

Cloud Object Storage

Console Guide

Product Documentation



Copyright Notice

©2013-2024 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

Bucket Overview

Creating Bucket

Deleting Buckets

Querying Bucket

Clearing Bucket

Setting Access Permission

Setting Bucket Encryption

Setting Hotlink Protection

Setting Origin-Pull

Setting Cross-Origin Resource Sharing (CORS)

Setting Versioning

Setting Static Website

Setting Lifecycle

Setting Logging

Accessing Bucket List Using Sub-Account

Adding Bucket Policies

Setting Log Analysis

Setting INTELLIGENT TIERING

Setting Inventory

Domain Name Management

Overview

Enabling Custom CDN Acceleration Domain Name

Enabling Custom Origin Server Domains

Granting Sub-Account Permission to Configure Bucket Acceleration Domain Names

Setting Bucket Tags

Setting Log Retrieval

Setting Cross-Bucket Replication

Enabling Global Acceleration

Setting Object Lock

Object Management

Uploading an Object

Downloading Objects

- Copying Object
- Previewing or Editing Object
- Viewing Object Information
- Searching for Objects
- Sorting and Filtering Objects
- Direct Upload to ARCHIVE
- Modifying Storage Class
- Deleting Incomplete Multipart Uploads
- Setting Object Access Permission
- Setting Object Encryption
- Custom Headers
- Deleting Objects
- Restoring Archived Objects
- Folder Management
 - Creating Folder
 - Deleting Folder
 - Sharing Folder
 - Viewing Folder Details
 - Setting Folder Permissions
- Data Extraction
- Setting Object Tag
- Exporting Object URLs
- Restoring Historical Object Version
- Batch Operation
- Monitoring Reports
 - Viewing Data Overview
 - Querying Monitoring Data
 - Setting Alarm Policies
- Data Processing
 - Image Processing
 - Basic Image Processing
 - Setting Image Advanced Compression
 - File Processing
 - Setting File Processing
 - Media Processing
 - Enabling Media Processing
 - Function Service
 - Setting CDN Cache Purge

Content Moderation

Moderation Details

Automatic Moderation

Setting Live Stream Moderation

Setting Image Moderation

Setting Video Moderation

Setting Audio Moderation

Setting Text Moderation

Setting Document Moderation

Historical data moderation

Configuring Historical Data Moderation Tasks

Setting Moderation Policy

Setting the Custom Image Risk Library

Setting the Business Field Risk Library

Smart Toolbox User Guide

Data Processing Workflow

Custom Function Processing

Configuring a Workflow

Configuring Job

Template

Queues and Callbacks

Application Integration

MySQL Backup

MongoDB Backup

SQL Server Data Backup

CKafka Message Backup

TDMQ Message Backup

Redis Backup

CDN Log Backup

CLS Log Backup

Adding Log Analysis Function

Data Export to CKafka

Data Export to ES

Console Guide

Console Overview

Last updated : 2024-03-26 16:32:31

Overview

The Cloud Object Storage (COS) console is an easy-to-use tool. It allows you to directly create buckets, upload/share/back up data, and perform batch operations, freeing you from the hassles associated with code writing and program running. The following table lists the features of the COS console as well as their related documents:

Note:

For more information about the features, see [Features](#).

Console Menu	Operation Documentation
Basic Bucket Operations	Bucket Overview Creating a Bucket Deleting a Bucket Querying Buckets Emptying a Bucket
Basic Object Operations	Uploading Objects Downloading Objects Copying Objects Viewing Object Information Searching for Objects Sorting and Filtering Objects Direct Upload to ARCHIVE Modifying Storage Class Deleting Incomplete Multipart Uploads Custom Headers Deleting Objects Restoring Archived Objects
Folder Operations	Creating a Folder Deleting a Folder Sharing Folder Viewing Folder Details Setting Folder Permissions
Lifecycle	Setting Lifecycle
Static Website	Setting up a Static Website

Inventory	Setting Inventory
Bucket Tagging	Setting Bucket Tags
Data Monitoring	Dashboard Querying Monitoring Data Setting an Alarm Policy
Logging	Setting Logging
Data Origin-pull	Setting Origin-Pull
Batch Jobs	Batch Operation
Data Extraction	Data Extraction
Remote Disaster Recovery	Setting Versioning Setting Cross-Bucket Replication
Encryption	Setting Object Encryption Setting Bucket Encryption
Hotlink Protection	Setting Hotlink Protection
Cross-Origin Access	Setting Cross-Origin Resource Sharing (CORS)
Bucket Policy	Adding a Bucket Policy
Access Control	Setting Object Access Permission Setting Bucket Access Permission Accessing Bucket List Using a Sub-Account
Endpoints and Access Acceleration	Domain Name Management Overview Enabling Custom Acceleration Domain Name Enabling Custom Endpoints Granting a Sub-Account Permission to Configure Bucket Acceleration Domain Names Enabling Global Acceleration
Data Processing	Image Processing Media Processing Function Service
Data Processing Workflow	Custom Function Processing Configuring a Workflow Configuring Job Template

	Queues and Callbacks
Application Integration	MySQL Backup MongoDB Backup SQL Server Data Backup CKafka Message Backup TDMQ Message Backup Redis Backup CDN Log Backup CLS Log Backup Multi-File Zipping Hash Calculation GZIP Decompression ZIP Decompression Adding Log Analysis Function Data Export to CKafka Data Export to ES
Application Integration	CKafka Message Backup Log Cleansing

Bucket Management

Bucket Overview

Last updated : 2024-01-06 14:59:34

The COS console provides an **Overview** page where you can view the usage overview, basic information, domain names/endpoints, configuration, and alarms for your bucket.

How It Works

Note:

If the sub-account does not have permission to access the dashboard, contact the root account and ask for request permission by adding user policy **GetBucket**.

1. Log in to the [COS console](#) and click **Bucket List** on the left sidebar.
2. Locate the bucket you want, and click the bucket name.
3. Click the **Overview** tab to enter the bucket overview page.

Usage Overview

Usage Overview shows the number of objects, incomplete multipart uploads, storage usage, traffic, and requests in the current bucket.

Note:

"Usage Overview" data is delayed for about two hours compared with real-time data. It is for monitoring purposes only. For accurate billing data, go to [Billing Center](#) to download usage details.

Number of objects/Number of incomplete multipart uploads: allows you to view the number of objects or incomplete multipart uploads in each COS storage class.

Storage: Allows you to view the storage usage for each available storage class including STANDARD, MAZ_STANDARD, STANDARD_IA, MAZ_STANDARD_IA, ARCHIVE, and DEEP ARCHIVE.

Note:

The MAZ_STANDARD, MAZ_STANDARD_IA, and DEEP ARCHIVE storage usage is available only for buckets in part of supported regions. For the supported regions, see [Storage Class Overview](#).

Traffic: Allows you to view the total traffic, downstream traffic (public network), downstream traffic (private network), and CDN origin-pull traffic for the current month in STANDARD, MAZ_STANDARD, STANDARD_IA, and MAZ_STANDARD_IA storage classes.

Requests: allow you to view the number of all requests, read requests and write requests for the current month.

Retrievals: allow you to view the amount of data retrieved from STANDARD_IA and ARCHIVE.

Basic Information

Basic Information includes bucket name, region, creation time and access permissions.

Bucket Name: consists of a custom bucket name and APPID. For naming information, see [Naming Conventions](#).

Region: specifies the region where the bucket resides.

Creation Time: specifies the time when the bucket was created.

Access Permissions: specify the access permissions for the bucket. For more information on permissions, see [Setting Access Permission](#).

Domain Information

Domain Information shows all the domain names/endpoints configured for the bucket.

Endpoint: the default COS access endpoint for this bucket. It is auto-generated based on the bucket's name and region when you create a bucket.

Default CDN acceleration domain: The auto-generated CDN domain name which uses CDN cache nodes for acceleration, and which you can choose whether to enable or not. If this feature was previously enabled, this option will be displayed. For more information, see [Default CDN Acceleration Domain Name](#).

Custom CDN acceleration domain: allows you to bind a custom domain name to Tencent Cloud CDN to speed up access to the objects in this bucket.

Custom endpoint: allows you to bind your own domain name as a custom endpoint to the bucket for access to the objects in it.

Global acceleration endpoint: the auto-generated endpoint after you enable global acceleration. You can use this endpoint to speed up uploads to the bucket globally. For more information on global acceleration, please see [Global Acceleration > Overview](#).

Static website endpoint: allows you to access a bucket configured as a static website. For more information on static website, please see [Setting Up a Static Website](#).

Bucket Configuration

Bucket Configuration shows the status of each bucket configuration.

MAZ Configuration: The multi-AZ storage architecture offered by COS, which can provide IDC-level disaster recovery capabilities for your data. For more information, see [MAZ Feature Overview](#).

Metadata Acceleration: A high-performance file system feature provided by COS. For more information, see [Metadata Acceleration Overview](#).

CORS: represents cross-origin access which requests resources from another origin over HTTP. Two origins that differ in any one of protocol, domain name, and port are treated as different origins. For more information, see [Setting](#)

Cross-Origin Access.

Versioning: retains multiple versions of an object after you enable versioning on your bucket. It helps to retrieve your data lost due to accidental deletion or application failure. For more information, see [Setting Versioning](#).

Origin-Pull: leads you from COS to another origin for data access using an origin-pull rule when the object you request does not exist in the COS bucket or a specific request needs to be redirected. For more information, please see [Setting Origin-Pull](#).

Bucket encryption: By setting bucket encryption, you can encrypt all new objects uploaded to a bucket with the specified encryption method by default. For more information, see [Bucket Encryption Overview](#).

Inventory: outputs an inventory report on object attributes, configuration details and other information for your bucket every day or every week. For more information, see [Enabling Inventory](#).

Hotlink Protection: prevents malicious programs' cheating for public network traffic using resource URLs or stealing of resources by malicious means. For details, please see [Setting Hotlink Protection](#).

Lifecycle: automatically transitions or deletes specified objects within the specified time according to your lifecycle rule. For more information, see [Setting Lifecycle](#).

Cross-Bucket Replication: Automatically replicates **incremental objects** asynchronously from the source bucket to the destination bucket in another region after you enable cross-region replication. For more information, see [Setting Cross-Bucket Replication](#).

Logging: logs all kinds of COS requests for **bucket operations** after you enable logging to help you better manage and use your bucket. For more information, see [Setting Logging](#).

Tag: a bucket tag used as an identifier to help group and manage buckets. For more information, see [Setting Bucket Tags](#).

Alarm Configuration

Alarm Configuration enables you to configure alarms on your bucket for daily monitoring purposes.

Current alarms: show the number of ongoing alarms.

Alarm policies: show the number of existing alarm policies.

Other Configurations

In addition to the above COS-related configuration items, COS also integrates CI features such as content moderation and data workflow. For more information, see [Overview](#).

Creating Bucket

Last updated : 2024-06-03 10:51:47

Overview

You can create a bucket on the bucket list page through the Cloud Object Storage (COS) console. For the concept of buckets, see [Bucket Overview](#). Below, we will detail how to create a bucket.

Note:

Each account can create up to 200 buckets regardless of the region.

Directions

1. Log in to the [COS console](#).
2. In the left navigation pane, click **Bucket List** to enter the bucket list page.
3. Click **Create Bucket**.
4. In the **Create Bucket** dialog box that is displayed, configure the following information:

4.1 Basic information

Region: Choose a COS region corresponding to the physical area where your business (or user base) is concentrated. Once set, this cannot be modified. For more information about regions, see [Regions and Access Endpoints](#).

Name: Enter a custom bucket name. Once set, this cannot be modified. For naming guidelines, see [Bucket Naming Conventions](#).

Access Permission: By default, a bucket provides three types of access permissions: private read/write, public read/private write, and public read/write. This can be modified after setting. For more information, see [Setting Access Permissions](#).

Endpoint: Automatically generated. After creating a bucket, you can use this domain name to access the bucket.

4.2 Advanced optional configuration

Note:

Advanced settings are optional and can be set as needed.

Versioning: After enabling, uploading an object with the same name or performing operations such as adding, deleting, or modifying objects will save historical versions, facilitating the retrieval of an object's historical versions.

Note:

If versioning and MAZ features are enabled at the same time, the status of versioning cannot be modified. Configure with caution.

MAZ configuration: The MAZ feature is a characteristic of the bucket. When you enable the MAZ configuration, your data will be stored in different data centers within the same region, providing intra-city disaster recovery. Currently, this feature is only available in certain regions, such as Beijing, Shanghai, Guangzhou, Hong Kong (China), and Singapore. For more applicable regions and feature introduction, see [MAZ Feature Overview](#).

Note:

Once the MAZ configuration for a bucket is enabled, it cannot be modified. After enabling, data will be stored in the bucket in storage types that support the MAZ feature (for example, MAZ_STANDARD and MAZ_STANDARD_IA). Configure with caution. If versioning is also enabled, the status of versioning cannot be modified.

MAZ configuration cannot be enabled for existing buckets. It can be enabled only for new buckets during creation.

Metadata Acceleration: This configuration is currently only available to allowlisted users. For more information, see [Metadata Acceleration Overview](#).

Logging: Records various request logs related to bucket operations for you.

Bucket Tag: A bucket tag serves as an identifier for managing buckets. You can set tags for your buckets to facilitate grouped management. For more information, see [Setting Bucket Tags](#).

Server-Side Encryption: You can choose a server-side encryption method. For an introduction to server-side encryption and supported regions, see [Server-Side Encryption Overview](#).

4.3 Confirm configuration

Confirm the bucket configuration information. If you need to make changes, click **Previous**.

5. After confirming the information is correct, click **Create** to create the bucket. On the bucket list page, you can see the bucket you just created.

<div>Create Bucket</div> <div>Manage Permissions</div> <div>Bucket Name ▼ <input type="text" value="Enter the bucket name"/></div>			
Bucket Name ↕ ?	Access ?	Region ▼	Creation Time ↕
cos- cos-1234567890 🗑️	Specified user	Beijing (China) (ap-beijing)	2023-12-20 09:17:32

Note:

The bucket list will only display the buckets you created with Data Lake Compute (DLC) and does not support configuration for now. If you need to configure, go to the [DLC console](#) to proceed.

Deleting Buckets

Last updated : 2024-01-06 14:59:34

Overview

You can delete buckets on the **Bucket List** page in the COS console. For more information on buckets, see [Bucket Overview](#).

Prerequisites

Before deleting a bucket, make sure that the corresponding operations have been completed based on system check results, for example, deleting all objects (including historical versions) and incomplete multipart uploads in the bucket and disabling the CDN acceleration domain name. For details, see [Emptying a Bucket](#) and [Enabling Custom CDN Acceleration Domain Names](#).

Directions

1. Log in to the [COS console](#). Click **Bucket List** on the left sidebar to open the bucket list page.
2. Find the target bucket and click **More > Delete** in the **Operation** column on the right.

examplebucket-125	Specified user	(China) (ap-chengdu)	2019-03-20 15:29:59	Monitor Configuration Management More
examplebucket-125	Specified user	(China) (ap-shanghai)	2020-06-19 16:42:21	Tag Clear Delete

3. In the pop-up window, perform the operation based on the system check result.

Querying Bucket

Last updated : 2024-01-06 14:59:34

Overview

You can quickly query the created buckets by bucket name and tag in the COS console.

Note:

Before you can access the bucket list with a sub-account, the sub-account must be authorized by the root account.

For more information, see [Accessing Bucket List Using Sub-Account](#).

As the `List Bucket` operation is not restricted by bucket permission, a sub-account cannot be restricted to querying just specified buckets.

Querying by Bucket Name or Tag

1. Log in to the [COS console](#) and click **Bucket List** on the left sidebar to enter the bucket list page, where you can view all the created buckets.
2. If there are many buckets, you can search for buckets by **bucket name** or **tag** in the top-right corner of the **Bucket List** page.

Query by **bucket name**: You can enter a specific bucket name or a bucket name **prefix** to query buckets.

Create Bucket	Manage Permissions	Bucket Name	exam	Q	↺	⬇	⚙
Bucket Name	Access	Region	Creation Time	Operation			
examplebucket-1250000000	Specified user	Chengdu (China) (ap-chengdu)	2019-03-20 15:29:59	Monitor	Configure	More	
examplebucket-125-1250000000	Specified user	Shanghai (China) (ap-shanghai)	2020-06-19 16:42:21	Monitor	Configure	More	

Query by **tag**: If you have set tags for a bucket as instructed in [Setting Bucket Tags](#), you can also select **Tag** in the top-right corner of the **Bucket List** page and enter a **tag key** to query buckets.

Create Bucket	Manage Permissions	Tag	exampletag	Q	↺	⬇	⚙
Bucket Name	Access	Region	Creation Time	Operation			
examplebucket-1250000000	Specified user	Chengdu (China) (ap-chengdu)	-	Monitor	Configure	More	

Clearing Bucket

Last updated : 2024-01-06 14:59:34

Overview

You can clear the specified bucket in the COS console. For more information on buckets, see [Bucket Overview](#).

Note:

Clearing a bucket will delete all objects and incomplete multipart uploads in this bucket. The deleted data is unrecoverable and inaccessible. Proceed with caution.

