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
Data Extraction
Batch Operation
Monitoring Reports
  Querying Monitoring Reports
# 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.

A maximum of 200 buckets can be created under a single account regardless of region.

Directions

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

3. In the Create Bucket dialog box, configure the information as follows:
   - **Name**: Enter a custom bucket name, which is non-modifiable once being configured. For information on naming, see Naming Conventions.
   - **Region**: Select the COS region where your business is operated mostly or most of your users reside. It is non-modifiable once being configured. For more information on regions, see Regions and Endpoints.
   - **Access Permission**: Three access permissions for buckets are available by default: "Private Read/Write", "Public Read/Private Write" and "Public Read/Write". The permission is modifiable after being configured. For more information, see Bucket Access Permissions.
   - **Bucket Tag**: Bucket tags are used to identify and group buckets for an easier management. For more information, see Setting Bucket Tags.
4. Verify that all the information entered is correct, and then click **OK** to create a bucket. In the Bucket List page, you can see the bucket you just created.
Deleting Buckets

Last updated: 2019-09-20 18:52:43

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.

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</th>
<th>Region</th>
</tr>
</thead>
<tbody>
<tr>
<td>eu-frankfurt-12567</td>
<td>None</td>
<td>Frankfurt, German federal state (Europe) (eu-frankfurt)</td>
</tr>
<tr>
<td>examplebucket-12567</td>
<td>None</td>
<td>Chengdu, China (ap-chengdu)</td>
</tr>
<tr>
<td>examplebucket-oversea</td>
<td>None</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

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-125###</td>
<td></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 Form]

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’s.

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

Last updated: 2019-11-01 16:43:25

Overview

You can set origin-pull rules for buckets through the COS Console. When the object you requested does not exist in the bucket, or a specific request needs to be redirected, you can set the origin-pull rules to access corresponding data from COS. Origin-pull settings are mainly used for live migration of data and redirection of specific requests. You can set them as needed.

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

Procedure

1. Log in to the COS Console, select Bucket List from the left sidebar to go to the Bucket List page. Click the bucket for which you want to set the origin-pull.
2. Click **Basic Configuration** to locate the origin-pull settings, change the status to **Enabled**, enter the origin server address, and click **Save**. The configuration items are as follows:

**Origin server address**: Only enter the domain name or IP address without **http://** or **https://**. You can also add the port number after the domain name or IP address. Example of a correct address:

<table>
<thead>
<tr>
<th>Origin server address</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>abc.example.com</td>
<td></td>
</tr>
<tr>
<td>abc.example.com:8080</td>
<td></td>
</tr>
<tr>
<td>10.10.10.10</td>
<td></td>
</tr>
<tr>
<td>10.10.10.10:8080</td>
<td></td>
</tr>
</tbody>
</table>

**Example**

**Background**
A user with APPID of 1250000000 created a bucket named "examplebucket-1250000000", and enabled the CDN accelerated domain name:

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

Set the origin server address for the bucket to:

```
abc.example.com
```

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

**The first 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
```

Then the origin server provides the object to the client to ensure the 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 object picture.jpg in the root directory and returns it to the client.
Setting Cross-Origin Access

Last updated: 2019-09-17 15:20:28

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.

   ![Bucket List](image)

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

   ![Add Rule](image)

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-125666666</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](image-url)

### Static website hosting

- **Status**: [On/Off]
- **Endpoint**: https://examplebucket-1250cos-website.ap-chengdu.myqcloud.com
- **Force HTTPS**: [On/Off]

*Do not enable this option if you have set up a CDN domain name back to the website endpoint and use the HTTP protocol (non-encrypted) to access the CDN.*

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

### Redirect rules

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

[Save] [Cancel]
4. After completing the configuration, click **Save**.

<table>
<thead>
<tr>
<th>Static website hosting</th>
<th>Edit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>On</td>
</tr>
<tr>
<td>Endpoint</td>
<td><a href="https://examplebucket-123.coswebsite.ap-chengdu.myqcloud.com">https://examplebucket-123.coswebsite.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>Type</td>
</tr>
<tr>
<td></td>
<td>No data to display</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.

