steps

1. Log in to the COS Console.
2. In the left sidebar, click Bucket List.
3. Select the bucket to which to add a bucket policy and enter it.

4. Click Permission Management and find Bucket Policy. COS supports adding the bucket policy through Generator and Strategy grammar, which you can choose as you like.

- Graphic settings
  Below is an example:
○ **Strategy grammar**

Click **Edit** and enter the policy syntax you define. COS provides policy syntax for a rich variety of
scenarios. For more information, see Bucket Policy Samples.

5. After confirming that the configuration information is correct, click **OK** or **Save**. At this point, sub-account can only access the resource range set by the policy after logging in to the COS Console.
Domain Name Management
Overview

CDN acceleration is used to speed up the download and delivery of COS bucket content, especially if the same content is downloaded repeatedly.

Setup Instructions

You can manage the following domain names to quickly download and deliver objects in buckets:

- **Default domain**: This is COS origin server's domain name, which is automatically generated based on the bucket name and region when the bucket is created. It should be distinguished from the default accelerated domain name.
- **Default accelerated domain**: This is the domain name passing through CDN acceleration nodes and is generated by the system. You can choose to enable/disable it.
- **Custom accelerated domain**: You can bind the registered custom domain name to the bucket on Tencent Cloud's domestic CDN acceleration platform, and access the objects in the bucket via the custom domain name.
- **Custom origin domain**: You can bind the registered custom domain name to the current bucket, and access the objects in the bucket via the custom domain name.

You must activate CDN acceleration to use a custom domain name supported by COS:

1. Domain names bound to CDN Mainland China needs ICP filing, but it does not need to be through Tencent Cloud.
2. Domain names bound to CDN Outside Mainland China do not need ICP filing, but note that the data and operations on Tencent Cloud still need to comply with the laws and regulations of relevant countries/regions and the Tencent Cloud Service Agreement.

With CDN acceleration enabled for the default accelerated domain name or the custom domain name, if the origin server is a public-read bucket, the objects in the origin server can be accessed directly via the CDN accelerated domain name or the custom domain name; if the origin server is a private-read bucket, it is recommended to enable the CDN origin-pull authentication and CDN authentication configuration options.

- Origin-pull authentication (CDN service authorization must be added before it can be enabled): If the data requested by a user is not cached in the edge node, CDN fetches the data from the origin server. If COS is used as the origin server and origin-pull authentication is enabled, the CDN edge server accesses the COS
origin server using a special service identity (which must be authorized by CDN service) to acquire and cache the data in the private bucket.

- CDN authentication: When a user attempts to acquire cached data by accessing an edge server, the edge server verifies the authentication field in the accessed URL based on the authentication configuration rules to prevent unauthorized access and realize hotlink protection, thus improving the security and reliability of the data cached in the edge server.

CDN authentication configuration and CDN origin-pull authentication do not conflict with each other, but whether to enable them can affect the level of data protection, as shown below:

<table>
<thead>
<tr>
<th>Bucket access permission</th>
<th>CDN origin-pull authentication</th>
<th>CDN authentication configuration</th>
<th>Origin server can be accessed via CDN accelerated domain name</th>
<th>Origin server can be accessed via COS origin server's domain name</th>
<th>Scenarios</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public read</td>
<td>Disabled</td>
<td>Disabled</td>
<td>Yes</td>
<td>Yes</td>
<td>Public read globally</td>
</tr>
<tr>
<td>Public read</td>
<td>Disabled</td>
<td>Enabled</td>
<td>URL authentication is required</td>
<td>Yes</td>
<td>Not recommended</td>
</tr>
<tr>
<td>Public read</td>
<td>Enabled</td>
<td>Disabled</td>
<td>No</td>
<td>Yes</td>
<td>Not recommended</td>
</tr>
<tr>
<td>Public read</td>
<td>Enabled</td>
<td>Enabled</td>
<td>URL authentication is required</td>
<td>Yes</td>
<td>Not recommended</td>
</tr>
<tr>
<td>Private read + CDN service authorization</td>
<td>Enabled</td>
<td>Enabled</td>
<td>URL authentication is required</td>
<td>COS authentication is required</td>
<td>Protection throughout link</td>
</tr>
<tr>
<td>Private read + CDN service authorization</td>
<td>Disabled</td>
<td>Enabled</td>
<td>URL authentication is required</td>
<td>COS authentication is required</td>
<td>Not recommended</td>
</tr>
<tr>
<td>Private read + CDN service authorization</td>
<td>Enabled</td>
<td>Disabled</td>
<td>Yes</td>
<td>COS authentication is required</td>
<td>Origin server protection</td>
</tr>
<tr>
<td>Bucket access permission</td>
<td>CDN origin-pull authentication</td>
<td>CDN authentication configuration</td>
<td>Origin server can be accessed via CDN accelerated domain name</td>
<td>Origin server can be accessed via COS origin server's domain name</td>
<td>Scenarios</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------------------------</td>
<td>--------------------------------</td>
<td>-------------------------------------------------</td>
<td>-------------------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>Private read + CDN service authorization</td>
<td>Disabled</td>
<td>Disabled</td>
<td>No</td>
<td>COS authentication is required</td>
<td>Not recommended</td>
</tr>
<tr>
<td>Private read</td>
<td>Disabled</td>
<td>Enabled or disabled</td>
<td>No</td>
<td>COS authentication is required</td>
<td>CDN is unavailable</td>
</tr>
</tbody>
</table>

For the first row of the above list, if the bucket access permission in origin server is public read, and neither CDN origin-pull authentication nor CDN authentication configuration is enabled, then CDN edge servers and buckets in origin server can be accessed directly via the CDN domain name, and buckets in origin server can be accessed directly via the COS domain name.

After CDN acceleration is enabled for a domain name, anyone can directly access the origin server via the domain name. Therefore, if you need to keep your data private, be sure to protect your data in the origin server through **Authentication Configuration**.

The relevant operation

- **Enabling Default Accelerated Domain Names**
- **Enabling Custom Accelerated Domain Name**
- **Enabling Custom Origin Domain**
- **Granting the sub-account accelerated domain name configuration permission**
Enabling Default Accelerated Domain Names

Overview

This article shows you how to turn on a custom accelerated domain name. The steps are as follows.

Procedure

1. Log in to the COS Console. Click **Bucket List** on the left sidebar to open the Bucket List page.
2. Click the bucket for which you need to set a domain name to go the COS configuration page, as shown below:

![Bucket List](image)

3. Click **Domain Name Management** on the left, click **Edit** in the **Default Accelerated Domain Name**, set the current status of the default accelerated domain name to **Enabled**, and configure as follows:
   - **Origin Server Type**: The origin server type usually defaults to **Default Origin Server**, but if you have enabled static website for the origin server bucket and want to accelerate content delivery for the
static website, select **Static Website Origin Server**.

- **Origin-pull Authentication**: For public-read buckets, you don't need to enable **Origin-pull Authentication**. For private-read buckets, enable **Origin-pull Authentication** after adding CDN service authorization.

  If you have never used Tencent Cloud CDN service, you need to go to CDN Console to activate CDN service before you can access **Domain Name Management**.

4. Click **Save** to activate CDN acceleration.

For private-read buckets, if both origin-pull authentication and CDN service authorization are enabled, signature is not required for the access to origin server via CDN, and cached resources in CDN will be distributed on the public network, which will affect the data security. Therefore, it is recommended to enable CDN authentication.

**Enabling origin-pull authentication**

1. For private-read buckets, **Origin-pull Authentication** needs to be enabled provided that CDN service authorization is added.
2. Enable **Origin-pull Authentication** on the bucket domain name management page. (CDN service authorization must be added before it is enabled.)
3. Click **Save** to activate CDN acceleration.