Use Cases

Clearing a bucket through a [lifecycle rule](#): This method is applicable to a bucket with more than 10,000 objects. A deletion job will be triggered when the trigger condition of a lifecycle rule is met. The job start and completion time are subject to the lifecycle rule configuration in the console.

Quickly clearing a bucket in the console: This method is applicable to a bucket with less than 10,000 objects. A bucket clearing job will take effect immediately upon completion.

Note:

If you have a large amount of data in your bucket, clearing the bucket using the console may be slow or even fail due to network reasons. In this case, we recommend you clear the bucket by setting lifecycle configuration.

Directions

Quickly clearing a bucket in the console

1. Log in to the [COS console](#).
2. Click **Bucket List** on the left sidebar.
3. Find the target bucket and click **More > Clear Data** on the right.
4. In the pop-up window, enter the name of the bucket you want to clear and click **Confirm**.
5. In the pop-up window, click **OK**.

Clearing a bucket through a lifecycle rule

1. Log in to the [COS console](#).
2. Click **Bucket List** on the left sidebar.
3. Locate the bucket for which you want to set the lifecycle feature. Click the bucket name to enter its details page.

4. Click **Basic Configurations** > **Lifecycle** and click **Add a Rule**.

5. In the **Add a Rule** pop-up window, set to delete all current and historical versions of files in the entire bucket.

Rule name: Enter the name of the lifecycle rule, which is required.

Applied to: Select **The whole bucket**.

Managing the current version: Set to delete files one day after modification.

Managing historical versions: Set to delete files one day after modification.

As bucket data deletion is a high-risk operation, you need to click **OK** to confirm the operation.

6. You can see that the deletion rule has been set successfully in the lifecycle rule list.

7. After the lifecycle rule is executed, you can see that both the number and volume of stored objects are zero on the bucket overview page, indicating that the bucket has been cleared. If you no longer use the bucket, you can delete it.

Setting Access Permission

Last updated : 2024-01-06 14:59:34

Overview

You can use the COS console to set or modify bucket access permissions of the following two types.

Public permissions: Include private read/write, public read/private write and public read/write. For more information, see **Types of Permission** under [Bucket Overview](#).

User ACLs: The root account has all bucket permissions (full control) by default. You can add sub-accounts and grant them permissions including read/write, read/write ACL, and even **full control**.

Note:

If the bucket permission is private read/write or a specified account is granted the permission, an object request needs to carry a signature for identity verification. For more information on signature, see [Request Signature](#).

If the bucket permission is public read/private write or public read/write, an object request doesn't need to carry a signature, and anonymous users can directly access the object at the URL. However, your data may be leaked.

Therefore, proceed with caution.

Granting Permissions for a Single Bucket

Directions

1. Log in to the [COS console](#).
2. On the left sidebar, click **Bucket List**.
3. Locate the bucket for which you want to set or modify access permissions, and then click the bucket name.
4. Select **Permission Management > Bucket ACL (Access Control List)** and you can set both public permissions and user ACLs for the bucket. For example, you can add a sub-account, whose ID can be viewed in the [CAM console](#).

5. Click **Save**.

Directions

1. Log in to the [COS console](#).
2. On the left sidebar, click **Bucket List**.
3. Click **Manage Permissions** above the bucket list.
4. In the pop-up window, select the buckets that you want to grant permissions for. Then, scroll down to set both public permissions and user ACLs. For example, you can add a sub-account, whose ID can be viewed in the [CAM console](#).

Authorize

Select (15 buckets)

Search bucket name

☐

Bucket Name

Region

☐

ap-beijing-125

Beijing

☐

ap-chengdu-125

Chengdu

☐

ap-chongqing-125

Chongqing

☐

ap-guangzhou-125

Guangzhou

☐

ap-hongkong-125

Hong Kong (China)

☐

ap-mumbai-125

Mumbai, India

☐

ap-seoul-125

Seoul, South Korea

(0) selected

Bucket Name

Region

The current list is empty

Public Permissions

☒ Modify

☒ Private Read/Write

☐ Public Read/Private Write

☐ Public Read/Write

User ACL

☒ Modify

User Type	Account ID ⓘ	Permissions	Operation
Root account	1000	Full control	--
Add User			

The authorization does not require a permission consistency check. The new permission will overwrite the same old one for an account that has already been added to the bucket.

OK

Cancel

5. Once completed, click **OK**.

Setting Bucket Encryption

Last updated : 2024-01-06 14:59:34

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, see [Bucket Encryption Overview](#).

Note:

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, see [Server-Side Encryption Overview](#).

Directions

Setting encryption during bucket creation

You can configure bucket encryption when [creating a bucket](#).

Create Bucket

Name

examplebucket-1256289578

Only support lowercase letters, numbers and "-". Up to 50 characters.

Region

China

Chengdu

Services within the same region can be accessed through private network

Access Permissions

☒ Private Read/Write

☐ Public Read/Private Write

☐ Public Read/Write

Identity verification is required before accessing objects.

Endpoint

examplebucket-1256289578.cos.ap-chengdu.myqcloud.com

Request endpoint

Bucket Tag

Enter a tag key

Enter a tag value

+

Server-Side Encryption

☐ None

☒ SSE-COS

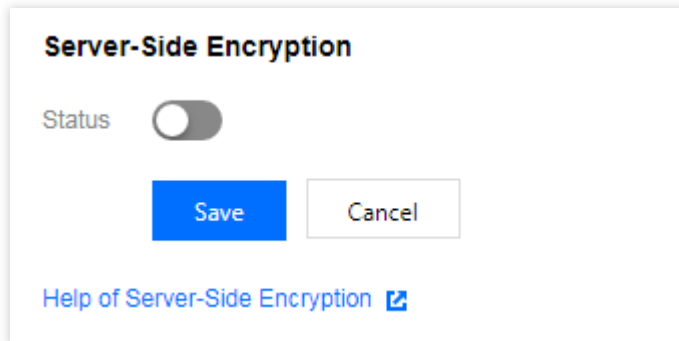
OK

Cancel

Setting encryption for existing bucket

If you did not set encryption when creating a bucket, follow the steps below to set it subsequently.

1. On the [Bucket List](#) page, click the name of the target bucket to enter the bucket configuration page.
2. Click **Security Management > Server-Side Encryption** on the left sidebar.
3. In the **Server-Side Encryption** configuration item, toggle the feature on.



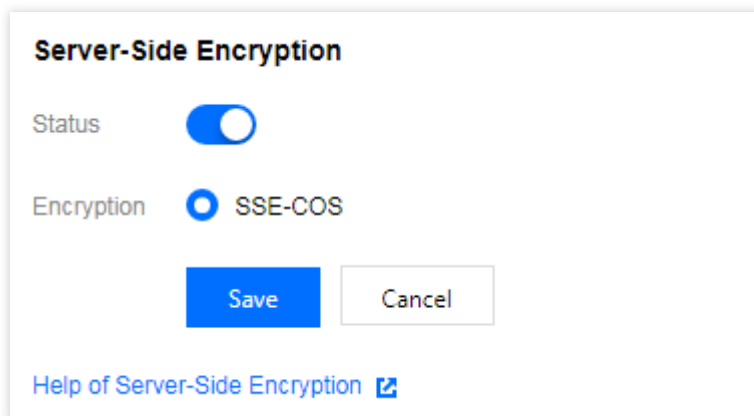
Server-Side Encryption

Status ☐

[Help of Server-Side Encryption](#)

[Save](#) [Cancel](#)

4. Select the specified encryption method and click **Save**.



Server-Side Encryption

Status ☒

Encryption ☒ SSE-COS

[Save](#) [Cancel](#)

[Help of Server-Side Encryption](#)

Setting Hotlink Protection

Last updated : 2024-01-06 14:59:34

Overview

Tencent Cloud COS provides hotlink protection to help users avoid unnecessary losses caused by malicious programs' stealing public network traffic using resource URLs or stealing resources. We recommend that you configure the blocklist/allowlist in Hotlink Protection Settings on the console to ensure security protection.

Note:

If a signature is carried in the access URL or headers, hotlink protection-based verification will not be performed. When configuring hotlink protection, you can add your domain to the allowlist for the multipart upload request of large files.

Directions

1. Log in to the [COS console](#). Click **Bucket List** on the left sidebar to open the **Bucket List** page.
2. Locate the bucket for which you want to set hotlink protection, and click its name to enter the bucket management page.
3. Click **Security Management > Hotlink Protection**, find the hotlink protection configuration item, and click **Edit**.
4. Switch the status to **Enable**, select a list type (blocklist or allowlist), enter the applicable domain names, and then click **Save**. The configuration items are described as follows:

Hotlink protection

Status

☒

Type

☒ Whitelist ☐ Blacklist

Allow empty referer①

☐ Allow ☒ Deny

Referer

Domain or IP

Please enter domain name or IP address, support multi-line, up to 10 lines, support wildcard *, such as: *.test.com

Save

Cancel

[Learn more](#)

Blocklist: 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.

Allowlist: 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.

Empty referer: For an HTTP request, the header referer can be left empty (i.e., the HTTP request header has no referer field or the referer field is empty).

Referer: Enter up to 30 domain names or IP addresses (one per line). The wildcard `*` is supported, such as

`*.test.com`. Examples are as follows:

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`.

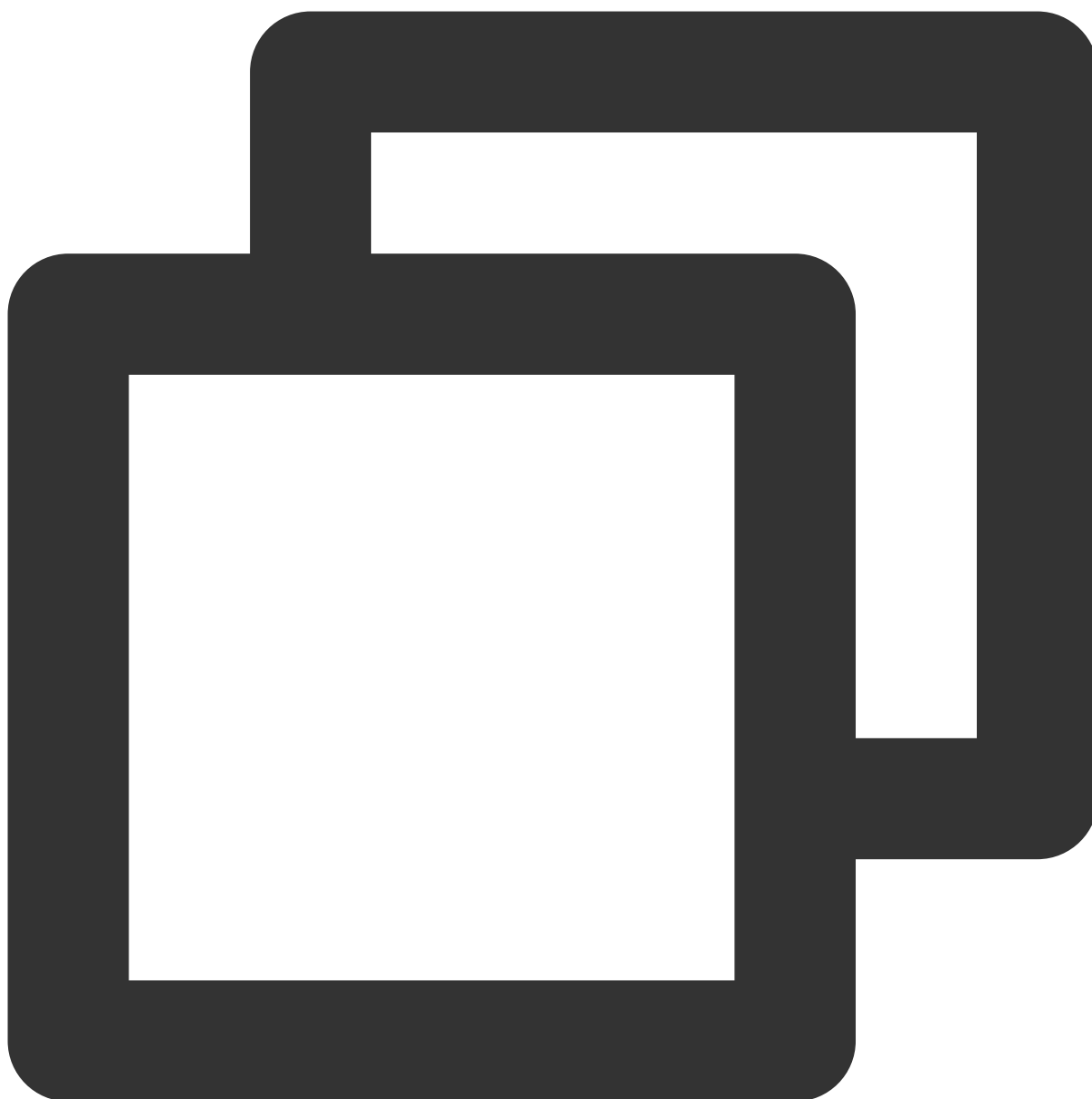
If `*.example.com` is specified, addresses such as `a.b.example.com/123` and `a.example.com` are also included.

Note:

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

Example

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



```
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`.



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

In such cases, to avoid losses for User A, we provide the following two methods of enabling hotlink protection.

Method 1

Configure the **blacklist** by entering the domain name `*.fake.com`, and save.

Method 2

The **allowlist** method: Add `*.example.com` to the allowlist and save.

Before enabling hotlink protection

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 enabling hotlink protection

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.

Notes for Mini Program

1. For network requests using Weixin Mini Programs, the referer value is fixed as

`https://servicewechat.com/{appid}/{version}/page-frame.html` .

2. If hotlink protection is enabled for your bucket, to allow Weixin Mini Programs to load COS images, add

`servicewechat.com` to your hotlink allowlist in the [COS console](#).

Setting Origin-Pull

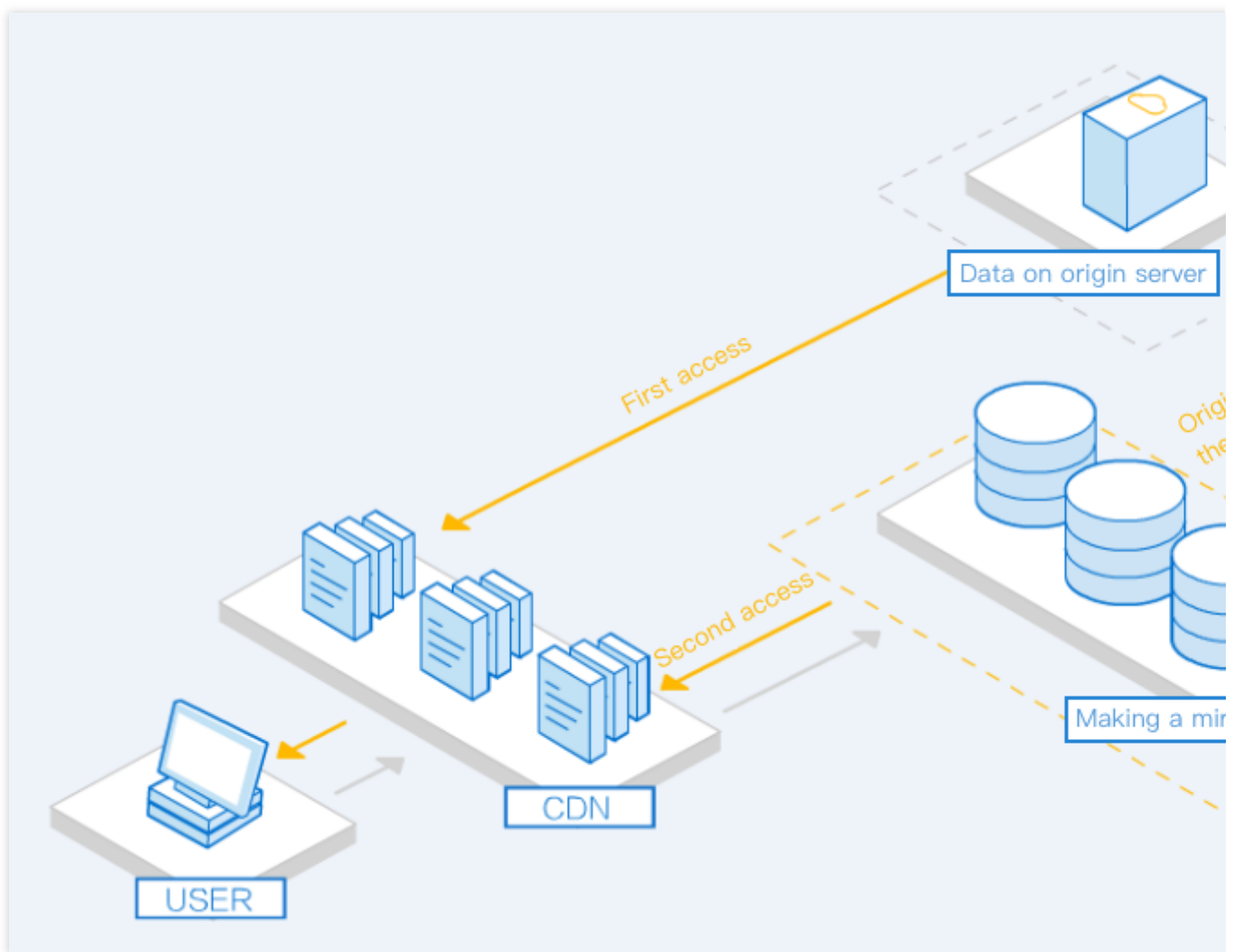
Last updated : 2023-12-15 16:23:25

Overview

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

Note:

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



Origin-Pull Rules

Trigger condition

In async and sync origin-pull modes, origin-pull is triggered only when the request returns the 404 error.

In redirect mode, you can customize HTTP status codes between 400 and 599 to trigger origin-pull.

Origin access

In async and sync origin-pull modes, you can set whether to pass through the `QueryString` and header information of the COS access request to the origin, and configure to carry additional header information when requesting the origin. In redirect mode, you can only set whether to pass through the `QueryString`.

If `GET range` is specified during the GET operation, COS will send an async request without `range` in addition to the original request to get the complete object data and store it in COS.

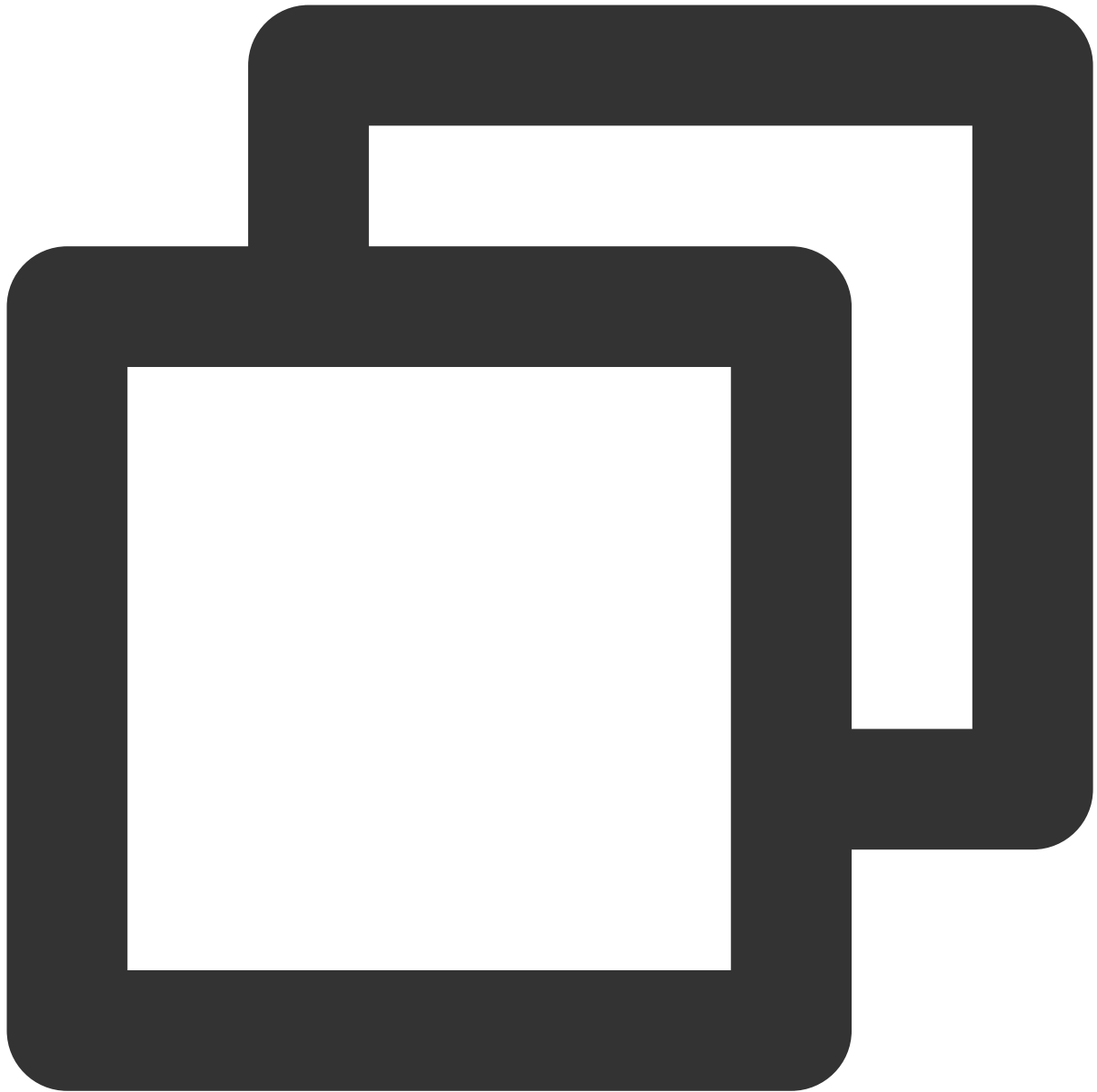
Response and storage

The origin can return data in chunked encoding.

If the origin returns a 404 status code, it will be passed through to COS and returned to the user. If **3xx Following Policy** is enabled, when the origin returns a 3xx status code, COS will pull data from another origin. If the origin returns other non-3XX status codes, COS will return a 424 status code.

The file returned by origin-pull will be stored in COS with the filename used when the origin is requested. For example, if the file `example.jpg` requested by a user does not exist in the bucket, COS will trigger the origin-pull mechanism to pull the file from the configured origin-pull address `http://origin.com/example.jpg` and rename the file stored in the bucket `example.jpg`.

The new object stored in COS will contain the following metadata, with the data content following the values in the origin:



```
cache-control  
content-disposition  
content-encoding  
content-type  
expires  
x-cos-meta-*
```

Directions

1. Log in to the [COS console](#).
2. Click **Bucket List** on the left sidebar.
3. Click the name of the bucket for which you want to set origin-pull.
4. Select **Basic Configurations** > **Origin-Pull** on the left, and click **Add Rule**.

Origin-pull Configurations

Origin-pull condition	Origin-pull Address	Origin-pull proces...	Origin-Pull Para
Add origin-pull rule			

[Learn more](#)

5. In the pop-up window, configure the following information and click **Next**:

Origin-Pull Mode: Select an origin-pull mode as needed.

Async Origin-Pull: If the requested file doesn't exist in COS, COS will search for it on the specified origin. In the Async Origin-Pull mode, COS returns 302 to the client after finding that the file does not exist. The client jumps to the specified origin, and then asynchronously uploads the file to the COS bucket.

Note:

Async origin-pull does not directly return the file; instead, it returns a 302 status code to the client first and then asynchronously uploads the file to COS.

1. We recommend you enable **Follow 302** to pull data from the origin.
2. The file upload time is subject to multiple factors, and no SLA can be promised. **We recommend you select sync origin-pull if your business is sensitive to delays.**

Sync Origin-Pull: If the requested file doesn't exist in COS, COS will search for it on the specified origin, return it to the client, and upload it to the bucket.

Redirect: If a specified error is reported when accessing the bucket, COS will return the redirection address to the client but will not save the file from the origin. The client can request the resource from the origin at the redirection address.

Origin-Pull Condition: Specify all conditions that must be met at the same time for triggering origin-pull.

HTTP Status Code 404: If you select **Async Origin-Pull** or **Sync Origin-Pull**, this parameter is required and cannot be canceled, and origin-pull will be triggered when the HTTP status code is 404. If you select **Redirect**, you can enter an HTTP status code ranging from 400 to 599.

File name prefix: When the requested file matches the prefix, the origin-pull rule will be triggered. For example, if you set this option to `prefix`, when you access `https://examplebucket-1250000000.cos.ap-chengdu.myqcloud.com/prefix123.jpg` and the returned HTTP status code is 404, the origin-pull rule will be triggered.

Origin-Pull Protocol: The protocol used by COS to access the specified origin. The options include `Force HTTPS` , `Force HTTP` , and `Follow request protocol` .

If you select `Force HTTPS` or `Force HTTP` , COS will access the origin using HTTPS or HTTP respectively.

If you select `Follow request protocol` , COS will access the origin with the protocol used in the request.

Request Parameter: Specify whether to pass through the queryString request parameters carried when accessing COS to the origin.

Passthrough specifies the request header: Specify the request headers you want to pass through to the origin. If you select **Redirect** as the origin-pull mode, do not set this parameter.

New request header: You can add additional request headers to be carried during origin-pull. If you select **Redirect** as the origin-pull mode, do not set this parameter.

6. Configure the following information based on the selected origin-pull mode and click **Next**:

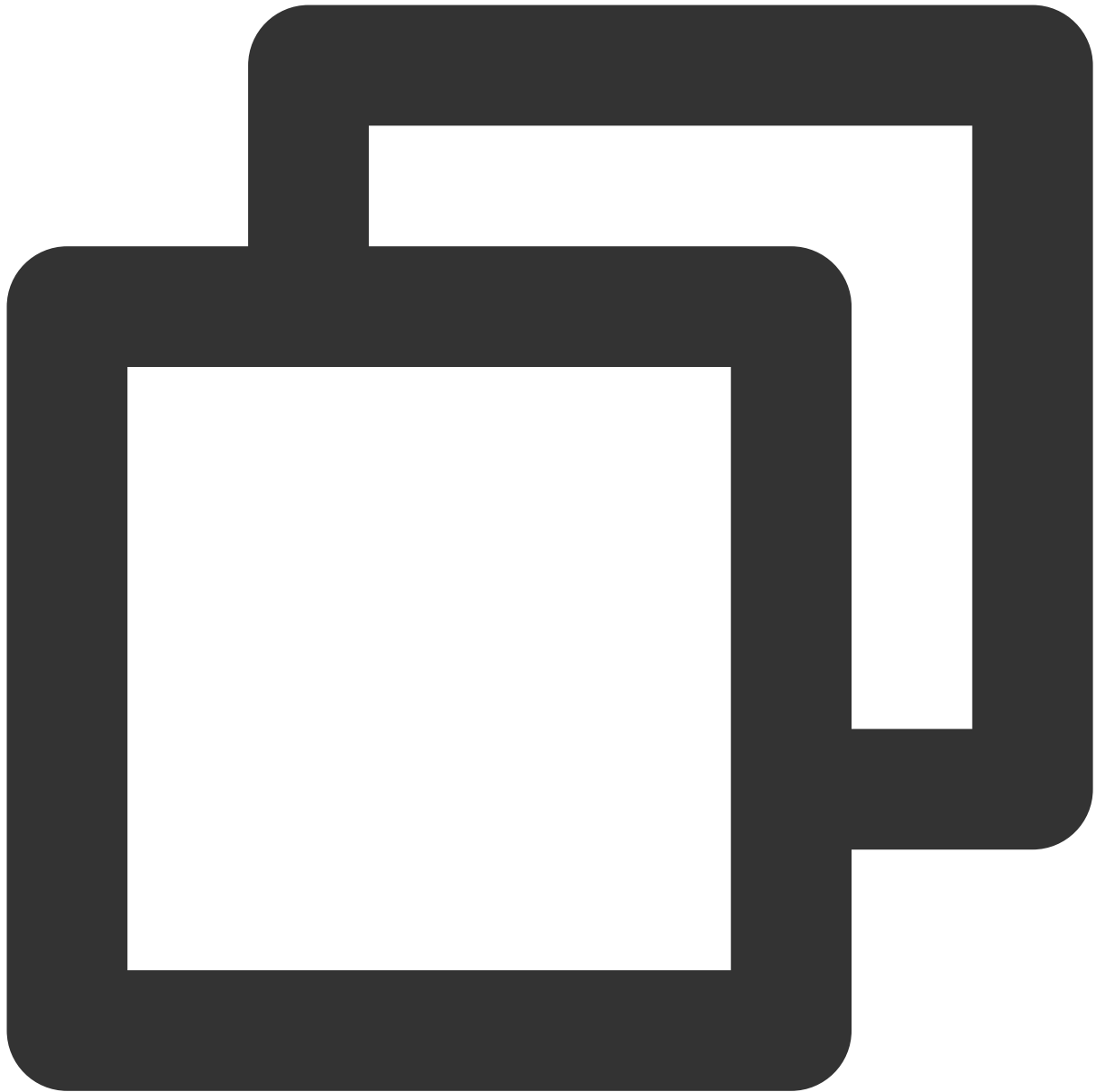
Async origin-pull

Sync origin-pull

Redirect

Origin-Pull Address: Enter the domain name or IP address without the `http://` or `https://` prefix. You can also add the port number after the domain name or IP address.

Example of a correct address:



```
abc.example.com
abc.example.com:8080
202.96.128.86
202.96.128.86:8080
```

Standby forwarding address: You can enter a domain name or IP address as configured below:

Fixed file: Specifies a fixed file to which all requests are redirected when the origin-pull rule is triggered.

Specified prefix: Specifies the prefix for the file to which a request is redirected when the origin-pull rule is triggered.

For example, if the prefix is specified as `test`, the request is redirected to `<origin-pull`

address>/test/prefix123. jpg when you access https://examplebucket-1250000000.cos.ap-chengdu.myqcloud.com/prefix123.jpg , and the origin-pull rule is triggered.

Specified suffix: Specifies the suffix for the file to which a request is redirected when the origin-pull rule is triggered.

For example, if the suffix is specified as .jpg , the request is redirected to <origin-pull

address>/prefix123.jpg when you access https://examplebucket-1250000000.cos.ap-chengdu.myqcloud.com/prefix123 , and the origin-pull rule is triggered.

Note

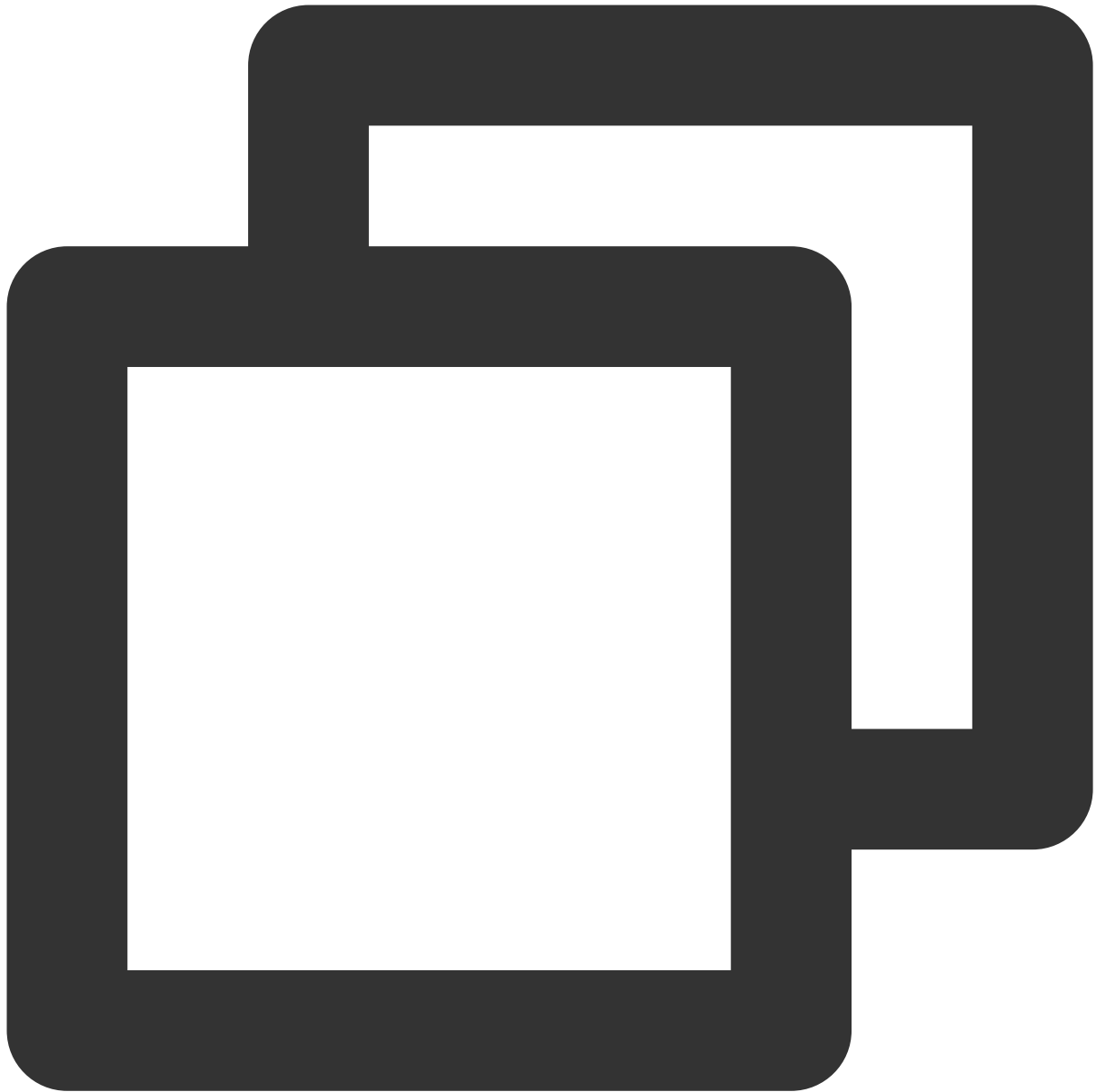
If you select Fixed file , the other fields cannot be used.

Specified prefix and Specified suffix can be used at the same time.

3xx Following Policy: If this policy is enabled, when your origin returns a 3xx redirect, COS will follow it to pull data from another origin.

Origin-Pull Address: Enter the domain name or IP address without the http:// or https:// prefix. You can also add the port number after the domain name or IP address.

Example of a correct address:



```
abc.example.com
abc.example.com:8080
202.96.128.86
202.96.128.86:8080
```

Standby forwarding address: You can enter a domain name or IP address as configured below:

Fixed file: Specifies a fixed file to which all requests are redirected when the origin-pull rule is triggered.

Specified prefix: Specifies the prefix for the file to which a request is redirected when the origin-pull rule is triggered.

For example, if the prefix is specified as `test`, the request is redirected to `<origin-pull`

address>/test/prefix123. jpg when you access https://examplebucket-1250000000.cos.ap-chengdu.myqcloud.com/prefix123.jpg , and the origin-pull rule is triggered.

Specified suffix: Specifies the suffix for the file to which a request is redirected when the origin-pull rule is triggered.

For example, if the suffix is specified as .jpg , the request is redirected to <origin-pull

address>/prefix123.jpg when you access https://examplebucket-1250000000.cos.ap-chengdu.myqcloud.com/prefix123 , and the origin-pull rule is triggered.

Note

If you select Fixed file , the other fields cannot be used.

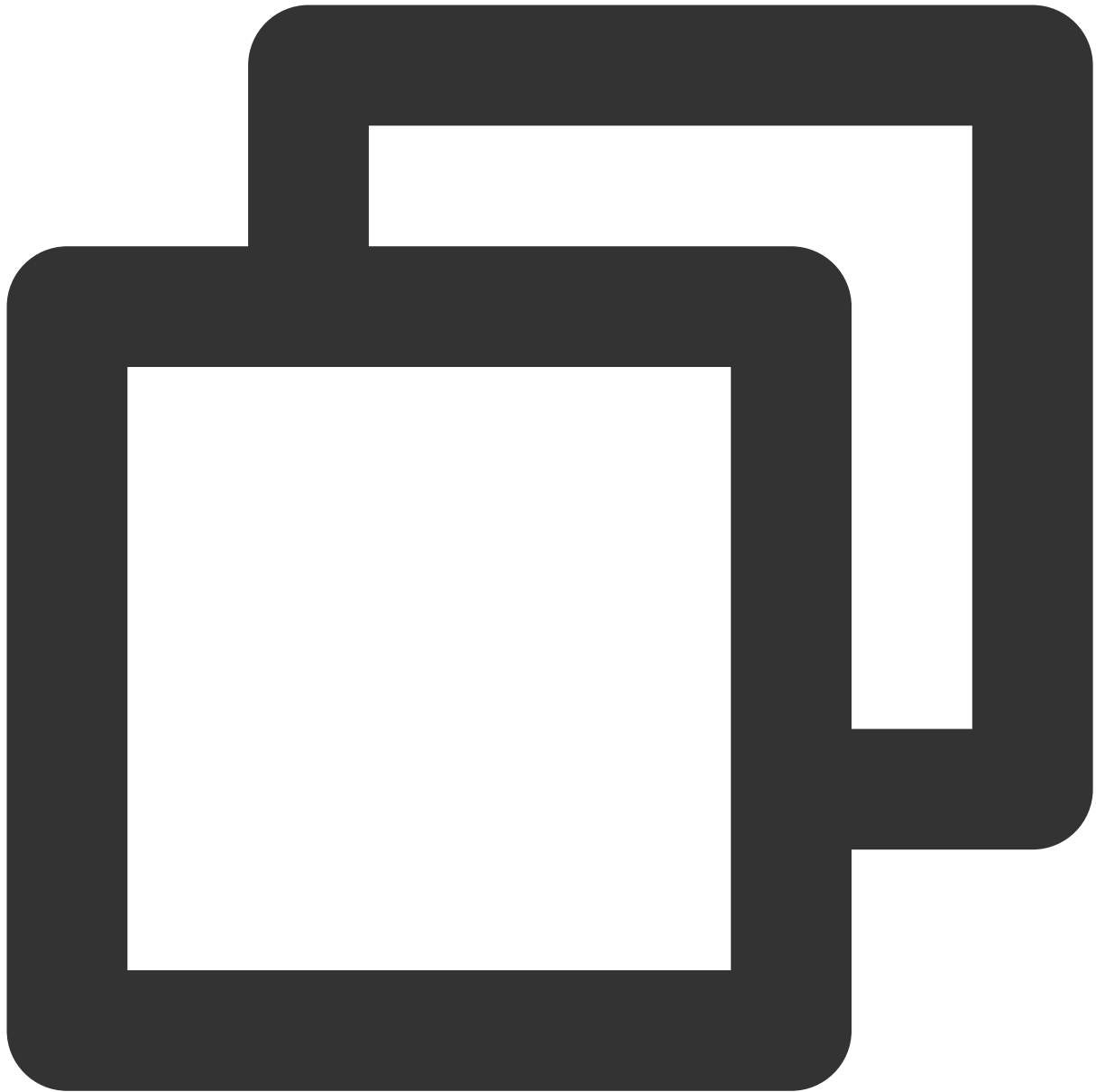
Specified prefix and Specified suffix can be used at the same time.

3xx Following Policy: If this policy is enabled, when your origin returns a 3xx redirect, COS will follow it to pull data from another origin.

Packet of origin site: After this feature is enabled, the packet from the origin will be directly returned, including the status code and other information.

Origin-Pull Address: Enter the domain name or IP address without the http:// or https:// prefix. You can also add the port number after the domain name or IP address.

Example of a correct address:



```
abc.example.com
abc.example.com:8080
202.96.128.86
202.96.128.86:8080
```

Standby forwarding address: You can enter a domain name or IP address as configured below:

Fixed file: Specifies a fixed file to which all requests are redirected when the origin-pull rule is triggered.

Specified prefix: Specifies the prefix for the file to which a request is redirected when the origin-pull rule is triggered.

For example, if the prefix is specified as `test`, the request is redirected to `<origin-pull`

address>/test/prefix123.jpg when you access https://examplebucket-1250000000.cos.ap-chengdu.myqcloud.com/prefix123.jpg , and the origin-pull rule is triggered.

Specified suffix: Specifies the suffix for the file to which a request is redirected when the origin-pull rule is triggered.

For example, if the suffix is specified as .jpg , the request is redirected to <origin-pull

address>/prefix123.jpg when you access https://examplebucket-1250000000.cos.ap-chengdu.myqcloud.com/prefix123 , and the origin-pull rule is triggered.

Note

If you select Fixed file , the other fields cannot be used.

Specified prefix and Specified suffix can be used at the same time.

Redirect Code: You can select 301 (default value), 302, or 307.

7. Confirm that the configured origin-pull rule is correct and click **OK**.

By default, COS always gives the highest priority to the most recent rule, by which it performs origin-pull. To change the priority manually, you can click the "Edit" icon under the "Priority" column in the rule list.

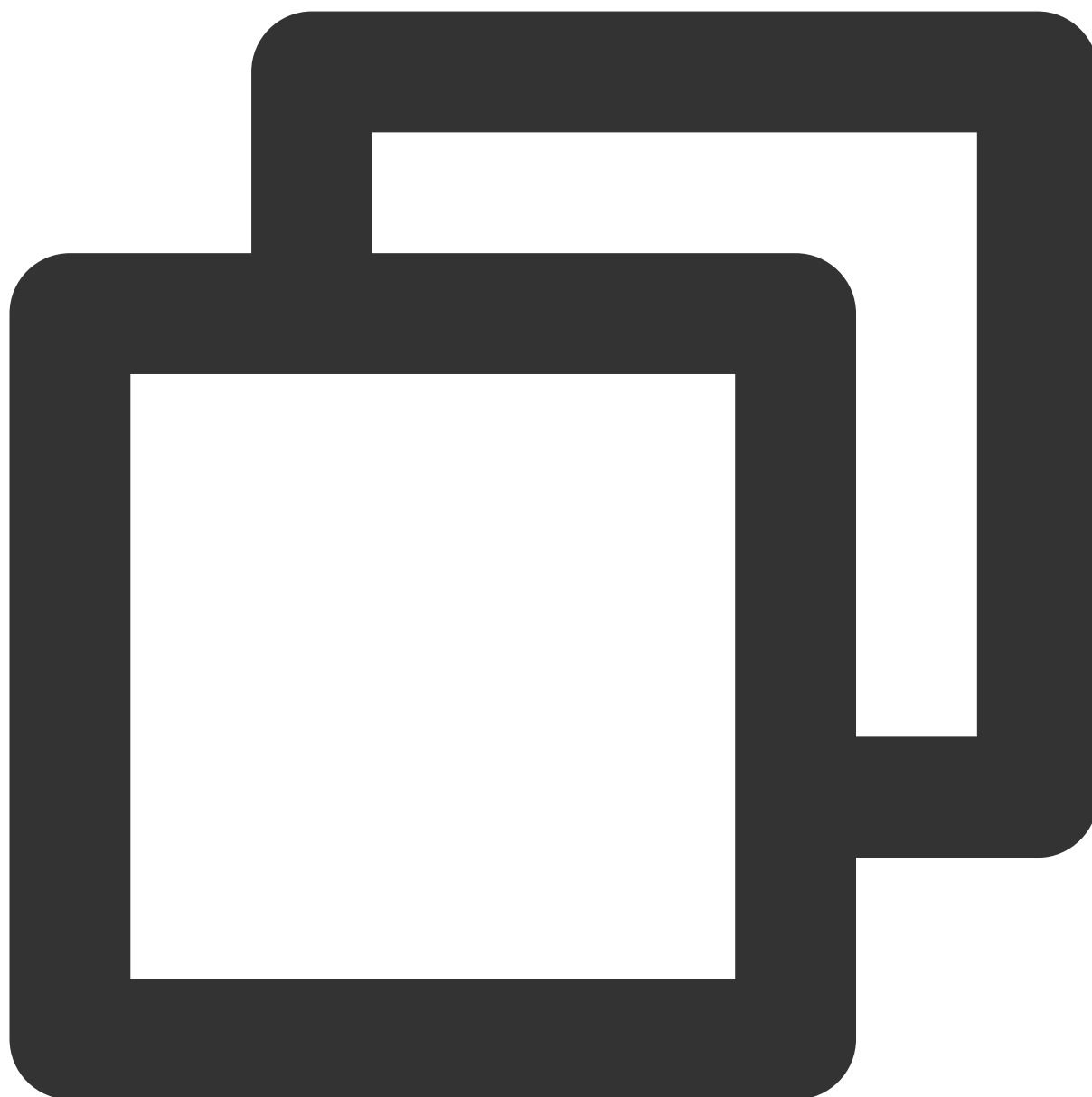
Origin-pull Configurations

Origin-pull con...	Origin-pull Address	Origin-pull pro...	Origin-Pull Par...	Priori
HTTP Status Code 404	http(s)://111.11.11.1/suffix1	Follow request protocol Follow the origin site 3xx redirect	pass-through queryString Redirect Code 302	2 
HTTP Status Code 404	http(s)://111.11.11.1/prefix1	Follow request protocol Follow the origin site 3xx redirect	pass-through queryString Redirect Code 302	1 

Examples

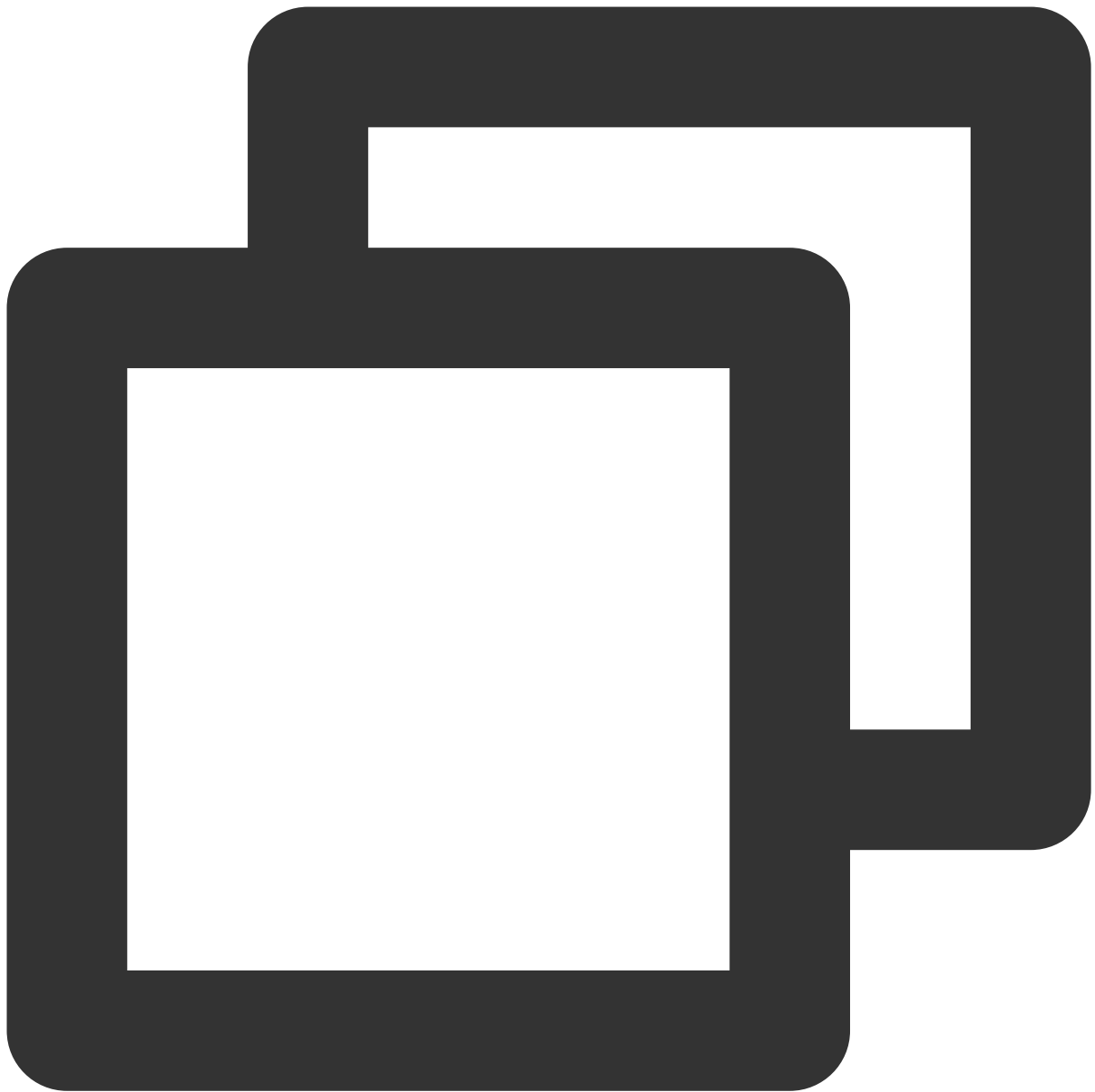
Background

A user whose APPID is 1250000000 created a bucket named "examplebucket-1250000000", and enabled CDN acceleration endpoint domain name:



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

Configure the origin-pull address of the bucket to be:



`abc.example.com`

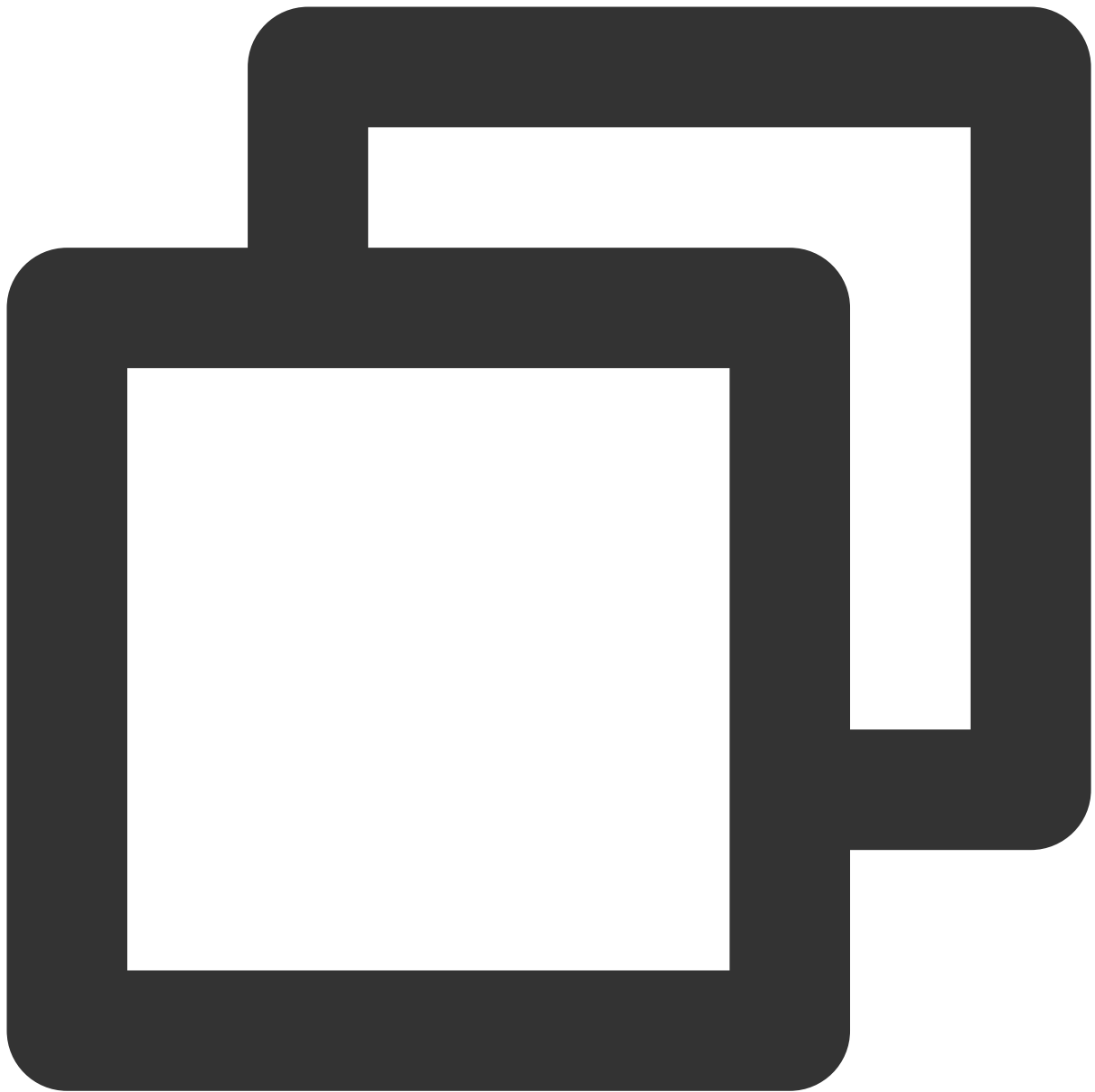
Store the image `picture.jpg` on the origin `http://abc.example.com` .

First access by client (without sync origin-pull enabled):



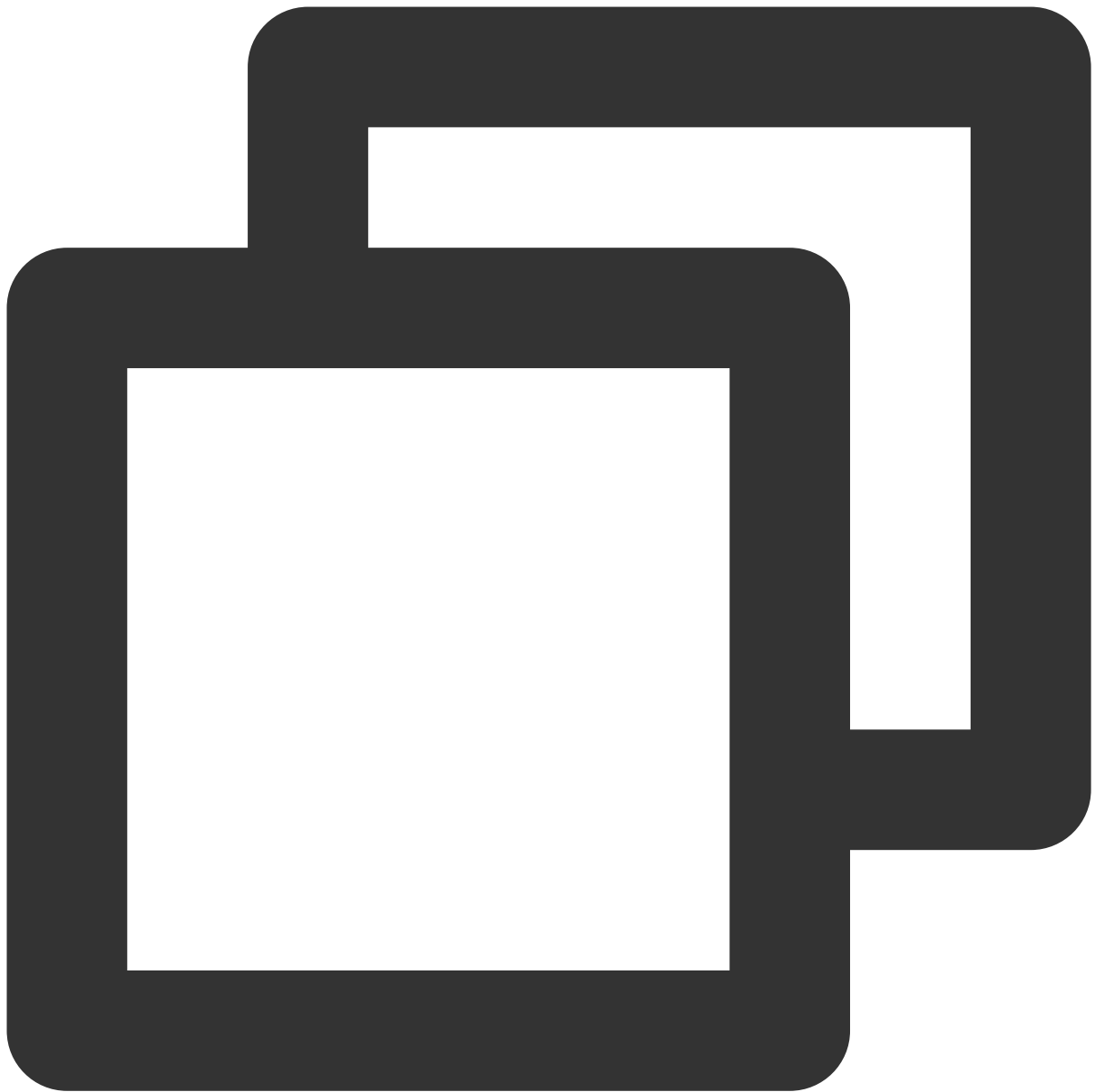
```
http://examplebucket-1250000000.file.myqcloud.com/picture.jpg
```

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



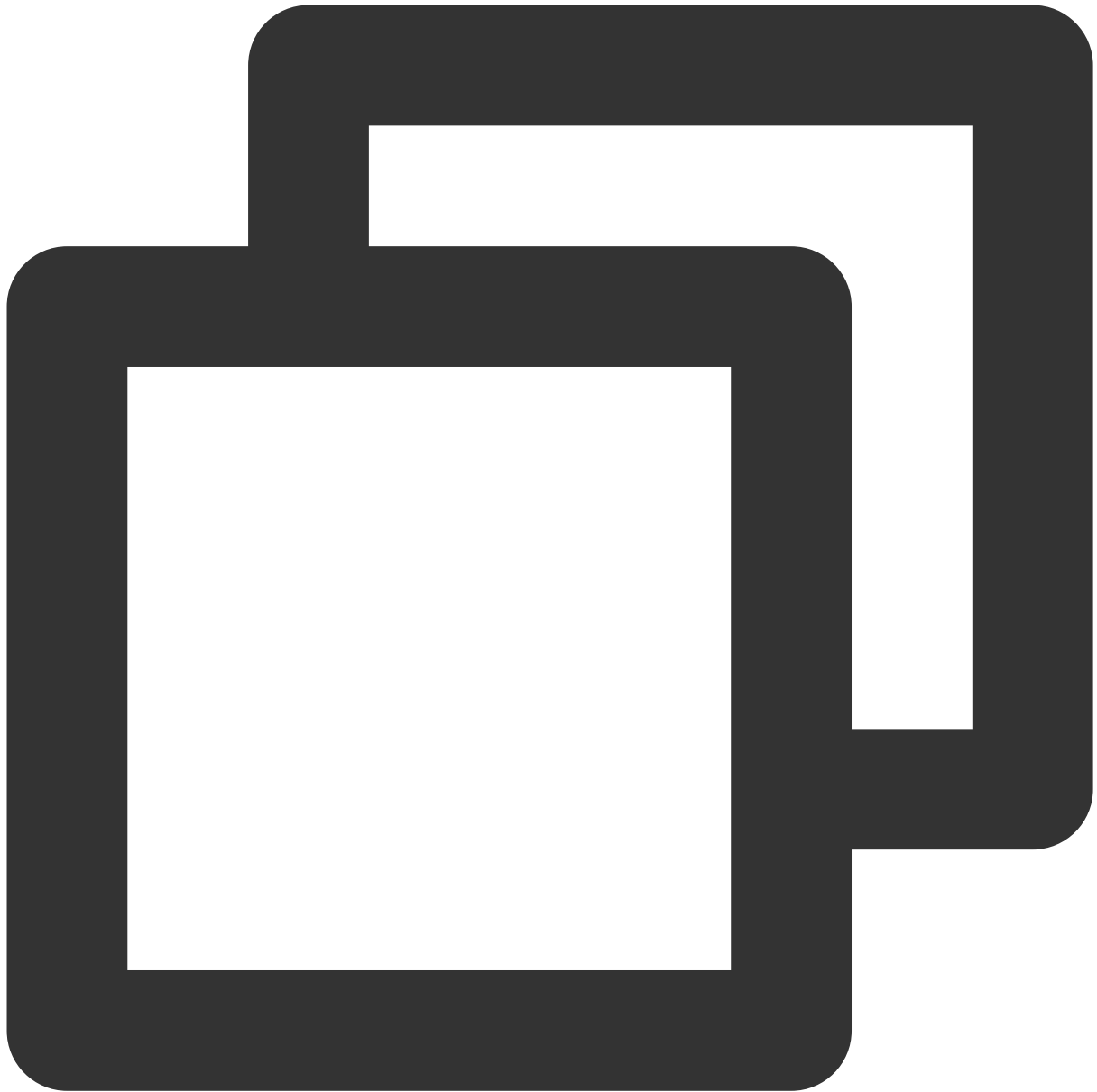
```
http://abc.example.com/picture.jpg
```

First access by client (with sync origin-pull enabled):



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

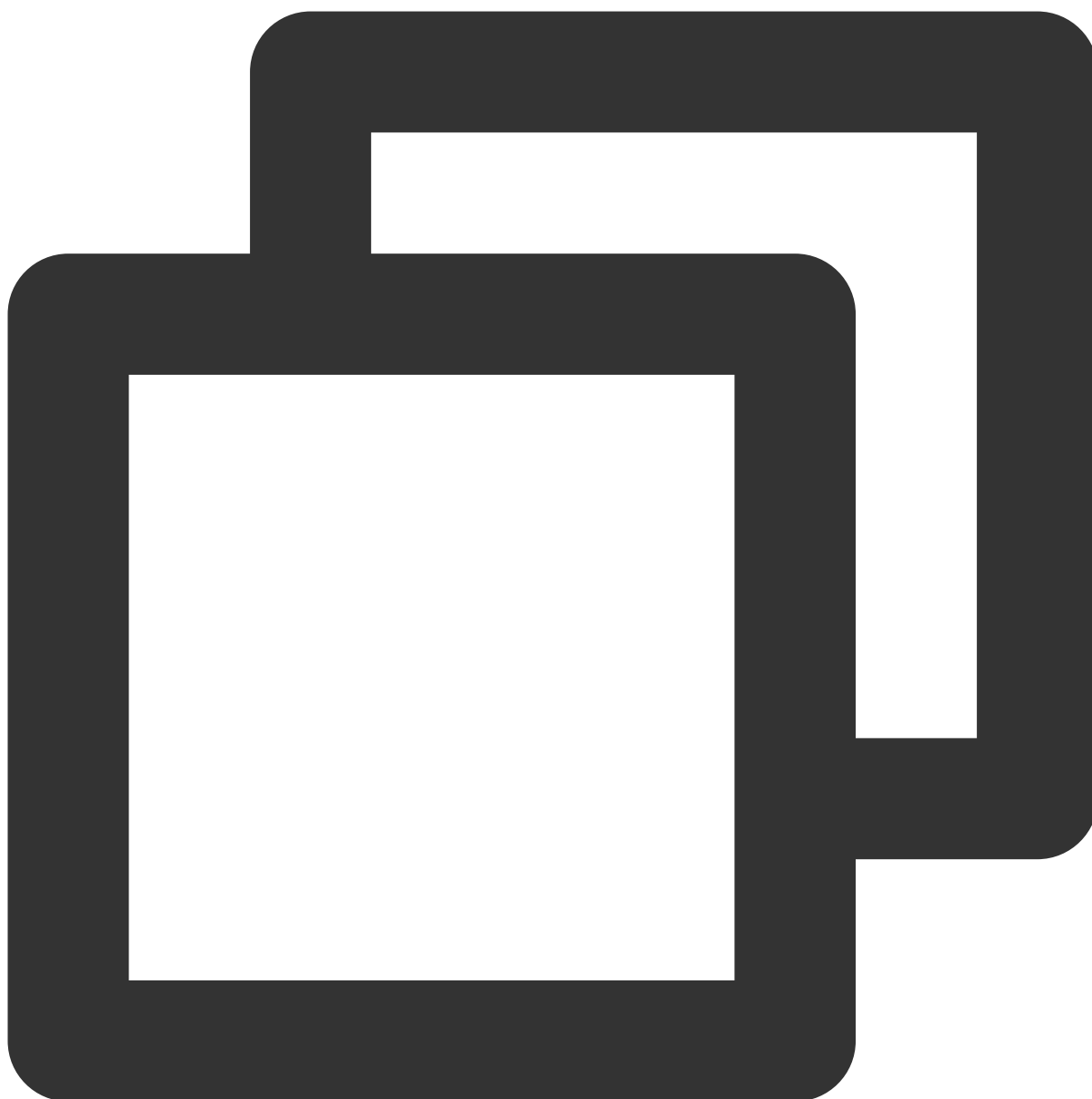
When COS finds that the object cannot be hit, it returns the HTTP status code 200 to the client and redirects to the following address:



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

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

Second-time access:



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

COS directly hits the picture.jpg object in the root directory and returns it to the client.

Setting Cross-Origin Resource Sharing (CORS)

Last updated : 2024-01-06 14:59:34

Overview

You can set Cross Origin Resource Sharing (CORS) for objects in buckets through the Cloud Object Storage (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, please see [Cross-Origin Resource Sharing](#) and [Setting Cross-Origin Access](#).

Directions

1. Log in to the [COS console](#).
2. Click **Bucket List** on the left sidebar.
3. Locate the bucket for which you want to set CORS and click the bucket name to enter the bucket details page.
4. Select **Security Management > CORS (Cross-Origin Resource Sharing)** on the left sidebar and click **Add a Rule**.

CORS (Cross-Origin Resource Sharing) setting

Origin	Allow-Metho...	Allow-Headers	Expose-Head...	Max-age	Actions
Add rule					

[Learn more](#)

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

Add rules

Origin * `https://intl.cloud.tencent.com`

A line can contain at most one * wildcard character

Allow-Methods * ☒ PUT ☐ GET ☐ POST ☐ DELETE ☐ HEAD

Allow-Headers `*`

Expose-Headers `multi-line text input`

Max-age * `5`

Submit **Cancel**

Allow-Origin: The sources from which cross-origin requests are allowed. You can add domains and IP addresses. The domain name does not need to end with a slash (/).

More than one domain name can be specified, with one domain name per line.

You can set a `*`, indicating that all domains and IPs are supported, which is not recommended.

A single specific domain name is supported, such as `http://www.abc.com`.

Second-level wildcard domain names, for example, `http://*.abc.com`, are supported. Note that each line can contain only one asterisk (*).

Be careful not to omit the protocol name (http or https). If the port is not the default port 80, you need to add a port. An example IP address is `http://10.10.10.10`.

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

Allow-Headers: notifies 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, for example, `Content-Type`.

Header is easy to omit. Therefore, if there is no special requirement, you are advised to set this field to `*`, meaning that all headers are allowed.

Uppercase and lowercase letters [a-z, A-Z] are supported, and no underscores (_) are allowed.

Each header specified in `Access-Control-Request-Headers` must correspond to a value in `Allowed-Header`.

Expose-Headers: Request headers commonly used in COS. For more information, please see [Common Request Headers](#). Set this parameter according to the specific application requirements. ETag is recommended. Headers do not allow wildcards and are case insensitive. You can set multiple headers, with one header per line.

Max-age: validity period (in seconds) of the results obtained by OPTIONS. The value must be a positive integer, such as 600.


Return Vary: Origin: Set whether to return the `Vary: Origin` header. Enable this option if the browser has both CORS and non-CORS requests; otherwise, cross-origin access issues will occur.

Note:

If `Return Vary: Origin` is selected, browser access or CDN origin-pull requests may increase.

6. After configuration, click **Save** and you will see the CORS rule added. To modify it, click **Edit**.

CORS (Cross-Origin Resource Sharing) setting					
Origin	Allow-Metho...	Allow-Headers	Expose-Head...	Max-age	Actions
https://intl.cloud.tencent.com	PUT	*	-	5	Edit Delete
Add rule					

[Learn more](#) 

Setting Versioning

Last updated : 2024-01-06 14:59:34

Overview

Versioning enables you to store multiple versions of an object in a COS bucket, and extract, delete, or restore a specific version of an object. With versioning, you can recover data that is lost due to accidental deletion or application failures. This document describes how to enable versioning for a bucket via the console. For more information about versioning, see [Versioning Overview](#).

Note:

Once versioning is enabled for a bucket, it cannot return to the prior status (initial status). However, you can suspend versioning for the bucket. In this way, subsequent uploads of objects whose name already exists in the bucket will not generate multiple versions.

Once versioning is enabled, multiple versions will be generated for any uploaded object whose name already exists in the bucket. Each of these versions occupies your storage capacity and is billed for storage equally.

To permanently delete a historical version, specify an ID.

Directions

1. Log in to the [COS console](#).
2. Click **Bucket List** on the left sidebar.
3. Click the name of the bucket that you want to enable versioning for.
4. Click **Fault Tolerance and Disaster Recovery** > **Versioning**, set the status to **Enable**, and click **Save**.
5. In the pop-up window, click **OK**.

To disable versioning, set the status to **Disable**.

6. If you upload an object whose name already exists to a versioning-enabled bucket, you can click **List Historical Versions** on the **File List** page to view all historical versions uploaded at different time points. You can also perform multiple operations on the latest versions, historical versions, and delete marker versions.
7. You can **restore**, **download**, **view details about**, or **delete** a historical version of an object.

Note:

If you need to permanently delete a historical version via the console, go to the **File List** page of the bucket, click **List Historical Versions**, and delete the desired version of an object.

8. If you delete objects, there will be delete records, meaning that the deleted object will be preserved. You can delete or restore specified versions of objects as needed.

Upload Files

Create Folder

Incomplete multipart Upload

Clear Buckets

More Actions

List Historical Versions

Enter a prefix for searching

Refresh

Total 9 objects

1

<input type="checkbox"/>	Object Name	Size	Storage Class	modification time	Operation
<input type="checkbox"/>	doc/	-	-	-	Delete
<input type="checkbox"/>	examplefolder/	-	-	-	Delete
<input type="checkbox"/>	1.txt			2021-01-20 14:37:01	
<input type="checkbox"/>	2021-01-20 14:37:01 (Latest Version)	0B	STANDARD		Download Details Delete
<input type="checkbox"/>	2.txt			2021-01-20 14:36:45	
<input type="checkbox"/>	2021-01-20 14:36:45 (Latest Version)	0B	STANDARD		Download Details Delete
<input type="checkbox"/>	exampleobject.txt			2020-10-23 09:42:10	
<input type="checkbox"/>	2020-10-23 09:42:10 (Delete Marker)	-	-		Delete
<input type="checkbox"/>	2020-09-29 11:10:32	338.48KB	STANDARD		Download Details Delete

Setting Static Website

Last updated : 2024-01-06 14:59:34

Overview

You can configure a bucket to host a static website in the COS console and access the static website at the bucket's static website endpoint. For more information, see [Static Website Hosting](#).

Note:

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

For the static website configuration to take effect, you should use a static website endpoint instead of a COS default endpoint to access the COS origin server.

Prerequisites

You have created a bucket. For more information, see [Creating Bucket](#).

Directions

1. Log in to the [COS console](#).
2. Click **Bucket List** on the left sidebar.
3. Find the target bucket and click the bucket name to enter the bucket details page.
4. Click **Permission Management > Bucket ACL (Access Control List)** on the left sidebar, select **Public Read/Private Write** for **Public Permissions**, and save.

Bucket ACL(Access Control List)

Public Permissions ☐ Private (read-write) ☒ Public read & Private write ☐ Public (read-write)

User ACL

User Type	Account ID ⓘ	Permissions	Actions
Root account	10000*****	Full control	--
Add User			

SaveCancel

6. Set the configuration items of the static website.

The access nodes of the static website are case-sensitive. Note that the letter cases of the filename and suffix entered when you configure the **index file**, **error file**, and **redirect rule prefix match** must be the same as those of files in the bucket.

Notes:

Note:

Ignore .html Extension (optional): If the access path is "index", the "index.html" object is automatically matched and returned.

Index Document (required): Homepage of the static website. It is a page returned when the root directory or any subdirectory of a website is requested, which is usually named "index.html".

Note:

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

Error Document (optional): A page returned when an access error occurs. This configuration item allows you to define an error document. When the static website failed to respond to the user's requests, the specified custom error page will be returned. For example, if you have configured an error document named "error.html", the "error.html" page will be returned when an HTTP error occurs to guide the user. If no error document is configured, the default error message will be returned.

Note:

Only files in the bucket's root directory or subdirectories can be configured as error documents. Use browser-supported formats such as `.html` or `.htm`. If the file format (for example, `.zip`) is not supported, most browsers will display "inaccessible" or "access request denied".

Error Document Response Code (valid only when **Error Document** is set): It can be set to **Original error code** or **200** as the HTTP response code for the returned error document.

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 (such as 404). You can customize the error page. If a corresponding HTTP error is triggered, you can provide guidelines for your users on the error page.

Prefix matching: You can use a prefix matching rule to redirect requests to files or folders in the bucket. For more information, see [Static Website Hosting](#).

Note:

Prefix match does not support wildcards. If you want to redirect two folders prefixed with `index1/` and `index2/`, you cannot use `index*/` as the match rule; instead, you should create corresponding match rules separately.

7. After completing the configuration, click **Save**.

Setting Lifecycle

Last updated : 2024-01-06 14:59:34

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](#).

Note:

A lifecycle can be set to as long as 3,650 days.

Directions

1. Log in to the [COS console](#).
2. Click **Bucket List** on the left sidebar.
3. Locate the bucket for which you want to enable the lifecycle feature. Click the bucket name to enter its details page.
4. Click **Basic Configurations** > **Lifecycle** and click **Add a Rule**.
5. Add lifecycle rules as needed. The configuration items are described as follows:

Rule name: name of the lifecycle rule

Apply to: range of the lifecycle rule. The rule can apply to the whole bucket or a specified range. The range is described as follows:

Prefix: The lifecycle rule applies to objects with a specified prefix (e.g., prefix/).

Object Tag: The lifecycle rule applies to objects with a specified tag. You can set multiple tags (case-sensitive).

Note:

The object prefix and object tag can be specified at the same time. The relationships between object prefix and object tag and between object tags are "AND".

Managing the current version: transitions or deletes the current object version. Objects in your bucket can be transitioned from STANDARD to STANDARD_IA, ARCHIVE, or DEEP ARCHIVE, or deleted upon expiration. COS storage classes include **STANDARD**, **STANDARD_IA**, **INTELLIGENT TIERING**, **ARCHIVE**, and **DEEP ARCHIVE** (from hot storage to cold storage). You can transition objects only from a hot storage class to a colder one, not vice versa. The number of days is measured according to the time an object is modified, that is, if you modify an object, the days will be remeasured as if you uploaded the object again.

Note:

For buckets with multi-AZ configuration enabled, the lifecycle transition order can only be **MAZ_STANDARD** > **MAZ_STANDARD_IA** > **INTELLIGENT TIERING (MAZ)**.