```
Bucket Name                      Monitoring          Region                        Time Created
examplebucket-12566789          -                   Chengdu (China) (ap-chengdu) 2019-03-20 15:29:59
```

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

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.
6. 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_url)

*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.*
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.

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 Table](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.

   ![Create User](image)

   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.

   ![Associate Policies](image)
3. You can view the added policies here. When you no longer need a policy, you can unbind it.
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.
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

Last updated: 2019-08-29 11:21:16

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

Last updated: 2019-09-30 17:49:40

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:

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:

<table>
<thead>
<tr>
<th>Default CDN Acceleration Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Status</strong></td>
</tr>
<tr>
<td><strong>Acceleration domain</strong></td>
</tr>
<tr>
<td><strong>Acceleration Region</strong></td>
</tr>
<tr>
<td><strong>Origin Type</strong></td>
</tr>
<tr>
<td><strong>Origin Domain</strong></td>
</tr>
<tr>
<td><strong>Origin-pull Authentication</strong></td>
</tr>
<tr>
<td><strong>CDN authentication</strong></td>
</tr>
</tbody>
</table>

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

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**

<table>
<thead>
<tr>
<th>Status</th>
<th>Edit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Off</td>
<td></td>
</tr>
</tbody>
</table>

**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

Last updated: 2019-12-20 15:47:24

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)

   - **Tag Management**
     - Tag Key
     - Tag Value
     - Actions
     - Add Tags
   - Help of Tag Management [?]

   See the figure below:
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.

2. Click Basic Configuration on the left to enter the basic configuration page of the bucket, scroll down to Global Acceleration and click Edit.

Note: After enabling global acceleration feature, your requests can be accelerated when using global accelerated domain names. For more information or help, please refer to Help of Global Acceleration Configurations.
3. Click "Enable" and save the change to enable global acceleration for the bucket.

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.

![Upload Files window](image)

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.
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.
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.

![Cloud Object Storage UI](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.

![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.

   ![](Bucket Management Page)

   - **Bucket Name**: examplebucket-12567890
   - **Monitoring**: LI
   - **Region**: Chengdu (China) (ap-chengdu)
   - **Time Created**: 2019-03-20 15:29:59

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

   ![](Select Objects and Download)

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

   ![](COSBrowser Client)

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.
<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
Copy 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**: "939165a4566ac3e0a001f541e94c519"
- **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
Searching for Objects

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-12567890123</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.
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.

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

Introduction

COS allows you to set access permissions for objects, and this setting has a higher priority than that for buckets.

The object access permission is valid only when an access attempt is made to the default domain name. For any access attempt made to a CDN-accelerated or custom domain name, the bucket access permission will prevail.

By setting object access permission, you can, for example, set the specific objects which allow public access in a "private read/write" bucket or set the specific objects which only allow access after authentication in a "public read/write" bucket. Object permissions include the following types:

- Inherited bucket permission: The object has the same access permission as the bucket. When you access an object with the "inherited bucket permission", COS will match the bucket permission to respond to the access. A new object inherits the permission from its bucket by default.
- Public read/private write: When you access an object with the public read permission, the object can be directly downloaded, regardless of the bucket permission.
- Private read/write: When you access an object with the private read/write permission, the object can only be accessed after signature authentication regardless of the bucket permission.

Directions

1. Log in to the COS Console and select Bucket List on the left sidebar to enter the bucket list page. Click the bucket of the object for which you want to modify access permission (such as example) to enter the bucket.
2. Locate the object for which you want to set permission (such as example.exe), click More > Set Permission on its right, and the Set Permission dialog box will pop up.
3. Modify the access permission and click **OK** to save the changes.
Setting Object Encryption

Overview

You can encrypt the objects stored in buckets in the COS Console to prevent data leakage. For more information about encryption, see Server-side Encryption Overview. The following section will guide you through how to encrypt objects.

- COS currently supports SSE-COS for encryption.
- Server-side encryption is currently only available in Beijing, Shanghai, and Guangzhou regions.
- The experience accessing an encrypted object is the same as that accessing an unencrypted one, provided that you already have access to it.
- Server-side encryption encrypts only the data but not the metadata of the object. Server-side encrypted objects can only be accessed with a valid signature but not by anonymous users.
- When you try to list the objects in a bucket, all objects will be listed, no matter whether they are encrypted.

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 **File List** and click **Details** to the right of the object you want to encrypt.

5. In the **Server-side Encryption** configuration item, select SSE-COS and click **Save** to encrypt the object.
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>
</table>

©2013-2019 Tencent Cloud. All rights reserved.
### 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>
</tr>
</thead>
<tbody>
<tr>
<td>Content-Type</td>
<td>text/plain; charset=utf-8</td>
<td>Edit</td>
</tr>
</tbody>
</table>

### Example

Under APPID 1250000000, 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: */*
```
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.
- Expeditied 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:

![Figure: Replica Validity Period](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.
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], [nul], [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.

![Create new folder dialog box](image)

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.

![Folder name input](image)

**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.

![Confirmation Window]

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

**Directory Statistics**

If there are a large number of files or nested directories in this directory, it will take awhile for the directory statistics to load.

Current Directory: examplefolder

<table>
<thead>
<tr>
<th>Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Objects</td>
<td>1</td>
</tr>
<tr>
<td>Object Capacity</td>
<td>2.70MB</td>
</tr>
</tbody>
</table>

Nested folders inside a folder are counted as objects.

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.
Data Extraction

Last updated : 2019-11-06 17:10:31

Overview

COS Select allows you to filter out the desired data at the storage level, which significantly reduces the amount of data transferred by COS and thereby lowers your usage costs and improves your data acquisition efficiency. In the COS Console, you can extract the contents of individual files stored in buckets using the basic SQL templates we provide or by entering syntax-compliant statements.

Notes

- Please make sure that the file to be extracted complies with the specification of COS. For more information on the specification of COS Select, see SELECT Overview.
- The extraction feature in the console allows you to extract up to 40 MB of data from a file of up to 128 MB. If you need to process larger files or extract more data, you need to use APIs or SDKs.

Directions

1. Log in to the COS Console.
2. On 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 Extract in the "Operation" column to the right of the object to be extracted.
5. Enter the extraction page in the console and select the type, header field, delimiter, and compression format of the file to be extracted.

- **File Type**: CSV, JSON
- **Header Field**: Included, Excluded
- **Separator**: Comma, Tab, Semicolon, Custom
- **Compression Format**: Non-compressed, ZIP, BZIP2
- **Encryption Format**: Non-encrypted
- **Size**: 5.03MB
- **Export Format**: CSV, JSON

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

- **Select an SQL Template**
  - select * from cosobject s limit 100
  - select s_1, s_2 from cosobject s
  - select * from cosobject s where s_N = 'xyz'
  - select * from cosobject s where s_N like '%xyz2%
  - select * from cosobject s where CAST(s_N as INTEGER) = 1234
  - select * from cosobject s where CAST(s_N as FLOAT) > 12.34
  - select count(*) from cosobject s
  - select s.key1 from cosobject s
  - select s.array1[0].key1 from cosobject s

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 Extraction Result**.
File Extraction

Select an SQL Template

```sql
select * from cosobject limit 100
```

Extraction Result

[Run SQL] [Export]

Extraction incurs request fee and data scanning fee. The request fee is billed based on the number of objects scanned. For more information on billing, please refer to the documentation. [View Documentation]

The console only downloads and displays the first 100 lines of the extraction results. Please refer to the documentation for more information.

No results available.
Batch Operation

Overview

The batch operation feature of COS allows you to manipulate objects in a bucket in batches. Currently, you can perform the following batch operations:

- Replicating objects

You can put the needed objects in an inventory file, which can come from the inventory report generated by the inventory feature (you need to enable the inventory feature first) or be created in the specified format on your own. The batch operation feature can operate on the objects in batches based on this inventory file. For more information, please see Batch Operation Overview.