4. After clicking **Save**, you can see the default accelerated domain name is under deployment. The status of **CDN authentication** is displayed at the bottom. Click **Authentication Configuration** to configure authentication, as shown below:

![Default CDN Acceleration Domain](image)

5. You can go to CDN authentication configuration page from **CDN Console** by clicking **Domain Management** -> **Management** for the domain name -> **Security Configuration**.
Enabling Custom Accelerated Domain Name

Overview

This document only describes how to add a custom accelerated domain name and enable CDN acceleration on the COS Console. For more information on how to add a custom domain name on the CDN Console, see Domain Names Access.

A maximum of 10 custom domain names can be added on the COS Console.

Procedure

1. Log in to the COS Console. Click Bucket List on the left sidebar to open the Bucket List page.
2. Click the bucket for which you need to set a domain name to go the COS configuration page, as shown below:

3. Click Domain Management on the left, click Add Domain in the column Custom Acceleration Domain, and configure as follows:
   - Domain Name: Enter the custom domain name to be bound (e.g. www.example.com). Ensure that the domain name entered has gone through the filing procedure, and that CNAME corresponding to this domain name has been set at the DNS service provider for the domain name. For more information, see CNAME Configuration.
   - Origin-pull Authentication: Enable origin-pull authentication. For private-read buckets, enable Origin-pull Authentication to protect the origin server.
For private-read buckets, if both origin-pull authentication and CDN service authorization are enabled, then signature is not required for accessing the origin server via CDN, and cached resources in CDN will be distributed on the public network, which will affect the data security. Therefore, it is recommended to enable CDN authentication (Step 5).

4. After the configuration, click **Save** on the operation column on the right to add the domain name. After it is saved, the Enable button for CDN authentication appears in the **CDN Authentication** column. You can click the button to enable the CDN authentication for custom domain name.

   **CDN Authentication**: Timestamp authentication can be configured to prevent stealing by malicious users. You can enable the feature after adding the domain name.

5. Log in to **CDN Console**. On the left sidebar, click **Domain Name Management**.

6. Locate the domain name you need to configure, click **Management** on the operation column on the right to go to the domain name management page, and then click **Security Configuration** at the top.

   After CDN acceleration is enabled for a domain name, anyone can directly access the origin server via the domain name. Therefore, if you need to keep your data private, be sure to protect your data in the origin server through **Authentication Configuration**.
Enabling Custom Origin Domain

Last updated: 2019-09-30 17:47:17

Overview

This step shows how to bind the custom domain name to the bucket. You can access the files in the bucket via the custom domain name.

A maximum of 20 custom domain names can be added on the COS Console. If you need to apply for a higher quota, submit a ticket to contact us.

Procedure

1. Log in to the COS Console. Click Bucket List on the left sidebar to open the Bucket List page.
2. Click the bucket for which you need to set a domain name to go the COS configuration page, as shown below:

3. Click Domain Management on the left, and click Add Domain in the column Custom Origin Domain. If your custom domain name has gone through the filing procedures with MIIT, and resolution has been added on the Domain Name Service, you can enter the custom domain name in the Domain Name input box, and click Save.
Granting the sub-account accelerated domain name configuration permission

Overview

On the domain management and configuration page in COS, you can configure the default accelerated domain name, the custom CDN accelerated domain name, and the custom origin server domain name. Among them, the configuration of the default accelerated domain name and the custom CDN accelerated domain name is logically related to the CDN service. Therefore, if you want a sub-account to be able to configure them, in addition to the COS management permission, you must also grant the sub-account relevant permissions to the CDN service.

To ensure resource security, if you do not grant the sub-account relevant permissions to the CDN service, the sub-account will not have the permission to configure the default accelerated domain name for a COS bucket and the CDN accelerated domain name by default. If an unauthorized sub-account logs in to the COS Console and navigates to the domain management configuration page, an access denied error will be displayed as shown below:

If the sub-account needs to configure such domain names, you need to authorize it in the CAM Console by following the steps below:

Directions

1. As there is no corresponding policy template in the CAM Console, you need to create a custom policy. Go to the Policies page in the CAM Console and select Create Custom Policy > Create by Product Feature or Project Permission to enter the service type configuration page.
The permissions can be configured by a **root account** by default. If you are using a sub-account and want to configure the permissions here, please confirm that the root account has granted you permissions to do so. The user policy that should be authorized by the root account in this case is **QcloudCamFullAccess**.

2. On the service type configuration page, enter your policy name (e.g., COS_DomainAccess) and select the service type as **CDN** as shown below:

3. Click **Next**. You can grant the user permissions to the corresponding feature APIs based on your business needs. Access to and configuration of the default accelerated domain name and CDN accelerated domain name for a COS bucket involve five features, i.e., **querying domain name information, adding domain names, enabling/disabling domain names, deleting domain names, and modifying domain name configuration**. If you want the sub-account to have full access to the configurations of all domain names on the domain name configuration page, please toggle on all of the above features.

4. After selecting the corresponding features, click **Next** to associate objects.

5. Associate the features with objects. Select **Associate an Object > All objects (including new resource objects purchased in the future)**, which has to be selected to make the policy configuration fully effective.

6. Confirm that the permissions are correctly configured and click **Finish** to create the custom policy.

7. After the custom policy is created, switch to the **User List** page and associate the sub-account with the policy.

8. In the **Associate a Policy** pop-up window, search for and select the custom policy you just created and click **OK**.
9. After the policy is associated, the sub-account is authorized and can log in to the COS Console to access and configure the default accelerated domain name and CDN accelerated domain name for a COS bucket
as shown below:

### Default CDN Acceleration Domain

| Status | Off |

Learn more

### Custom Acceleration Domain

<table>
<thead>
<tr>
<th>Domain</th>
<th>Acceleration Region</th>
<th>Origin Type</th>
<th>Origin-pull Authentication</th>
<th>CDN Authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Add Domain

Note: Make sure that the added domain name has been filed and the corresponding CNAME has been set on the DNS provider website.

For more information or help, please refer to Learn more

### Custom Origin Domain

<table>
<thead>
<tr>
<th>Domain</th>
<th>Origin Type</th>
<th>CNAME</th>
<th>State</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Add Domain</td>
</tr>
</tbody>
</table>

Note: This bucket provides service in Mainland China. Please make sure that your domain has been filed. Domain that is not filed cannot be bound to the bucket in Mainland China as a custom domain.

Meanwhile, set corresponding CNAME records on DNS service provider website and route to COS.

For more information or help, please refer to Help of Custom Origin Domain
Setting Bucket Tags

Overview

A bucket tag is a key-value pair (key = value) consisting of the tag’s key, value, and =, such as group = IT. It can be used as an identifier for easier bucket grouping and management. Tags for the specified bucket can be set, queried, and deleted in the console.

Steps

- Up to 10 tags can be added to one bucket, and the tag keys cannot be the same.
- Tag keys and values cannot contain reserved words such as qcs: and project. For more information about restrictions, see Bucket Tag Overview.

Adding a Tag When Creating a Bucket

You can add a bucket tag when creating a bucket, as shown in the figure below:

Adding a Tag to an Existing Bucket

If you do not add a tag when creating a bucket, you can follow the steps below to add one subsequently.
1. On the **Bucket List** page, click the name of the bucket to which to add a tag to enter the bucket configuration page.