Managing historical versions: you can transition or delete previous versions of an object using this option. If it is not enabled, only the latest version of an object is processed by default.

Remove Delete Markers from objects with no noncurrent versions: If the latest version of an object is a delete marker and all of its noncurrent versions have been deleted, the delete marker will also be deleted if you enable this option. Note that you cannot enable this option if you have selected the delete upon expiration option under **Managing the current version**.

Deleting incomplete multipart uploads: allows you to delete expired incomplete multipart uploads that have failed due to any reason.

6. Click **OK**.

7. To disable a lifecycle rule, click **Edit** and change the rule status to **Off**, or simply delete the rule.

8. To delete all lifecycle rules in the bucket, click **Clear all rules**.

Setting Logging

Last updated : 2024-01-06 14:59:34

Overview

COS introduces the Logging feature to record **bucket operation** requests, facilitating bucket usage and management. You can enable it in the COS console. For more information, see [Logging Overview](#).

Note:

Currently, COS offers the logging feature only in Beijing, Shanghai, Guangzhou, Nanjing, Chongqing, Chengdu, Hong Kong (China), Singapore, Seoul, Toronto, Silicon Valley, and Mumbai regions.

Currently, only the **bucket owner** has permission to set Logging, and other users cannot see the **Logging** configuration item in the console.

Logs are delivered once every 5 minutes and are not 100% accurate. Therefore, they are for reference only and cannot be used for usage measurement and billing.

Directions

1. Log in to the [COS console](#).
2. Click **Bucket List** on the left sidebar.
3. Click the source bucket that you want to enable Logging for.
4. On the left sidebar, select **Logging** > **Logging**, click **Edit**, and toggle on the feature.
5. Configure the configuration items of Logging as follows:

Logging

Status ☒

Destination Bucket

Target prefix

Log File Storage Path: examplebucket-1250000000/cos-access-log/{YYYY}/{MM}/{DD}/{time}_{random}_{index}.gz

Note that the path format of the log file generated in destination bucket is: {Destination bucket}/{Path prefix} {YYYY}/{MM}/{DD}/{time}_{random}_{index}.gz
For more information or help, please refer to [Learn more](#)

Destination Bucket: The **destination bucket** that stores the source bucket's logs must reside in the same region as the source bucket. We recommend you not set the source bucket itself as the destination bucket.

Path Prefix: A custom path prefix for the logs. If this field is left empty, logs will be delivered to the root directory of the destination bucket.

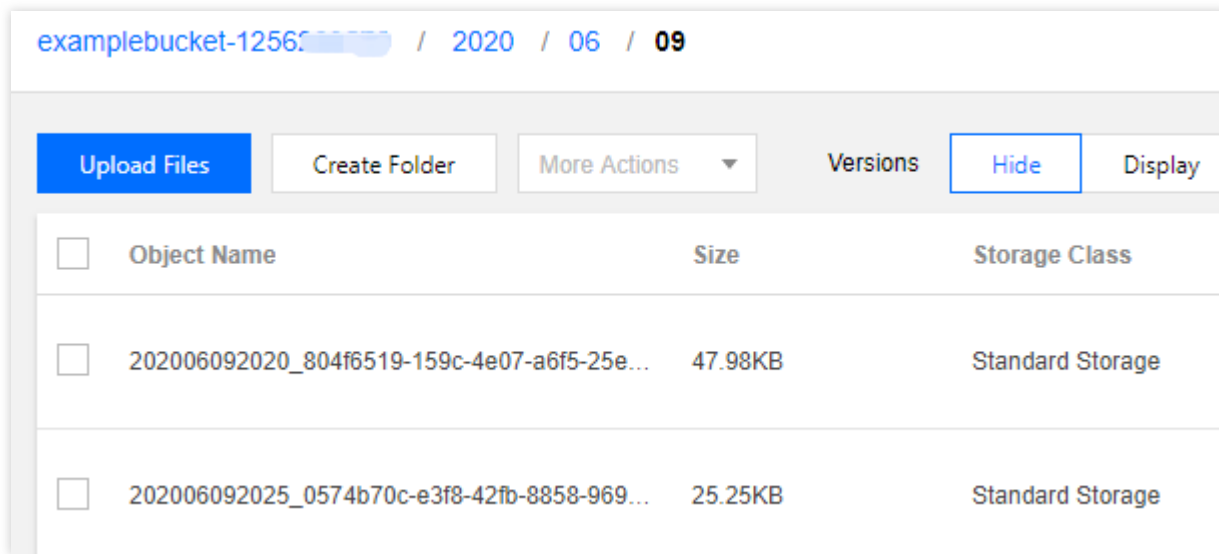
Service Authorization: CLS needs to be authorized to deliver logs to your bucket.

6. After confirming that everything is correct, click **Save**.

Note:

It takes several minutes or longer for the logs to be generated and delivered to the destination bucket.

7. Go to the destination bucket configured to view the generated logs.



8. After downloading the logs, you can view them in detail. For more information, see [Logging Overview](#).

Notes

1. To enable Logging, you need to create a log role in the CAM console and grant the role permissions to read/write logs of the source bucket.
2. If Logging is disabled yet the role is not deleted, the role's read/write permissions on the source bucket's logs still exist.

Accessing Bucket List Using Sub-Account

Last updated : 2024-01-06 14:59:34

Overview

Sub-accounts have no permissions to pull a bucket list by default. Therefore, if you log in to the [COS console](#) with a sub-account, you cannot access overview data, bucket list, or any other administration items that require permissions.

Sub-accounts can access a bucket list using the following two methods:

Adding an access path: this method applies to scenarios where a sub-account has permissions to operate on objects but no permissions to access a bucket list. The access path can be a **Bucket** or a **Path under the bucket**. Please make sure the added path is authorized.

Adding a preset policy: you can add a preset policy `QcloudCOSGetServiceAccess` with your root account for a sub-account to access a bucket list. This method also allows you to check the statistics overview in the console.

Note:

This feature applies to scenarios where a sub-account accesses a bucket list using the console.

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., Read or Write) to a bucket by the root account, a sub-account can then access this bucket by **adding an access path**.

Prerequisites

The sub-account has been granted user permissions on a bucket by the root account. For more information, see [Set Access Permission](#).

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/doc/exampleobject.txt`).
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.
4. Click **Objects** on the right, and you can see the object(s) to which the sub-account has been granted access.

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.

Note:

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.

1. Log in to the [CAM console](#) with the root account to enter the user list page.
2. Locate the sub-account to which you want to add a policy, and click **Grant Permission** on the right to enter the Associate Policies page.
3. Search for and add the preset policy [QcloudCOSGetServiceAccess](#) (i.e., the permission to access the bucket list in COS) in the policy list.
4. Click **OK**.
5. Click the sub-account name to enter its details page where you view the added policies. When you no longer need a policy, you can unbind it.

Note:

Now, you have successfully added a preset policy for the sub-account through the root account. Log in to the COS console with the sub-account, and you can check the bucket list and statistics overview.

Adding Bucket Policies

Last updated : 2024-01-06 14:59:34

Overview

You can add a policy for a bucket via the COS console to allow/deny access to specified COS resources from an account, IP, or IP range. For more information about bucket policy and examples, see [Access Policy Language Overview](#) and [Examples of Bucket Policies](#). The following describes how to add a bucket policy.

Note:

Each root account can create up to 1,000 bucket ACL rules.

Prerequisites

You have created a bucket. For more information, see [Creating a Bucket](#).

Directions

1. Log in to the [COS console](#).
2. Click **Bucket List** on the left sidebar.
3. Click the name of the target bucket to enter the configuration page.
4. On the left sidebar, click **Permission Management** > **Permission Policy Settings**. Then, you can add a bucket policy as detailed below. For more information about the configuration items, see [Access Policy Language Overview](#).

Visual Editor

Policy Syntax

On the **Visual Editor** tab page, click **Add Policy**. In the pop-up window, configure the policy in the following steps:

(1) Select a template

COS provides you with different templates depending on the combination of authorized users (grantees) and resource scope you choose to help you quickly configure bucket policies.

Grantee

All users (allow anonymous access): Select this option if you want to grant operation permissions to anonymous users. If you select this option, all users () will be automatically selected for you during policy configuration in step

2. Because it is risky to grant permissions on operations such as listing buckets (`ListBucket`) and configuring bucket configuration permissions to anonymous users, COS does not provide corresponding templates when this option is selected. You can add policies during policy configuration in step 2 if necessary.

Specified user: Select this option if you want to grant operation permissions to specified sub-accounts, root accounts, or cloud services. During policy configuration in step 2, you need to further specify the specific account UINs.

Note:

If **Grantee** is set as **Specified user**, an object request needs to carry a signature for identity verification. For more information on signature, see [Request Signature](#).

If **Grantee** is set as **All users (allow anonymous access)**, an object request doesn't need to carry a signature, and all users can directly access the object at the URL. However, your data may be leaked. Therefore, proceed with caution.

Resource Scope

The whole bucket: If you want to configure bucket configuration permissions or set the resource scope to the entire bucket, you can select this option to automatically add the entire bucket as a resource for you during policy configuration in step 2.

Specified directory: Select this option if you want to restrict the resource scope to a specified folder. During policy configuration in step 2, you need to further specify the specific directory. When this option is selected, COS does not provide policy templates related to bucket configuration, because for such permissions, the entire bucket must be specified as the resource.

Template: Collection of operations that you want to authorize.

Custom (no preset configuration): If you do not need to use a template, select this option and add policies as needed during policy configuration in step 2.

Other templates: COS provides you with different recommended templates depending on the combination of authorized users and resource scope you choose. After you select a template, COS automatically adds the corresponding operation permissions for you during policy configuration in step 2.

Note: If the authorized operations provided by the template do not meet your requirements, you can add or delete authorized operations during policy configuration in step 2.

Templates are described in the following table.

Grantee	Resource Scope	Policy Template	Description
All combinations		Custom	For any combination of authorized users and resource scopes, this template does not provide any preset policies. You can add policies during policy configuration in step 2.
All users (allow anonymous access)	The whole bucket	Read-Only objects (listing objects is not included)	For anonymous users, COS provides you with recommended templates for reading files (such as downloading files) and writing files (such as uploading and modifying files). COS's recommended templates do not list all objects in your bucket, and sensitive permissions, such as read and write permissions and bucket configuration permissions, are not allowed to improve
		Read/Write	

	Specified directory	objects (listing objects is not included)	data security. You can add or delete operation permissions during policy configuration in step 2 as needed.
		Read-Only objects (listing objects is not included)	
		Read/Write objects (listing objects is not included)	
Specified user	The whole bucket	Read-Only objects (listing objects is not included)	<p>COS provides the most recommended templates for the combination of **Specified user** and **The whole bucket**. In addition to reading, writing, and listing files, COS provides the following sensitive permission templates for trusted users:</p> <p>Read/Write buckets and object ACLs: get and modify buckets and object ACLs. Options include GetObjectACL, PutObjectACL, GetBucketACL, and PutBucketACL. General bucket configuration items: non-sensitive permissions such as bucket tagging, CORS, and origin-pull. Bucket sensitive configuration item: sensitive permissions such as bucket policies, bucket ACLs, and bucket deletion. Sensitive permissions should be used with caution.</p>
		Read-Only objects (listing objects is included)	
		Read/Write objects (listing objects is not included)	
		Read/Write objects (listing objects is included)	
		Read/Write buckets and object ACLs	
		General bucket	


		configuration items		
		Bucket sensitive configuration item		
	Specified directory	Read-Only objects (listing objects is not included)		For the combination of **Specified user** and **Specified directory** , COS provides you with recommended templates for reading files (such as downloading files) and writing files (such as uploading and modifying files), as well as recommended templates for listing objects. If you need to grant read, write, and list permissions to a specified folder to a specified user, this combination is recommended. You can add or delete operation permissions during policy configuration in step 2 as needed.
		Read-Only objects (listing objects is included)		
		Read/Write objects (listing objects is not included)		
		Read/Write objects (listing objects is included)		

(2) Configure the policy

Based on the combination of authorized users, specified directories, and templates you select in step 1, COS automatically adds operations, authorized users, and resources to the configuration policy for you. If you specify a user and a directory, you need to specify the user UIN and directory during policy configuration.

If the recommended templates provided by COS do not meet your requirements, you can add or delete authorized users, resources, and operations in this step. The configuration items are described as follows:

Effect: Select **Allow** or **Deny**, corresponding to **allow** or **deny** in the policy syntax.

User: Add or delete authorized users. Options include **Everyone** (), **Root account**, **Sub-account**, and **Cloud service**.

Resource: Add the whole bucket or a specific directory resource.

Operation: Add or delete authorized operations as needed.

Condition: You can specify conditions for permission authorization. For example, you can specify a user access IP.

(3) Confirm the configuration information

After confirming that the configuration information is correct, click **Finish**. In this way, if a sub-account logs in to the COS console, it can only access resources allowed by the policy.

(1) Click **Edit** to enter the user-defined policy syntax. COS provides policy syntax for various scenarios. For more information, see [Working with COS API Authorization Policies](#).

(2) Confirm that the policy syntax is correct and click **Save**. In this way, if a sub-account logs in to the COS console, it can only access resources allowed by the policy.

Setting Log Analysis

Last updated : 2024-01-06 14:59:34

Overview

If COS log storage is enabled, you can use the log analysis feature to further analyze the generated log files. This feature consolidates log files within a specified time range for statistical analysis and extracts key metrics for your reference.

Prerequisites

To use the log analysis feature, you need to [Enable COS Log Storage](#), and then create a log analysis function. For detailed instructions, see [Adding Log Analysis Function](#).

Directions

1. Log in to the [COS console](#).
2. Choose **Bucket List** on the left sidebar.
3. Click the bucket that requires log analysis.
4. On the left sidebar, select **Log Management > Logging**.

Note:

To use the log analysis feature, first enable log storage as instructed in [Setting Logging](#).