Directions

1. Log in to the COS Console and click Batch Operation on the left sidebar to enter the batch operation job management page.
2. Click Create Job to start creating a batch operation job. The main configuration items are described as follows.
   - **Job Region**: Select a region for the job to be created. The task region should be the same as the bucket region where the objects pending operations in your inventory reside; otherwise, the job would fail. The Chengdu and Chongqing regions are currently in beta test.
   - **Inventory Format**: Select a format for the inventory objects as needed. There are two formats:

<table>
<thead>
<tr>
<th>Inventory Format</th>
<th>Field</th>
<th>Configuration Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>COS inventory report</td>
<td>-</td>
<td>Please select this format if the inventory file comes from an inventory report generated by the inventory feature</td>
</tr>
<tr>
<td>CSV</td>
<td>Ignore</td>
<td>Placeholder field, which can be used when your inventory file contains irregular fields</td>
</tr>
<tr>
<td></td>
<td>Bucket</td>
<td>Bucket name</td>
</tr>
<tr>
<td></td>
<td>Key</td>
<td>Name of an object in a bucket. If CSV file format is used, the object name is URL-encoded and must be decoded before it can be used</td>
</tr>
<tr>
<td></td>
<td>VersionId</td>
<td>Object version ID. If versioning is enabled for the bucket, COS assigns a version number to the objects added to the bucket. If you want to use an object version other than the latest</td>
</tr>
</tbody>
</table>
version, you can select a version ID that contains an 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, reflecting that you have selected the correct inventory objects. Then, you will enter the operation configuration page.

- **Job Type**: Select the type of operation you want to perform on all the objects in the inventory list.
- **Destination Bucket**: Select the bucket where to store the replicas of the objects in the inventory list.
- **Storage Type**: Standard or Standard_IA.
- **Server-side Encryption**: Select whether to encrypt the object replicas. Options include no encryption or SSE-COS encryption.
- **Access Permission**: Set access permissions to the object replicas. Options include inheriting destination bucket's permission, private read/write, and public read/private write.
- **Object Metadata**: Set metadata for the object copies. You can choose to copy the original metadata or replace all metadata.
4. Click **Next** to enter the "Other Configurations" page where you can configure the following items:

- **Job Description (Optional)**: Description of the job; optional.
- **Job Priority**: A job of a higher priority will be performed 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 authorize COS.

To authorize COS to batch operate, you need to create a CAM role. For more information on CAM roles, please see [Role Overview](#).

5. Click **Next** to enter the information check page where you can check the batch operation job configuration items. If you need to make a change, click **Modify** or **Previous** accordingly.
confirming that everything is correct, click **OK**.

![Create Job](image)

<table>
<thead>
<tr>
<th>Region and Inventory Configuration</th>
<th>Other Configurations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job Region</td>
<td>Job Description</td>
</tr>
<tr>
<td>Inventory Format</td>
<td>Job Priority</td>
</tr>
<tr>
<td>Inventory Bucket</td>
<td>Job Report</td>
</tr>
<tr>
<td>Inventory File Path</td>
<td>CAM Role</td>
</tr>
<tr>
<td>Inventory ETag</td>
<td>Do not generate</td>
</tr>
<tr>
<td>&quot;a9f50e587172cd1181e25dc368ac8a68&quot;</td>
<td>sRole</td>
</tr>
</tbody>
</table>

**Operation Configuration**

<table>
<thead>
<tr>
<th>Batch Operation</th>
<th>Destination Bucket</th>
<th>Storage Class</th>
<th>Server-Side Encryption</th>
<th>Access Permissions</th>
<th>Metadata Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Batch Data Copy</td>
<td>Chengdu:examplebucket-125</td>
<td>Standard Storage</td>
<td>None</td>
<td>Inherit destination bucket permissions</td>
<td>Copy all metadata</td>
</tr>
</tbody>
</table>

![Create Button](image)
Monitoring Reports

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)</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 using the root account, click **Users** in the left sidebar, and click a sub-account.

2. Select the QcloudMonitorFullAccess 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**.

3. Use the blank template to create a new 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.