2. Click **Basic Configuration**, scroll down to find the **Tag Management** configuration item, and add the bucket tag. See the figure below:

![Tag Management](image)
Setting Cross-region Replication

Overview

When cross-region replication is enabled, new objects in the source bucket can be automatically and asynchronously replicated to the destination bucket in another region. When you manage the objects in the source bucket (such as adding or deleting objects), COS will automatically replicate those operations to the objects in the destination bucket. To enable cross-region replication, you need to make sure that the source and destination buckets are in different regions and both have versioning enabled. You can enable or disable cross-region replication as needed. For more information, please see Cross-region Replication Overview.

Directions

Enabling Cross-Region Replication

1. Log in to the COS Console, click Bucket List in the left sidebar to enter the bucket list page, and click the source bucket to be configured to enter the bucket details page.

2. Click Advanced Configuration on the left to enter the advanced configuration page, scroll down to Cross-region Replication, and click Add Rule to configure a cross-region replication rule.

3. To configure a cross-region replication rule, you need to enable versioning for both the source and destination buckets. If it is disabled in the source bucket, please enable it before configuring the rule.
After completing the configuration, click **OK**.

The options in the cross-region replication rule configuration box are as follows:

- **Source Region**: the region where your source bucket resides.
- **Applied to**: the objects in the source bucket that need to be replicated. If you leave it blank, all the objects in the source bucket will be replicated by default. If a prefix is specified, only objects with this prefix will be replicated. For example, to replicate objects prefixed with `logs/`, enter `logs/`.
- **Resource Path**: the path to your source bucket.
- **Destination Bucket**: Refers to the bucket to which the objects are replicated. The bucket should be in a different region from the source bucket and should be one under the current account in the selected region.
- **Destination Storage Class**: the storage class of the objects after they are replicated to the destination bucket, which is by default the same as that in the source bucket. You can also change the destination storage class. Currently, Standard and IA storage classes are available.

When you finish configuring a rule, you can manage the rule. You can click the button to enable or disable the current rule and click the Edit button to modify the current rule.
If you set to apply the cross-region replication rule to all the objects in the source bucket during configuration, you will not be able to add any other rules; you can modify it by editing the current rule or by adding it again after deleting the current rule.

If you set to apply the cross-region replication rule only to objects with a particular prefix during configuration, you can still modify the scope of the application to all of the contents of the bucket by editing the current rule.

Disabling Cross-Region Replication

You can disable cross-region replication by clicking the Disable button or deleting the rule.

- **Click the Disable button**: you can suspend a rule by clicking its Disable button. By doing so, the cross region replication feature will be suspended. The replicated data will be retained in the destination bucket, and new data added to the source bucket will not be replicated.

- **Delete the rule**: after you delete a rule in Cross-region Replication, the rule will be invalid. The replicated data will be retained in the destination bucket, and new data added to the source bucket will not be replicated. To enable cross-region replication again, you need to configure a rule again.

Ongoing cross-region replication will be stopped when cross-region replication is disabled.

When cross-region replication is enabled again, it will be only applied to objects added after that.
Enabling Global Acceleration

Overview

You can enable global acceleration for your bucket in the COS Console, so that end users around the world can quickly access your bucket, which improves your business access success rate and business stability. For more information on global acceleration, please see Global Acceleration Overview.

Directions

1. Log in to the COS Console, click Bucket List on the left navigation bar, and select the bucket for which you want to configure global acceleration to enter the bucket details page.

   ![Bucket List](image)

2. Click Advanced Configuration on the left to enter the advanced configuration page of the bucket, scroll down to Global Acceleration and click Edit.
3. Click "Enable" and save the change to enable global acceleration for the bucket.

![Global Acceleration](image)

4. After enabling global acceleration, you can quickly access the bucket using a global acceleration domain name in the format of `<BucketName-APPID>.cos.accelerate.myqcloud.com`.

Enabling global acceleration will not affect the existing default bucket domain name. You can still use them.
Object Management
Uploading Objects

Overview

You can upload objects on the **Objects** page of buckets via COS Console. For more information on objects, see **Object Overview**.

Directions

1. **Entering the Objects**

Log in to the **COS Console**. Click **Bucket List**, and select the bucket to store objects to enter the bucket's **Objects** page. Click **Upload Files** and the **Upload Files** window pops up as shown below.

![Image of Upload Files window]

2. **Selecting the Object(s) to Upload**

On the **Upload Files** page, click **Select Files** or **Select Folders** to upload a single or multiple local files/folders. After selecting the objects to upload locally, click **Upload** to upload the objects, or click **Next** to
set the object attributes before uploading (see Step 3).

3. Setting Object Attributes (Optional)

Set the storage class, access permissions, server-side encryption and metadata (optional) for the files to upload, and then click **Upload**. The configuration items are described as follows:

- **Storage Class**
  You can set a storage class for each object based on the use case. The default storage class is COS Standard. For more information on storage classes, see [Storage Classes](#).

- **Access Permissions**
  You can set access permissions for each object as needed. Default is "Inherit Permissions" (inherit permissions from bucket). For more information on access permissions, see [Basic Concepts of Access Control](#).

- **Server-side Encryption**
  You can configure server-side encryption for the objects you want to upload. Tencent Cloud COS will apply data encryption protection to the uploaded objects, so as to automatically encrypt data before it is written, and automatically decrypt the data when you access it. Tencent Cloud COS supports AES-256 encryption of data using the master key. For more information, see [Server-side Encryption Overview](#).

- **Metadata**
  The object metadata, or HTTP Header, is a string sent by the server over HTTP protocol before it sends HTML data to browser. By modifying the HTTP Header, you can change the response form of the page or communicate configuration information, such as modifying the caching time. Modifying an object's HTTP
Header does not modify the object itself. For more information, see Custom Object Headers.

After an object is uploaded successfully, the system automatically refreshes the list to get the latest object information, as shown below.

Some browsers do not support uploading multiple files. It is recommended to use mainstream browsers such as IE10 or above, Firefox, or Chrome.
4. Verifying the Completion of Upload

After clicking **Upload**, you can check the upload progress in **Task completed** in the top right of the page. After the upload is completed, you can see the uploaded object in the **Objects** page of the bucket.

![Example of Task completed and uploaded object]
Overview

You can download existing objects in a bucket in the COS Console. Specifically, you can download a single object in the console or download multiple objects in batches using the COSBrowser tool.

Prerequisites

Before downloading an object, make sure that the object already exists in the bucket. If no objects have been uploaded, upload them first as instructed in Uploading an Object.

Downloading a Single Object

Directions

1. Log in to the COS Console and click Bucket List on the left sidebar to enter the bucket list page.
2. Find the bucket where the object is stored and click the bucket name to enter the bucket management page.

<table>
<thead>
<tr>
<th>Bucket Name</th>
<th>Monitoring</th>
<th>Region</th>
<th>Time Created</th>
</tr>
</thead>
<tbody>
<tr>
<td>examplebucket-1250010001</td>
<td></td>
<td>Chengdu (China) (ap-chengdu)</td>
<td>2019-03-20 15:20:59</td>
</tr>
</tbody>
</table>

3. On the "Objects" tab, find the object you want to download. You can download it in three ways:
   i. Click Download to the right of the selected object to download it.
ii. Select the object and click **Download** in the **More Actions** drop-down list.

![Image of Cloud Object Storage interface](image)

iii. Click **Details** to the right of the object to enter the file details page. Click **Download Object** to download the object. Or, click **Copy Temporary Link**, paste the link into a browser address bar, and press Enter to download the object.

![Image of file details page](image)

- If the bucket where the object is stored is Private Read/Write, a signature will be automatically calculated and added at the end of the address copied here. For more information on how to generate a signature, see **Request Signature**.
- The temporary link with a signature is valid for one hour from the moment you click to view the **Details**. You can refresh the validity period of the signature by clicking **Refresh**.