5. If you have added a COS log analysis function, click **Use Now** in the **COS Log Analysis** section. The system will check whether you have added log analysis function rules.

If you haven't added such a function, add one as instructed in [Adding Log Analysis Function](#).

6. Select a corresponding function and time range. Click **New Analysis Task** and configure the following information in the pop-up window:

Time Range: Period of logs you want to analyze, up to 30 days. Logs are retrieved according to **end time**. Logs in the specified time range cannot exceed 200 GB.

Cloud Function: Select a COS log analysis function added in the region where this bucket resides.

Product Destination Directory: After analysis, the output result will be zipped and saved to the directory you set. The output file contains **result file** and **inventory file**. **Result file** is based on the scenario you select. **Inventory file** refers to the log file list retrieved for this analysis.

Scenario: Scenario supported by this analysis.

Value of N: It must be a positive integer.

Task Description: Custom description.

7. Click **Confirm**.

You can perform the following operations on the created task:

Click **View Result** to view the result of this analysis task and where the result files are saved.

Note:

You can query log analysis tasks created in the last 3 days.

You can view the result only after a log analysis task is finished. A task takes a few to tens of minutes depending on the log size.

Click **Running Log** to go to the SCF console and view logs of COS log analysis.

Setting INTELLIGENT TIERING

Last updated : 2024-01-06 14:59:34

Overview

You can specify INTELLIGENT TIERING as the storage class of your objects to reduce storage costs. Then, COS automatically moves objects between two storage tiers (frequent access and infrequent access) when the data access pattern changes.

INTELLIGENT TIERING is ideal for data with unknown or changing access patterns. It offers the same low latency and high throughput as STANDARD while featuring lower costs. You can change the storage class of objects with uncertain access patterns from STANDARD to INTELLIGENT TIERING as needed to reduce your cloud storage costs.

For more information on INTELLIGENT TIERING and the supported regions, see [INTELLIGENT TIERING Overview](#).

Note:

Storage usage fees of INTELLIGENT TIERING are described as follows:

Storage fees for data in the frequent access tier are consistent with the published prices of STANDARD.

Storage fees for data in the infrequent access tier are consistent with the published prices of STANDARD_IA.

The request fees of INTELLIGENT TIERING are consistent with the published prices of STANDARD. The traffic fees, management feature fees, and supported regions are the same as those of other storage classes. INTELLIGENT TIERING also charges for object monitoring rather than data retrieval. For more information, see [Pricing | Cloud Object Storage](#).

Directions

1. Log in to the [COS console](#).
2. Click **Bucket List** on the left sidebar.
3. Find the target bucket and click the bucket name to enter the bucket details page.
4. Click **Basic Configurations** > **INTELLIGENT TIERING**, find the **INTELLIGENT TIERING** configuration item, click **Edit** to toggle it on, and set the configuration items as follows.

Conversion days: Specifies the time period to move objects to the infrequent access tier. The valid values are 30, 60, and 90. For example, if this parameter is set to 30, an object not accessed in 30 consecutive days will be moved from the frequent access tier to the infrequent access tier.

4. After confirming that everything is correct, click **Save**.

Note:

INTELLIGENT TIERING cannot be disabled or suspended once configured.

5. After enabling INTELLIGENT TIERING, click **File List** on the left sidebar.
6. On the **File List** page, click **Upload Files**.
7. In the pop-up window, select the file to be uploaded, click **Configure Parameters** to configure **Object Properties**, and set **Storage Class** to **INTELLIGENT TIERING**.
8. Click **Upload** to upload the object to the INTELLIGENT TIERING storage class. COS will move the object between storage tiers automatically. For more information on other configuration items, see [Uploading Object](#).

Setting Inventory

Last updated : 2024-01-24 14:39:14

Overview

You can enable inventory for your bucket in the [COS console](#). The inventory feature allows you to regularly (daily/weekly) publish inventory reports about the object attributes, configurations, and more. For more information about inventory, see [Inventory Overview](#). The following describes how to enable the inventory feature for a bucket. COS allows you to generate inventories on schedule or on the fly as needed.

Note:

You can configure multiple inventory jobs for a single bucket.

Inventory jobs do not directly read the object content during execution. Instead, they only scan the attribute information such as the object metadata.

Currently, the inventory feature is not available for Finance Cloud regions.

Prerequisites

You have created a bucket. For more information, see [Creating a Bucket](#).

Directions

Adding a scheduled inventory

1. Log in to the [COS console](#).
2. On the left sidebar, click **Bucket List**.
3. Click the name of the source bucket that you want to enable inventory for.
4. Select **Basic Configurations** > **Inventory** on the left and click **Add Inventory**.
5. On the **Configuration** page, you can configure the following items:

Basic information

Rule Status: Whether to enable this inventory rule. Valid values: **Enable**, **Disable**.

Inventory Name: Name of the inventory.

Destination Bucket: Bucket where the inventory is stored. Defaults to the source bucket. The destination bucket must be in the same region as the source bucket.

Report Prefix (Optional): Prefix selected for the destination bucket. The prefix can be used to group the inventory files in a public location. The default value is used initially.

Filter

Scope of the file: Select the scope of the inventory objects, which can be either the entire bucket or a subset of files with the same prefix. For example, to select all files under the 'doc' path in the 'folder' path of the bucket, specify the file prefix as `folder/doc`.

Object Version: Whether to include all object versions or only the current version in the inventory. If not set, only the current version will be included.

Filter Labels (optional): Lists objects with the same tag to the inventory. If this field is not set, no tag will be filtered.

Filter Time (Optional): Filters only objects modified after the specified time or within the specified period in the inventory. If not set, no time filter will be applied.

Custom Header Output (Optional): If you want the inventory report to include custom headers of objects, you can enter the required custom headers for output, which only supports x-cos-meta-* headers. If left blank, custom headers will not be output by default.

Inventory Information: Object information to be included in the inventory report. Options include object size, storage class, ETag, cross-bucket replication status, multipart upload status, last updated time, tag, and CRC-64. If not specified, all options will be selected.

Note:

`ETag` (entity tag) is the hash value of the object. It only reflects changes in the object content but not the object metadata. The value of `ETag` is not necessarily the MD5 checksum of the object. The value can be different if the uploaded object is encrypted.

The generated inventory contains the `Appid`, `Bucket`, `Key`, and `LastModifiedTime` fields by default. If versioning is enabled for the bucket, the generated inventory will also contain the `VersionId`, `IsLatest`, and `IsDeleteMarker` fields.

Output format

Output Format: The output inventory file is a CSV file compressed with GZIP.

Generate Lifecycle: Specifies whether to generate the inventory **Everyday** (default) or **Everyweek**. For example, an inventory added at 15:00 today will be generated and delivered to the destination bucket before 6:00 tomorrow in most cases. If you select to generate inventories by week, an inventory will be generated every 7 days. For example, if you enable inventory on September 1, then an inventory will be generated on September 2, 9, 16, and so on.

Inventory Encryption: whether to encrypt the inventory on the server. Options include:

None: The inventory is not encrypted (default).

SSE-COS: Encrypt the inventory report using server-side encryption with COS-managed key. For more information, see [SSE-COS Encryption](#) in the COS Developer Guide.

Access authorization: This field needs to be enabled to proceed with the next step. By default, this field is disabled.

Information confirmation

Confirm the bucket inventory configurations. If you need to change anything, click **Previous** and modify as needed.

6. Click **OK**. COS will generate inventory reports daily or weekly and deliver them to the destination bucket you set.

Note:

For more information about the format and content of the generated inventory reports, see [Inventory Overview](#).

Generating an instant inventory

1. Log in to the [COS console](#).
2. On the left sidebar, click **Bucket List** and then click the bucket (source bucket) that you want to enable inventory for.
3. Click **Basic Configurations > Inventory** on the left, select an inventory rule, and click **More-Generate list on the fly** on the right to generate an instant inventory.

Note:

To generate an instant inventory, click **More-Generate list on the fly** in the **Operation** column.

If you haven't configured inventory, you can configure one and then generate an instant inventory.

Domain Name Management

Overview

Last updated : 2024-01-06 14:59:34

Overview

After an object is uploaded to the bucket, COS will automatically generate a URL (i.e., default domain name) for you to access this object directly. To use CDN or your domain name to access COS objects, you can bind your domain or CDN to the bucket where the objects are stored.

You can set a domain name to access objects as needed. To accelerate access using CDN, you can access using the URL generated with the CDN acceleration domain name.

Description

You can quickly download and deliver objects in a bucket by managing the following domain names:

Default domain name: COS origin domain name, which is automatically generated based on the bucket name and region when you create a bucket.

Custom CDN acceleration domain name: you can bind for your bucket a custom domain name to Tencent Cloud Content Delivery Network (CDN), and access objects in your bucket using this domain name. (If you have enabled "User-defined domain name" in the legacy COS console, then the new console will continue to display "User-defined domain name" instead of "Custom CDN acceleration domain".)

Custom endpoint: Allows you to bind your own domain name as a custom endpoint to the bucket for access to the objects in it.

Note:

Currently, you must activate the CDN service to use a custom domain name in COS.

For content delivery in the Chinese mainland, ICP filing is required. You are not required to do so through Tencent Cloud though.

For content delivery outside the Chinese mainland, ICP filing is not required, but note that your data and operations in Tencent Cloud still need to comply with local laws and regulations as well as [General Service Level Agreements](#).

With CDN acceleration enabled for the custom CDN acceleration domain name, if the origin is a public-read bucket, the objects in the origin can be accessed via the custom CDN acceleration domain name. If the origin is a private-read bucket, we recommend you 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. If COS is used as the origin and origin-

pull authentication is enabled, the CDN edge node accesses the COS origin 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 accesses an edge node to acquire cached data, the edge node verifies the authentication field in the access URL based on the authentication configuration rules. This prevents unauthorized access and hotlinking, thereby improving the security and reliability of the data cached in the edge node.

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:

Bucket access permission	CDN origin-pull authentication	CDN authentication	Origin can be accessed via CDN acceleration domain name	Origin can be accessed via COS endpoint	Scenarios
Public read	Disabled	Disabled	Yes	Yes	Site-wide public access
Public read	Enabled	Disabled	Yes	Yes	Not recommended
Public read	Disabled	Enabled	URL authentication is required	Yes	Not recommended
Public read	Enabled	Enabled	URL authentication is required	Yes	Not recommended
Private read + CDN service authorization	Enabled	Enabled	URL authentication required	COS authentication required	Full-linkage protection
Private read + CDN service authorization	Disabled	Enabled	URL authentication is required	COS authentication is required	Not recommended
Private read + CDN service authorization	Enabled	Disabled	Yes	COS authentication is required	Origin protection
Private read + CDN service authorization	Disabled	Disabled	No	COS authentication is required	Not recommended
Private read	Disabled	Enabled or disabled	No	COS authentication	CDN is unavailable

				is required	
--	--	--	--	-------------	--

Note:

Take the first row in the above list as an example. If the origin bucket is public read, and neither CDN origin-pull authentication nor CDN authentication configuration is enabled, you can access CDN edge nodes and the origin bucket using the CDN domain name, and access the origin bucket using the COS domain name.

Origin protection is useful in cases where your data cached on CDN edge nodes may be maliciously pulled due to a lack of CDN authentication. Therefore, we strongly recommend you enable CDN authentication to mitigate data security issues.

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

More

[Enabling Custom Acceleration Domain Names](#)

[Enabling Custom Origin Domain Names](#)

[Granting a sub-account permissions to configure bucket acceleration domain names](#)

[Supporting HTTPS for Custom Endpoints](#)

Enabling Custom CDN Acceleration Domain Name

Last updated : 2024-01-06 14:59:34

Overview

This document only describes how to add a custom acceleration domain name and enable CDN acceleration in the COS console. For more information on how to add a custom domain name by using the CDN console, see [Adding Domain Names](#).

Directions

1. Log in to the [COS console](#). Click **Bucket List** on the left sidebar to open the Bucket List page.
2. Click the bucket you need to set a domain name to go to the bucket configuration page.
3. Click **Domains and Transfer** > **Custom CDN Acceleration Domain** on the left and click **Add Domain** to perform the configurations below.

Note:

If you have enabled **Custom Domain** in the previous console, you will see **Custom Domain** still displayed, with Custom CDN Acceleration Domain not displayed in the current console.