### Downloading Objects/Folders in Batches
You can only download individual objects in the COS Console. To download multiple objects or folders in batches, it is recommended that you install the COSBrowser client. Here is how to download objects or folders in batches in the console in conjunction with the COSBrowser client.

**Directions**

1. Log in to the COS Console and enter the bucket list page. Find the bucket where the object is stored and click the bucket name to enter the bucket management page.

<table>
<thead>
<tr>
<th>Bucket Name</th>
<th>Monitoring</th>
<th>Region</th>
<th>Time Created</th>
</tr>
</thead>
<tbody>
<tr>
<td>examplebucket-123456789</td>
<td></td>
<td>Chengdu (China) (ap-chengdu)</td>
<td>2019-03-20 15:29:59</td>
</tr>
</tbody>
</table>

2. Select multiple objects and click **Download** in the **More Actions** drop-down list.

   ![Download List](image)

3. Follow the on-screen prompts to install or launch the COSBrowser client and log in.

4. After COSBrowser is launched, the selected files will be automatically added to the download queue and start to download. You can click **Download List** to view them.
## Download List

<table>
<thead>
<tr>
<th>Name</th>
<th>Size</th>
<th>State</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>exampleobject...</td>
<td>13.78KB</td>
<td>Download success, Cost 191ms</td>
<td></td>
</tr>
<tr>
<td>exampleobject...</td>
<td>500KB</td>
<td>Download success, Cost 2s</td>
<td></td>
</tr>
</tbody>
</table>

Selected 0 items, Total 2 items

Items per page 100

[Delete] [Delete All] [Download] [Download Error] [Download Success] [Cancel]
Copying Objects

Overview

You can use the COS Console to copy single or multiple objects uploaded to the bucket from the source path to the destination path.

Copy and paste is not supported for objects in the archive storage class.

Directions

1. Log in to the COS Console and click Bucket List on the left sidebar to enter the bucket list page.
2. Click the name of the desired bucket such as examplebucket-1250000000 to enter its file list page.
3. Select one or more objects or folders you want to copy and click Copy in More.
4. After the system prompts that the copy is successful, you can paste them to the destination path, such as the target folder in the examplebucket1-1250000000 bucket.
The destination path cannot be the same as the source path; otherwise, the paste will fail.

5. After successful paste, you can see that the objects or folders have been copied to the `target` folder.
Viewing Object Information

Last updated: 2019-09-30 11:11:04

Overview

You can check the attributes (such as size and address) and set configurations (object access permission, storage class, etc.) of an object in the COS console.

Directions

1. Log in to the COS Console, click Bucket List to go to the Bucket List page, and then click the bucket of the object.

2. In the File List of the bucket, click Details on the right.

3. By clicking Details, you can check the information such as object size and object address, and get the signature URL. You can also make configurations for the object.
Basic Information

Object Name: exampleobject.txt
Object Size: 500.00KB
Last Modified: 2019-09-29 16:50:00
ETag: "939165e4566ac3e9ba011f641e94c519"
Specified Domain: Default Origin Domain
Object Address: https://examplebucket-1234567890.cos.ap-chengdu.myqcloud.com/exampleobject.txt

Temporary Link:

- Copy Temporary Link
- Download Objects
- Refresh

The temporary link carries the signature parameter, and the temporary link can be used to access the object during the validity period of the signature, and the signature is valid for 1 hour (2019-09-29 17:54:14).

Please take care of your temporary links to avoid leakage, otherwise your objects may be accessed by other users.

Server-Side Encryption

Encryption: None, SSE-COS
Overview

You can search for uploaded objects/folders or objects in uploaded folders. COS supports searching for objects/folders as well as hierarchical folders and their objects in the current bucket.

Searching for Current Objects in a Bucket

Directions

1. Log in to the COS Console and click Bucket List on the left sidebar to enter the bucket list page.
2. Click the bucket in which the objects are stored to enter the bucket management page.
3. Enter an object name prefix in the search box in the top-right corner on the Objects tab and click the Search icon to display the objects or folders with the specified name prefix in the current bucket. To search for a specific object, you can enter a full object key such as exampleobject.txt.

Searching for Objects in Hierarchical Folders

Directions

1. Log in to the COS Console and click Bucket List on the left sidebar to enter the bucket list page.
2. Click the bucket in which the objects are stored to enter the bucket management page.

<table>
<thead>
<tr>
<th>Bucket Name</th>
<th>Monitoring</th>
<th>Region</th>
<th>Time Created</th>
</tr>
</thead>
<tbody>
<tr>
<td>examplebucket-12583235332</td>
<td></td>
<td>Chengdu (China) (ap-chengdu)</td>
<td>2019-03-20 15:29:59</td>
</tr>
</tbody>
</table>

3. Enter the full path to the object (or folder name) and object prefix (full or partial) in the search box in the top-right corner on the **Objects** tab and click the Search icon to display the search results with the **specified object prefix** in the folder.
Direct Upload Archiving

Last updated: 2020-02-26 14:39:26

Currently, there are two archive storage modes: Cloud Archive Storage (CAS) and archive storage in Cloud Object Storage (COS) through lifecycle transition. We will unify those two modes in the future by removing the former and retaining the latter. In addition, we have implemented direct upload archiving in COS, i.e., directly uploading objects to COS in the archive storage class.

You can use the console, API, SDK, or COSCMD tool for direct upload archiving in COS.

- Upload via the console
  After selecting the object to be uploaded through **Upload a File** in the **COS Console**, select the storage
class as **Archive Storage** in the "Set Object Properties" tab.

- **Upload via API**
  Direct upload archiving can be implemented by setting `x-cos-storage-class` to `ARCHIVE` in the PUT Object, POST Object, or Initiate Multipart Upload APIs.

  The Append Object API does not support direct upload archiving.
- **Upload via SDK**
  Currently, all SDKs of COS support direct upload archiving by setting the StorageClass parameter to ARCHIVE during file upload.

- **Upload via COSCMD**
  The COSCMD tool supports direct upload archiving by adding the header field x-cos-storage-class and setting it to ARCHIVE during file upload.

**Archive Storage Restoration and Download**

Downloading the archive storage is different from the standard and standard infrequent access storage. You need to restore it first before you can download it. The restoration can be performed in the following three ways:

- **Expedited mode**: Files below 256 MB can be read in 1 to 5 minutes.
- **Standard mode**: Restoration can be completed generally in 3 to 5 hours.
- **Batch mode**: Data can be retrieved generally in 5 to 12 hours with the lowest cost.

In addition, the console, API, SDK, and COSCMD tool all support archive storage restoration and download.

**Current Constraints for Direct Upload Archiving**

- If you want to download an archive storage object, you need to restore it first.
- If you want to replicate an archive storage object, you need to restore it first.
- Archive storage objects cannot be replicated across regions.
- Archive storage objects cannot be converted to standard or standard infrequent access storage.
Modifying Storage Class

Overview

You can modify the storage class of uploaded objects in the COS Console at any time to meet your business needs in different scenarios. COS provides standard storage, standard infrequent access storage and archive storage. The following section will guide you through how to modify the storage class of an object.

If an object is stored in the **archive storage** class, you need to restore it to standard storage before you can modify its storage class.

Steps

1. Log in to the **COS Console**.
2. In the left sidebar, click **Bucket List**.
3. Click the bucket name to enter the bucket where the object is stored.

4. In the "File List" module of the bucket, click **Details** in the "Action" column to the right of the object for which you want to set the storage class.
5. Scroll down, find the **Storage Class** configuration item, and select the desired storage class.

![Storage Type](image.png)

Standard Storage is for high-frequency, high-performance data access and without minimal storage time constraints and data retrieval costs. Learn more

6. Click **Save** to modify the storage class of the object.
Deleting File Fragments

Introduction

If you try to delete the specified bucket but the system prompts that "Deletion failed. Please delete the valid data in the bucket first", you can enter Incomplete Multipart Uploads to view the files that have not been completely uploaded and delete them. The bucket can be deleted only after you confirm that all completely and partially uploaded files have been deleted from the bucket.

- During the object upload progress, the files that are paused or canceled will be displayed in Incomplete Multipart Uploads. Files can be viewed in Objects Only after they are completely uploaded.
- Multipart uploads and normal objects will occupy storage space, so it will produce storage capacity cost.

Delete multipart uploads manually

1. Log in to the COS Console And click Bucket List in the left sidebar to enter the bucket list page.
2. Click the bucket you want to delete to enter the bucket details page.
3. On the Objects Page, select the Multipart Upload Tab to view the files that have not been completely uploaded.
4. You can click .setRegion(region) To the right of an incomplete multipart upload to delete it or click Clear Incomplete Multipart Uploads At the top to delete all incomplete multipart uploads.
5. After you perform the "Clear Incomplete Multipart Uploads" or "Delete" operation, the list will be empty.

Configure lifecycle to clean up multipart uploads regularly

1. Log in to the COS Console And click Bucket List in the left sidebar to enter the bucket list page.
2. Click the bucket you want to delete to enter the bucket details page.
3. Click Advanced configuration in the menu on the left, and then go down to the Lifecycle configuration item.
4. Click "add Rule", and the configuration information is shown in the following figure. The rule here is set to be deleted 7 days after incomplete multipart uploads is created under the entire Bucket scope.
5. Click "OK" to see the lifecycle rules that have been successfully set in the console.
Setting Object Access Permission

Overview

COS allows you to configure access permissions for objects, which have a higher priority than that for buckets.

- The object access permission is valid only when the user accesses via the default domain name. When the access is made via a CDN accelerated domain name or custom domain name, the bucket access permission takes priority.
- For more information, see Specifications and Limits.

Steps

1. Log into the COS Console and click Bucket List in the left sidebar to enter the bucket list page.
2. Find the bucket for which you need to configure object access permissions, click its bucket name to enter the details page.
3. In [File List], find the object whose permission needs to be configured, and click [Details] on the right to enter the file details page (If it is a folder, click [Permissions] on the right).
4. Click the [Object Permissions] configuration item above, and configure access permissions based on actual needs (such as granting sub-account object permissions, sub-account ID can be found in Cloud Access Management Console). COS supports two types of permissions for objects:
- **Public Permissions**: Inherited permission, private read/write, and public read/private write. For more information on public permissions, see [Access Permission Types](#).

- **User Permissions**: The root account has all object permissions (full access) by default. In addition, COS allows you to grant sub-accounts data read/write, permission read/write, and even **full access** permissions.

![Object ACL (Access Control List)](image)

5. Click [Save] to configure the object access permissions.

6. If you need to configure or modify access permissions for multiple objects in batches, you can check multiple objects and select [Modify Access Permissions] under [More Actions].
Setting Object Encryption

Overview

You can encrypt the objects stored in buckets on COS console to prevent data leakage. For more information on encryption, see Server-side Encryption Overview. The following shows you how to configure object encryption:

- This operation does not support configuring encryption for objects of archive type. If encryption is needed, restoring archived objects first. After the restoration is complete, modify the storage type to standard or low frequency before configuring the encryption.
- As long as you have access permissions to objects, the way you access encrypted and non-encrypted objects has no difference.
- Server encryption only encrypts object data, not its metadata. Objects using server encryption can only be accessed with a valid signature, not by anonymous users.
- When you list the objects in a bucket, all objects will be listed, no matter whether they are encrypted.

Steps

1. Log into the COS Console.
2. In the left sidebar, click Bucket List.
3. Select the bucket to which a bucket policy will be added to enter the details page.
4. In **File List**, click **Details** to the right of the object you want to encrypt.

5. Scroll down to find the [Server-Side Encryption] configuration item and select the corresponding encryption method. Currently, two encryption methods are supported:
   - SSE-COS: Server-side encryption with a key managed by COS. For more information on SSE-COS encryption, see [SSE-COS Encryption](#).
   - SSE-KMS: Server-side encryption with a key managed by Tencent Cloud Key Management System (KMS). You can use the default key or create a key. For more information on keys, see [Create KMS Key](#). For more information on SSE-KMS, see [SSE-KMS Encryption](#).

6. Click **Save**.

7. If you need to configure encryption for multiple objects in batches, you can check multiple objects, and then select [Modify Encryption Method] under [More Actions].

- If you use SSE-KMS encryption for the first time, you need to **enable KMS service**.
- Currently, SSE-KMS encryption only supports Beijing, Shanghai, and Guangzhou regions.
Custom Headers

Last updated: 2019-10-12 16:31:49

Overview

The HTTP header of an object is a string sent by the server over HTTP protocol before it sends HTML data to browser. By modifying the HTTP header, you can change the response form of the page or communicate configuration information, such as modifying the caching time. Modifying an object's HTTP header does not modify the object itself.

For example, if the Content-Encoding in Header is modified to gzip, but the file itself has not been compressed to .gz file in advance, a decoding error will occur.

Configuration Steps

1. Log in to the COS Console, and select Bucket List from the left side bar to access the Bucket List page. Click the bucket (such as example) you want to configure origin-pull for and enter the bucket.

2. Locate the object you want to set header for (such as example.exe), and click More on the right side of object, then click Set Header to pop up the head setting dialog box.

3. Click +Add Parameter, then choose the type of parameter you want to set (enter the custom name for custom content), enter the corresponding value and click OK to save. COS provides six object HTTP header identifiers for configuration:

<table>
<thead>
<tr>
<th>HTTP Header</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### HTTP Header

<table>
<thead>
<tr>
<th>HTTP Header</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content-Type</td>
<td>MIME information of file</td>
<td>text/html</td>
</tr>
<tr>
<td>Cache-Control</td>
<td>Caching mechanism of file</td>
<td>no-cache;max-age=200</td>
</tr>
<tr>
<td>Content-Disposition</td>
<td>Extension of MIME protocol</td>
<td>attachment; filename=&quot;fname.ext&quot;</td>
</tr>
<tr>
<td>Content-Encoding</td>
<td>Encoding format of file</td>
<td>UTF-8</td>
</tr>
<tr>
<td>Expires</td>
<td>The expiration date used to control the cache</td>
<td>Wed, 21 Oct 2015 07:28:00 GMT</td>
</tr>
<tr>
<td>x-cos-meta-[custom content]</td>
<td>Custom content</td>
<td>Custom content</td>
</tr>
</tbody>
</table>

#### Custom headers

<table>
<thead>
<tr>
<th>Parameter</th>
<th>value</th>
<th>Actions</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content-Type</td>
<td>text/plain; charset=8</td>
<td>Edit</td>
<td>Delete</td>
</tr>
</tbody>
</table>

---

### Example

Under APPID 12500000000, a bucket named "examplebucket" is created. The object example.txt is uploaded under the bucket root directory.

If you do not customize the HTTP header for the object, the browser or client will get the following Object headers during download:

#### request

```
GET /exampleobject.txt HTTP/1.1
Host: examplebucket-1250000000.file.myqcloud.com
Accept: */*
```
Cloud Object Storage

response

HTTP/1.1 200 OK
Content-Type: text/plain
Content-Disposition: attachment; filename="UTF-8''example.txt"
Access-Control-Allow-Origin: *
Last-Modified: Tue, 11 Jul 2017 15:30:35 GMT

Add the following configurations:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>value</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cache-Control</td>
<td>no-cache</td>
<td></td>
</tr>
<tr>
<td>Content-Disposition</td>
<td>attachment filename=&quot;abc.txt&quot;</td>
<td></td>
</tr>
<tr>
<td>Content-Type</td>
<td>image/jpeg</td>
<td></td>
</tr>
<tr>
<td>x-cos-meta-md5</td>
<td>1234</td>
<td></td>
</tr>
</tbody>
</table>

When you send a request again, the browser or the client will get the following object headers:

request

GET /exampleobject.txt HTTP/1.1
Host: examplebucket-1250000000.file.myqcloud.com
Accept: */*

response

HTTP/1.1 200 OK
Cache-Control: no-cache
Content-Type: image/jpeg
Content-Disposition: attachment; filename="abc.txt"
x-cos-meta-md5: 1234
Access-Control-Allow-Origin: *
Last-Modified: Tue, 11 Jul 2017 15:30:35 GMT
Deleting Objects

Overview

You can delete a single object or multiple objects uploaded to a bucket via the COS Console.

Deleting a Single Object

Procedure

1. Log in to the COS Console, enter the appropriate bucket, then select the object to be deleted, and click **Delete**. The **Delete File** dialog box pops up.

2. Click **OK** to delete the object.

Deleting Multiple Objects

Procedure

1. Select the objects to be deleted in the COS Console, and click **Delete in Batch**. The **Delete File** dialog box pops up.
2. Click **OK** to delete the objects in batch.
Restoring Archived Objects

Overview

Archived objects can be restored in the COS Console, so that they can be accessed or manipulated. For more information about object storage classes, see Object Overview.

The restoration operation will create a replica of the object in standard storage class, which can be read and downloaded. The object replica will be billed as a standard storage object. For pricing details, see Product Pricing.

Directions

1. Log in to the COS Console and click Bucket List in the left sidebar to enter the bucket list page.

2. Click the bucket name to enter the bucket details page.

3. In the "File List" module on the bucket details page, click Restore in the "Action" column to the right of the object you want to restore.

4. In the dialog box for restoring the archived object, configure the restoration mode and the validity period in days of the replica. The related configuration items are detailed below.

   Restoration Mode: Standard, Expedited, or Batch mode.
- Expedited mode: This is the fastest way of restoration. Files below 256 MB can be restored in 1 to 5 minutes. When you need to access the archival data urgently under certain circumstances, using this mode can greatly reduce the time required and increase the efficiency.
- Standard mode: Restoration can be completed generally in 3 to 5 hours.
- Batch mode: If your need for the archival data is not urgent, this mode can help retrieve massive amounts of data generally in 5 to 12 hours with the lowest cost.

**Replica Validity Period:** Set in how many days the replica should automatically expire and be deleted. The value range is 1 to 365 days. After the object is successfully restored, you can click **Restore** again to change the validity period of the replica in the pop-up window. See the figure below:

![Restore Archived Objects](image)

5. Click **OK** after the configuration items are set, and the object restoration will start. You can click **Details** to enter the object details page and check whether the restoration has been completed.
6. After confirming that the object has been successfully restored, you can click **Restore** again to modify the validity period of its replica.
7. Enter the object details page where you can access, download, and do more with the object.

<table>
<thead>
<tr>
<th>Basic Information</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Object Name</strong></td>
<td>exampleobject.zip</td>
</tr>
<tr>
<td><strong>Object Size</strong></td>
<td>13.78KB</td>
</tr>
<tr>
<td><strong>Storage Class</strong></td>
<td>Archive Storage</td>
</tr>
<tr>
<td><strong>Last Modified</strong></td>
<td>2019-03-21 12:05:51</td>
</tr>
<tr>
<td><strong>ETag</strong></td>
<td>&quot;7007e843b054a06baeb2c57a257473e48&quot;</td>
</tr>
<tr>
<td><strong>Specified Domain</strong></td>
<td>Default Origin Domain</td>
</tr>
<tr>
<td><strong>Object Address</strong></td>
<td><a href="https://examplebucket-1234.cos.ap-chengdu.myqcloud.com/exampleobject.zip">https://examplebucket-1234.cos.ap-chengdu.myqcloud.com/exampleobject.zip</a></td>
</tr>
<tr>
<td><strong>Temporary Link</strong></td>
<td><img src="#" alt="Temporary Link" /></td>
</tr>
</tbody>
</table>

The temporary link carries the signature parameter, and the temporary link can be used to access the object during the validity period of the signature, and the signature is valid for 1 hour (2019-09-29 16:19:13). Please take care of your temporary links to avoid leakage, otherwise your objects may be accessed by other users.
Folder Management
Creating Folder

Overview

In COS that comes with no folders, objects are stored in a flat structure. To make it easier for you to get started, objects named by using "/" as suffix in the object key can be used as "folders". In fact, the storage space of a "folder" in COS is 0.

**Note:**
The folder name is limited to 255 characters, and the reserved characters and fields are not supported as follows:

- Reserved characters: [con], [aux], [null], [prn], [com0], [com1], [com2], [com3], [com4], [com5], [com6], [com7], [com8], [com9], >[lpt0], [lpt1], [lpt2], [lpt3], [lpt4], [lpt5], [lpt6], [lpt7], [lpt8], and [lpt9].
- Reserved ASCII control characters:
  - Up (↑): CAN (24)
  - Down (↓): EM (25)
  - Right (→): SUB (26)
  - Left (←): ESC (27)

Steps

1. Log in to the COS console, and select **Bucket List** from the left side bar to enter the Bucket List page. Click the bucket you want to create folder and enter the bucket.
2. Click **Create folder** and the **Create new folder** dialog box pops up.

3. Enter the folder name and click **OK** to save it. Naming Rules for Folders are as follows:
   - A combination of numbers, letters and visible characters is supported.
   - A folder cannot begin with `/` and does not allow two or more consecutive `/`.
   - A subdirectory can be created quickly by separating the path by `/`.
   - The folder name cannot be empty.
   - Do not use `..` as the folder name.

Note:
Folders do not support renaming, please note the naming.
Deleting Folders

Overview

You can delete a created folder in the COS Console.

Deleting a folder in the console will delete the folder and all objects in it. Please do so with caution.

Directions

1. Log in to the COS Console and click Bucket List on the left sidebar to enter the bucket list page.
2. Click the bucket in which you want to delete the folder to enter the bucket management page.
3. On the "Objects" tab, click Delete in the Action column to the right of the folder to be deleted.
4. A confirmation window will pop up.

5. Click **OK** to delete the folder.
View Folder Details

Last updated: 2019-09-30 11:14:50

Overview

In the COS Console, you can view the details of folders that have been created, including the number and size of objects in the current folder. This document describes how to view folder details.

COS stores objects in a flat structure with no traditional folder concept. In order to make COS customary, we turn an object into a "folder" by suffixing it with / in its key. In fact, a "folder" in COS is an object with a storage capacity of 0 KB.

Directions

1. Log in to the COS Console and click Bucket List in the left sidebar to enter the bucket list page.
2. Locate the bucket that includes the folder you want to view and click the bucket name.

3. Click Details in the Action column to the right of the folder you want to view.
4. You can view the statistics regarding the folder, including the total number and the size of objects in it.

Example 1. If a folder contains 1 empty folder and 5 objects, then the total number of objects in the folder will be 6.

Example 2. If a folder contains 1 folder (containing 2 objects) and 5 objects, then the total number of objects in the folder will be 8.
Setting Folder Permissions

Last updated : 2020-03-25 18:11:57

Overview

You can set access permissions of folders in the COS Console, so that specified users can perform specified operations on the contents of the folders. You are recommended to follow the principle of least privilege when configuring permissions to protect your data assets.

COS stores objects in a flat structure with no traditional folder concept. In order to make COS customary, we turn an object into a "folder" by suffixing it with / in its key. In fact, a "folder" in COS is an object with a storage capacity of 0 KB.

The folder permission is essentially an access permission at the object level, which takes precedence over the bucket access permission. COS supports the following two types of object permissions:

- Public permissions: inherited permission, private read/write, and public read/private write. For more information on public permissions, please see Access Permission Types.
- User permissions: the root account has all the permissions of the object by default (i.e., full access). In COS, sub-accounts can be added to read/write data, read/write permissions, and have the full access.

Directions

1. Log in to the COS Console and click Bucket List on the left sidebar to enter the bucket list page.
2. Find the bucket where a folder is located and click the bucket name to enter the bucket management page.
3. On the "File List" tab, click Set Permission in the "Operation" column to the right of the folder for which to set permission.
4. You can set folder permissions based on your business needs as detailed below:

<table>
<thead>
<tr>
<th>Permission Type</th>
<th>Configuration Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public permissions</td>
<td>Inherited permissions</td>
<td>Same as the bucket permission by default.</td>
</tr>
<tr>
<td></td>
<td>Private read/write</td>
<td>Only the root account can read/write, while non-root accounts (sub-accounts, other users' root accounts, or anonymous users) cannot access this folder.</td>
</tr>
<tr>
<td></td>
<td>Public read/private write</td>
<td>The root account can read/write, while non-root accounts (sub-accounts, other users' root accounts, or anonymous users) can only read the contents of the folder but not write new data into it.</td>
</tr>
<tr>
<td></td>
<td>Public read/write</td>
<td>Both the root account and non-root accounts (sub-accounts, other users' root accounts, or anonymous users) can read/write.</td>
</tr>
<tr>
<td>User permissions</td>
<td>User type</td>
<td>A root account refers to the root account ID of other user accounts, while a sub-account refers to the sub-account under the currently used root account. If you want sub-accounts under another root account to have access permissions, you must grant access permissions to that root accounts first, so that it can grant access permissions to its own sub-accounts.</td>
</tr>
<tr>
<td></td>
<td>Data read</td>
<td>Permission to read data.</td>
</tr>
<tr>
<td></td>
<td>Data write</td>
<td>Permission to write data.</td>
</tr>
<tr>
<td></td>
<td>Permission read</td>
<td>Permission to read folder permission configuration. If this permission is granted, authorized users can get details of folder permission configuration.</td>
</tr>
<tr>
<td></td>
<td>Permission write</td>
<td>Permission to modify folder permission configuration. If this permission is granted, authorized users can modify the details of folder permission configuration. <strong>This configuration will cause permission change. Please select it with caution.</strong></td>
</tr>
<tr>
<td></td>
<td>Full access</td>
<td>Including four permissions: data read, data write, permission read, and permission write. <strong>This configuration grants a wide range of permissions. Please select it with caution.</strong></td>
</tr>
</tbody>
</table>
5. After setting the permission, click **Save** on the right.
Data Extraction

Overview

COS Select allows you to filter out desired data at the storage level, significantly reducing the amount of data transferred by COS, thereby lowering your usage costs, and improving data acquisition efficiency. In COS Console, you can extract the content of individual files stored in buckets using standard SQL templates we provide or by entering statements that meet syntax rules.

- COS Select currently only supports objects in json and csv file formats, and public cloud regions in mainland China.
- Please make sure the file to be extracted complies with the specification of COS Select. For more information on the specification of COS Select, see SELECT Overview.
- COS Select in the console supports data extraction of up to 40M for 128MB files. If you need to process larger files or extract more data, please use API or SDK.

Steps

1. Log into the COS Console.
2. In the left sidebar, click Bucket List.
3. Click the bucket name to enter the bucket where the object is stored.
4. In the "File List" module of the bucket, locate the object to be extracted and click Extract in the right-side "Operation" column.
5. Enter the extract object content page in the console, select the type, header field, separator, and compression format of the file to be extracted.

6. Click **Select an SQL Template**, select the desired template statement, and click **OK**.

7. Edit the statement in the text box based on the actual file and click **Run SQL**.
8. After the process is finished, you can view the first 100 results in the text box at the bottom. To obtain complete data, click **Export**.
Batch Operation

Overview

The batch operation feature of COS allows you to implement large-scale batch operations on objects in the bucket. Currently, you can perform the following batch operations:

- Replicating Objects
- Restoring an archived object

You can put objects to be operated on in an inventory file, which is based on the inventory report generated by the inventory feature (you need to enable Inventory feature first), or you can create one in the specified format. COS batch operation will operate on the objects in batches based on this inventory file. For more information, see Overview.

Steps

1. Log into the COS Console and click Batch Operation on the left sidebar to enter the batch operation management page.

2. Click Create Job to start creating a batch operation job. Configuration items are described as follows.

   - **Job Region**: Select a region for the job to be created. The job region should be the same as the bucket region of the objects to be operated on in your inventory file, otherwise the job will fail. *Chengdu and Chongqing regions are currently in beta test.*

   - **Inventory Format**: Select a format for the inventory objects. There are two formats:

     | Inventory Format       | Field | Configuration Instructions                                           |
     |------------------------|-------|---------------------------------------------------------------------|
     | COS inventory report   |       | Please select this if the inventory file comes from an inventory report generated by the inventory feature |
     | CSV                    | Ignore| Placeholder field, which can be used when your inventory file contains irregular fields |
     |                        |       | Bucket name                                                         |
     |                        |       | Key Name of an object in a bucket. If CSV file format is used, the object name is URL-encoded and must be decoded before use |

*Last updated: 2020-03-17 17:27:04*
Object version ID. If versioning is enabled for the bucket, COS assigns a version number to the objects added to the bucket. If you do not want to use the latest object version, you can select a version ID that contains the inventory object.

- **Inventory Bucket**: Select the bucket where the inventory is stored.

- **Inventory File Path**: Enter the inventory file or CSV file path in the format of `directory/manifest.json` or `directory/manifest.csv`, respectively. For example, if you have an inventory stored in the `examplebucket-1250000000` root directory, the inventory path will be `manifest.json`.

3. Click **Next** and the inventory Etag will be displayed, meaning you have selected the correct inventory objects. Then, you will enter the operation configuration page.

- **Replicating data in batch**:
  - Destination Bucket: Select the bucket to store the replicas of objects in the inventory list.
  - Storage Type: Standard or Standard_IA.
  - Server Encryption: Select whether to encrypt the object replicas. Options include no encryption or SSE-COS encryption.
  - Access Permissions: Configure access permissions for the object replicas. Options include using permissions of the destination bucket, private read/write, and public read/private write.
- Object Metadata: Configure metadata for the object replicas. Options include copying the original metadata or replacing all metadata.
  
  **Restoring archived storage in batch**
  
  - Restoration Mode: Standard mode and batch mode. For more information on restoration mode, see [Restoring Archived Objects](#).
  
  - Replica Validity Period: Configure the number of days after which the copy will expire and be deleted automatically. The configuration range has a minimum of 1 day and a maximum of 365 days.

4. Click **Next** to enter the "Other Configurations" page where you can configure the following items:

  - **Job Description (Optional)**: Description of the job, which is optional.
  
  - **Job Priority**: A job of a higher priority will be operated on first. The value can be a positive integer. The greater the value, the higher the priority.
  
  - **Job Report**: Select whether to generate a job report.
CAM Role: You can create a CAM role or select an existing one to grant operation permissions to COS. To grant batch operation permissions to COS, you need to create a CAM role. For more information on CAM roles, see Role Overview.

5. Click Next to enter the information check page where you can check the configurations of your batch operation job. If you need to make a change, click the corresponding Modify or Previous. Click OK if
everything is correct.

6. After the batch operation job is created, find the newly created job in the job list and click [OK]. To cancel the job, click [Cancel] on the right.
Overview

COS can monitor stored data. In the monitor window, you can find details and trends of various metrics, including basic information such as number of requests, traffic, and data reads as well as statistics on return codes.

Directions

Querying with a Root Account

1. Log in to the COS Console and click Bucket List in the left sidebar to enter the bucket list page.

2. Find the bucket whose statistics you want to view and click in the Monitor column as shown below:

<table>
<thead>
<tr>
<th>Bucket Name</th>
<th>Monitoring</th>
<th>Region</th>
</tr>
</thead>
<tbody>
<tr>
<td>examplebucket-125</td>
<td></td>
<td>Chengdu (China) (ap-chengdu)</td>
</tr>
</tbody>
</table>
3. Enter the monitoring page as shown below:
In the **Current** section, you can switch between current data and data of this month, including storage capacity, number of read and write requests, traffic, return codes, and data reads. The time granularities available include today, yesterday, last 7 days, and last 30 days.

In the **This Month** section, you can view data for the month, including the daily average storage capacity of each storage class and total traffic (accumulated public network traffic, accumulated CDN origin-pull traffic, and accumulated cross-region replication traffic).

### Querying with a Sub-account

To query monitoring reports with a sub-account, you need to first grant the sub-account permission to do so. You can grant the permission using a policy template or a custom access policy.

#### Granting a Sub-account Permission to Access Monitoring Reports

**Configuring with a Policy Template**

1. Log in to the [CAM Console](https://console.cloud.tencent.com) using the root account, click **Users** in the left sidebar, and click a sub-account.

2. Select the [QcloudMonitorFullAccess](https://console.cloud.tencent.com) policy in the policy list and click OK to add it to the sub-account. Then the sub-account should be able to access monitoring reports.
This policy template will grant a sub-account full access to Cloud Monitor. For more account security, you can customize an access policy to grant Read access to your sub-accounts.

**Configuring with a Custom Access Policy**

1. Log in to the CAM Console using the root account and select **Policies > Create a Custom Policy**.
2. Click **Create by Policy Syntax**.

![Select a method to create policy](image)

- **Create by policy generator**: Select services and operations from the list to automatically generate policy syntax.
- **Create by Policy Syntax**: Compile policy syntax to create related policy.
- **Authorize by tag**: Resources that have certain type of tag attribute are quickly authorized to users and user groups.

3. Use the blank template to create a new policy.

![Select policy template](image)

- **Select policy template**: Choose a policy type.
- **Edit Policy**: Edit the selected policy.

4. Copy and paste the following policy syntax into the **Edit Policy Content** input box in the blank template. You can rename the policy as needed.

**Policy syntax:**

```
{  
  "version": "2.0",  
  "statement": [  
    {  
      "effect": "allow",  
      "action": [  
        "monitor:GetMonitorData"  
      ],  
      "resource": "*"  
    }  
  ]  
}

Edit the policy content in the input box:

```json
{
  "version": "2.0",
  "statement": [
    {
      "effect": "allow",
      "action": ["monitor:GetMonitorData"],
      "resource": "*"
    }
  ]
}
```
5. Click **Create a Policy**. After the policy is created successfully, you can associate it with a sub-account. For directions, see **Configuring by Policy Template**.
Picture Processing

Turn on image processing

Last updated: 2020-03-25 15:56:39

Note

This article describes how to use the image processing capabilities of COS through the console. You can use the image processing feature in two ways. For instructions on image processing, see [Overview of picture processing](#).

- **By adding parameters to the picture URL** You can process the image by adding the appropriate parameters after the object address (URL) of the image.
- **Use picture styles** You can save different processing effects by creating styles, and then use styles to deal with the picture uniformly. The style set here is a template for real-time processing parameters when the picture is downloaded.

The image processing function only supports the public cloud region of Mainland China, China.

The image processing function is a charge item, which is collected by data Vientiane. For detailed billing instructions, please see data Vientiane. [Billing and pricing](#).

Add URL parameter

1. Login [Cloud Object Storage console](#).
2. Find the Bucket where the picture is located, click its storage name, and go to the Bucket management page.
3. Under the operation bar on the right side of the picture file, click "details" to enter the file details page.
4. Copy [object address] and paste it into the browser window address bar.

To deal with pictures, you need to write Permission with objects. For more information about the settings of object Permission, please see [Setting Object Access Permission](#).

5. In the address bar, add the appropriate parameters after the object address in the following format.

   Object address? Processing interface name / processing operation name / processing parameters.

   For more image processing parameters and instructions, see [Basic picture processing of data Vientiane](#) API Documentation.
If Access Permission of the picture file is privately read, you need to add image processing parameters to the signed address.

**Example: zoom the width and height of the picture to 50% of the original image**
Assuming that the effect of the original image is as follows, Access and Permission of the object are public read and private write, and the object address URL is `https://examplebucket-1250000000.cos.ap-chengdu.myqcloud.com/sample.jpeg`.

Then add the following parameters to the URL link:

- Zoom processing interface: imageMogr2
- Zoom operation name: thumbnail
- Processing parameters: ! 50p

The address after adding the parameter is: `https://examplebucket-1250000000.cos.ap-chengdu.myqcloud.com/sample.jpeg?imageMogr2/thumbnail/!50p`  Paste this address into the address bar and
enter, and you can see the zoomed effect as follows.

Use picture styles

The picture style function can help you to present different processing operation parameters in the form of a template and uniformly process the picture through the style. The style set here is a template that is combined for real-time processing parameters when the picture is downloaded. The following is to **Set the style that limits the picture to 480px wide and high 270px**. As an example, describe how to:

1. Login Cloud Object Storage console.
2. Find the Bucket where the picture is located, click its storage name, and go to the Bucket management page.
3. In the left menu bar, click "Image processing" to enter **Style management** page.
   - **Separator** The style delimiter is the symbol that separates the file name and the processing style, including an underscore (_), an underscore (_), a slash (/), and an exclamation point (!). Select the exclamation point (!) here and save it.
4. Click [add style] to enter **New style** Page, the configuration information is as follows:
   - **Style Nam** Enter a custom style name, as an example here: yunstyle.
     - The style name needs to be case-sensitive and cannot be modified after saving.
     - To avoid ambiguity, the currently enabled interval marker must not appear in the processing style name.
     - **Edit mode** Select a basic editor.
   - Thumbnail mode: select zoom only.
   - Zoom selection: select to limit the width and height scale.
   - Thumbnail size: 480px wide, high 270px.
Progressive display: if turned on, Access pictures are displayed in a progressive way. Saving here is not enabled by default.

Output format: optional image output format, which keeps the default original image here.

5. After the configuration information is complete, you can click the preview button on the right to view the preview effect.

6. After the preview is correct, click "Save", and you can see that a picture style named yunstyle has been added.

- A maximum of 100 styles can be set under the same Bucket.
- The average effective time is 30 minutes.
- To change the delimiter, you need to clear the cache. It takes at least 24 hours for entire network to take effect.
- Canceling the used delimiter may result in Features exception.
- For more information about picture styles, see Style setting.

vii. Go to the object details page, copy the object address and add a delimiter and style name after the object address in the following format.

Object address + delimiter + processing style name

The final object address is: https://examplebucket-1250000000.cos.ap-chengdu.myqcloud.com/sample.jpeg!yunstyle Paste this address into the address bar and enter, and you can see the zoomed effect as follows.