Domain Name: Enter the target custom domain name (such as `www.example.com`). Make sure that an ICP filing has been obtained and a CNAME record has been configured at the DNS service provider for the entered domain. For more information, see [CNAME Configuration](#). If the custom CDN acceleration domain you are connecting is in the following situations, you need to verify your domain ownership as instructed in [Domain Name Ownership Verification](#).

The domain name is being connected for the first time.

The domain name has been connected by another user.

The domain name is a wildcard domain name.

Acceleration Region: CDN acceleration is supported for regions in the Chinese mainland, outside the Chinese mainland, and globally, with global acceleration for buckets across all regions.

Origin Server Type: Select **Default Endpoint** or **Static Website Endpoint**. Select the first option unless your bucket has enabled static website. If you want to use your custom CDN acceleration domain name as static website, select **Static Website Endpoint** here and enable static website for your bucket.

Authentication: Enable origin-pull authentication. For private-read buckets, enable **Origin-pull Authentication** to protect the origin server.

Note:

For private-read buckets, if both origin-pull authentication and CDN service authorization are enabled, signature is not required for accessing the origin via CDN, and cached resources in CDN will be distributed on the public network, which will affect the data security. Therefore, we recommend you enable CDN authentication (Step 5).

Automatic CDN Cache Purge: After this feature is enabled, when a file in the COS bucket is updated, the CDN cache will be automatically purged. You can go to the **Function Service** section in the COS console to configure this feature as instructed in [Setting CDN Cache Purge](#).

HTTPS Certificate: To add an HTTPS certificate for the custom domain name, go to the [CDN console](#).

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

Note:

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

5. Log in to the [CDN console](#) and click **Domain Management** on the left sidebar.

6. Locate the domain name you need to configure and click **Manage** under **Operation** on the right to open the domain management page. Click **Access control** at the top, and then locate **Authentication Configuration**. For details, see [Instruction](#).

Enabling Custom Origin Server Domains

Last updated : 2024-01-06 14:59:34

Overview

This document describes how to bind a custom domain name to a bucket. You can access the files in the bucket via the custom domain name.

Note:

Up to 20 custom domain names can be added in the COS console. To add more, [contact us](#).

Directions

1. Log in to the [COS console](#).
2. Click **Bucket List** on the left sidebar.
3. Click the bucket for which you need to set a domain name to go to the bucket configuration page.
4. Click **Domains and Transfer** > **Custom Endpoint** on the left sidebar, click **Add Domain**, and configure the following items:

Domain Name: Enter the target custom domain name (such as `www.example.com`). Make sure that an ICP filing has been obtained, a DNS record has been added in the [Domains console](#), and a CNAME record has been configured at the DNS service provider for the entered domain name. For more information, see [CNAME Configuration](#). If the custom CDN acceleration domain you are connecting is in the following situations, you need to verify your domain ownership as instructed in [Domain Name Ownership Verification](#).

The domain name is being connected for the first time.

The domain name has been connected by another user.

The domain name is a wildcard domain name.

Origin Server Type: Select **Default Endpoint** or **Static Website Endpoint**. Select the first option unless your bucket has enabled static website. If you want to use your custom domain name as static website, select **Static Website Endpoint** here and enable static website for your bucket.

HTTPS Certificate: After the domain name is saved, you can choose to bind a certificate. For detailed instructions, see [Certificate Installation](#).

Note:

HTTPS certificate hosting for custom origin server domain names of COS is supported in public cloud regions in the Chinese mainland and in Singapore. If no HTTPS certificate is available for your domain name, click [Apply for Free Certificate](#).

HTTPS certificate hosting currently is not supported in other regions. If you need to use HTTPS certificates, see [Method 2](#).

Granting Sub-Account Permission to Configure Bucket Acceleration Domain Names

Last updated : 2024-01-06 14:59:34

Overview

On the **Domain Management Configuration** page of a COS bucket, you can configure the default CDN acceleration domain name, custom CDN acceleration domain name, and custom endpoint. Among them, the configurations of the first two are logically related to the CDN service. Therefore, if you want a sub-account to configure them, in addition to COS management permissions (to configure buckets, for example), you must also grant the sub-account relevant permissions of the **CDN service**.

To ensure the resource security, if you don't grant the **sub-account** relevant permissions of the CDN service, the **sub-account** will not be able to configure the default and custom CDN acceleration domain names for a COS bucket 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.

Default CDN Acceleration Domain

You have no access to bucket CDN Domain Management configurations. For more information, please refer to [Authorization Document](#)

Custom Acceleration Domain

You have no access to bucket CDN Domain Management configurations. For more information, please refer to [Authorization Document](#)

If you want the sub-account to properly configure such domain names, you need to authorize it in the [CAM console](#) by following the steps below:

Directions

1. Log in to the CAM console and go to the [Policies](#) page.
2. Click **Create Custom Policy > Create by Product Feature or Project Permission** to enter the **Configure Service Types** page.

Note:

The permissions can be configured by the **root account** by default. If you are using a sub-account and want to configure the permissions here, make sure 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`.

3. Enter your policy name (e.g., COS_DomainAccess), select **CDN** as the **Service Type**, and click **Next**.

4. Grant corresponding feature APIs to the sub-account based on your business needs.

Access to and configuration of the default and custom CDN acceleration domain names for a COS bucket involve five features: **querying domain name information, adding domain names, enabling/disabling domain names, deleting domain names, and modifying domain name configurations**. If you want the sub-account to have full access to the configurations of all domain names on the **Domain Management Configuration** page, toggle on all these features.

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

6. Associate features with objects. Select **Associate Objects > All (including resource objects purchased in the future)**, which **must** be selected to make the policy configuration fully effective.

7. Confirm that the permissions are correctly configured and click **Complete** to create the custom policy.

8. After the custom policy is created, switch to the [User List](#) page, and then associate the sub-account with the policy by clicking **Authorize** on the right.

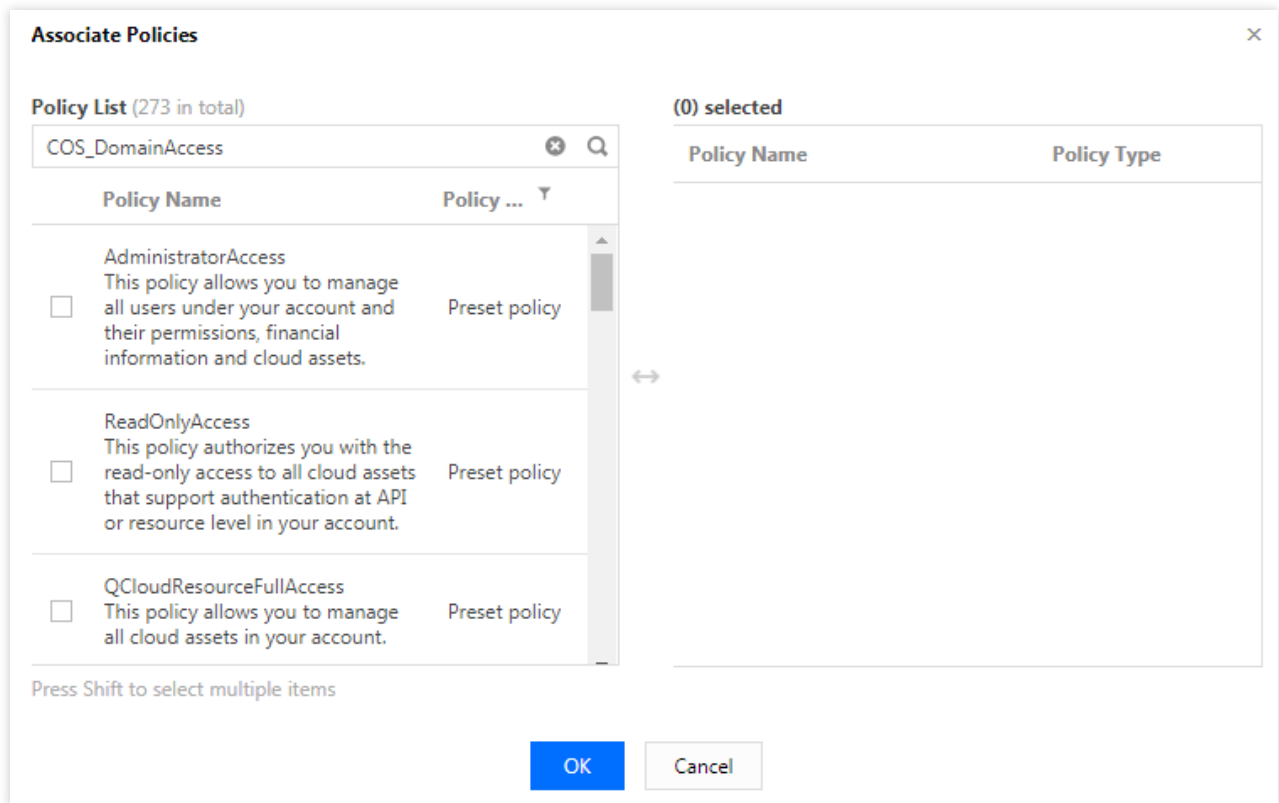
User

How to view more information?
CAM protects the security of your sensitive info. You can click the button [•] in the column [Details] to view more info of the user, such as identity security status, the group the user belongs to, and subscription. You can also click the username to view or edit in the User Info page.

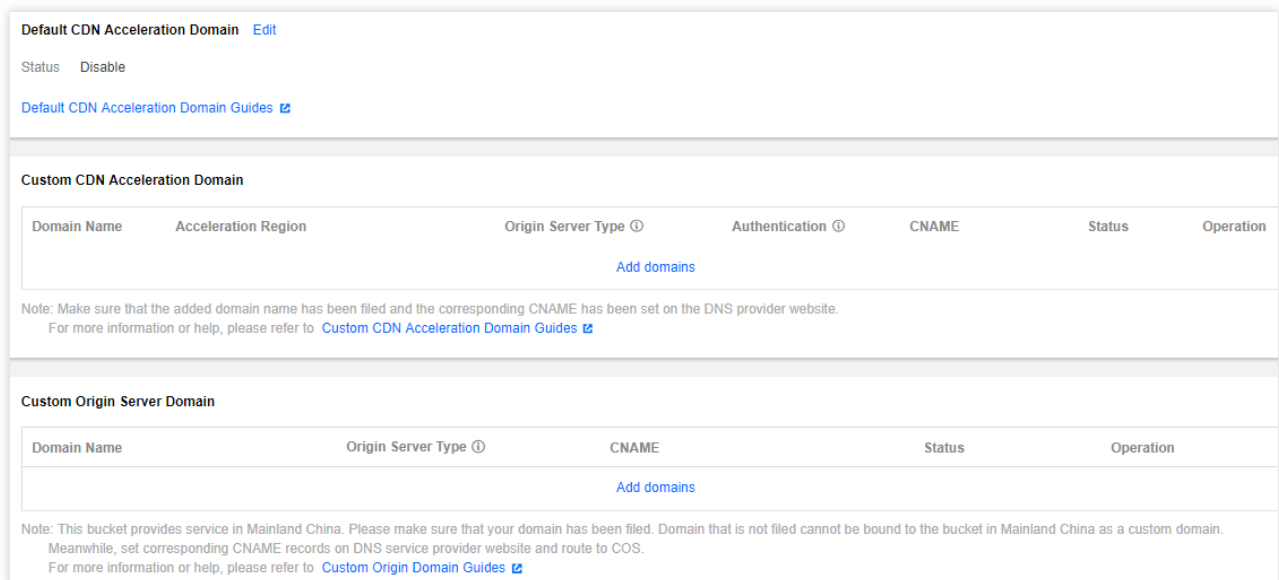
[Create User](#) [More](#)

<input type="checkbox"/>	Det...	User Name	User type	Account ID	Associated information	Operation
<input type="checkbox"/>	▶	Root Account	Root Account	1000		Authorize
<input type="checkbox"/>	▶	jason.read	Sub-user	1000	-	Authorize

9. In the **Associate Policy** pop-up window, search for and select the custom policy you just created and click **OK**.



10. After the policy is associated, the sub-account is authorized and can log in to the [COS console](#) to access and configure the default and custom CDN acceleration domain names for a COS bucket.



Setting Bucket Tags

Last updated : 2024-01-06 14:59:34

Overview

A bucket tag is a key-value pair (key = value), where the tag key and tag value are connected by an equal sign (=), for example, group = IT. It can be used to manage buckets in groups. You can set, query, and delete the tags for a specified bucket via the console.

Adding a Tag When Creating a Bucket

You can add a bucket tag when [creating a bucket](#), as shown in the following figure:

The screenshot shows the 'Create Bucket' dialog box with the 'Advanced optional configuration' step selected. The steps are: 1. Information, 2. Advanced optional configuration, and 3. Confirm.

Versioning ☐
 Keeping multiple versions of an object in the same bucket will incur storage usage fees. [Learn More](#)

Logging ☐
 Logging helps you log all kinds of requests for bucket operations. [Learn More](#)

Bucket Tag
 Enter a tag key Enter a tag value +
 You can also create 49 labels to manage buckets in groups by adding bucket labels. [Learn More](#)

Server-Side Encryption
 ☒ None ☐ SSE-COS ⓘ

[Previous](#) [Next](#)

Adding a Tag to an Existing Bucket

If you didn't add a tag when creating a bucket, you can perform the following steps to add a tag for your bucket:

1. On the [Bucket List](#) page, click the name of the desired bucket to enter the bucket configuration page.
2. Click **Basic Configurations** on the left, find the **Tagging** configuration item, and click **Add Tags**.

Tagging

Tag key ⓘ	Tag value ⓘ	Operation
exampletag	<input type="text" value="100"/>	Save Cancel
Add Tags		

The configuration items are described as follows:

Tag key: It is case-sensitive and can contain uppercase/lowercase letters, digits, and symbols (+, -, _, =, /, ., :, @).

Tag value: It is case-sensitive and can contain uppercase/lowercase letters, digits, and symbols (+, -, _, =, /, ., :, @).

Note:

Each bucket can have up to 50 different bucket tags.

`qcs:` and `project` are reserved fields. Therefore, do not use them in tag keys or tag values. For more limits, see [Bucket Tag Overview](#).

3. Enter the tag key and tag value. Then, click **Save**.

Setting Log Retrieval

Last updated : 2024-04-07 17:21:13

Overview

Log retrieval is also known as the real-time log function. Cloud Object Storage (COS) provides this function to record various bucket-related request logs and retrieve and analyze log data in real time. You can quickly enable this function for **buckets** in the COS console to retrace exceptional events and locate faults.

Note

To enable the real-time log function for a COS bucket, enable [Cloud Log Service](#).

When using the real-time log query function, you are charged by Cloud Log Service (CLS). For details about billing standards, see [Billing Overview](#).

Currently, the log retrieval function of COS is available in the regions, including Beijing, Guangzhou, Shanghai, Chengdu, Nanjing, Chongqing, Hong Kong (China), Silicon Valley, Singapore, Mumbai, Frankfurt, Toronto, Shenzhen Finance, and Shanghai Finance. This function will be available in more regions. Please stay tuned for product updates.

COS does not ensure the accuracy of log data. Log data is for reference only and cannot be used as a basis for measurement and billing.

Directions

Activating Log Retrieval

1. Log in to the [COS console](#).
2. On the left sidebar, click **Bucket List** to go to the bucket list page.
3. Locate the bucket for which you want to activate log retrieval, and click the bucket name to go to the management page.
4. In the left sidebar, choose **Logging > Log Retrieval**.
5. On the **Log Retrieval** page, if the real-time log function is not enabled for the current bucket, click **Activate Now**.

Note:

After the function is enabled, access logs of this bucket will be shipped to the log topic named cos-log-store in the same region of CLS. Authorization is required for the initial activation.

The real-time log function is not enabled for the current bucket

CLS provides real-time query of access logs and saves nearly 7 days of data by default. [Click to learn more](#)
CLS will create a log topic named cos-log-store for the logs in all buckets for each region. To edit or view log topics, go to [CLS Log subject page](#)
Use log query function will incur log service CLS product fee, click to know [Billing Description](#)

[Activate Now](#)

Activating Field-Based Statistical Analysis

Log retrieval enables you to perform quick statistical analysis based on fields without the need to enter query statements. For default supported fields, see [Log Fields](#). For more information, see [Quick Analysis](#).

Note:

If you want to perform statistical analysis on logs based on a specific field, enable statistics for that field in the following two ways.

Method 1: Enable Statistics on the Raw Logs Tab Page

1. Go to the **Raw logs** tab page.
2. Locate the target field and click **enable now**.

Raw logs Chart

Search

Showed Field

Raw logs

Hidden Field

- ☐ _SOURCE_
- ☐ _FILENAME_
- ☐ _HOSTNAME_
- ☐ _INDEX_STATUS_
- ☐ _CONTENT_
- ☐ eventVersion
- ☐ bucketName
- ☐ qcsRegion
- ☐ eventTime
- ☐ eventSource
- ☒ **eventName** [Show](#) [Statistics is not enabled for the field. Click to enable now](#)
- ☐ remotelp [Statistics is not enabled for the field](#)
- ☐ userSecretKeyId
- ☐ reqBytesSent

Log Count 0

14:20:00.000 14:22:00.000 14:24:00.000 14:26:00.000 14:28:00.000 14:30:00.000

[Original](#) Table ☐ Line Break ☒ Line No. ☒ Log Time ☐ Format JSON

Lin... **Log Time** ↓ Raw logs

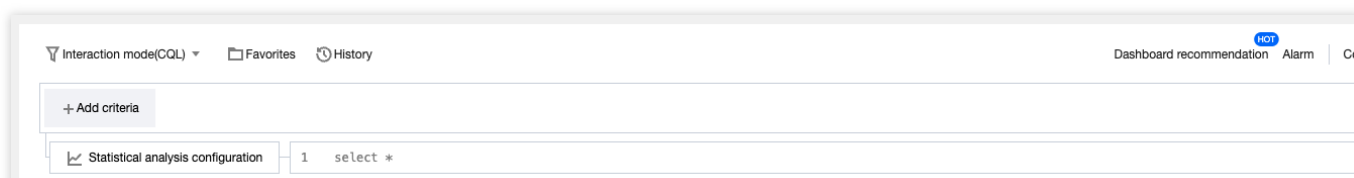
The current search result is empty

You can optimize the search results in the following ways

1. Check [Index Configuration](#). Index configuration is required for search and analysis via CLS.
2. Change time range to search
3. Optimize Query Syntax
 - Full text search: abc
 - Fuzzy search: abc*
 - Key-value search: info:abc

Method 2: Enable Statistics on the Index Configuration Page

1. Click **Index Configuration** to go to the index configuration page.



2. On the index configuration page, click **Edit** in the upper right corner, locate the target field, turn on the switch in **Enable Statistics** column, confirm the information, and click **OK**.

Index Configuration: cos-log-store

Key-Value Index



After it is enabled, key-value search is supported for logs. For example, you can enter "level:error" to search for logs where level is error. This feature will not incur additional traffic or storage fees during the full-text indexing period.

Case sensitive



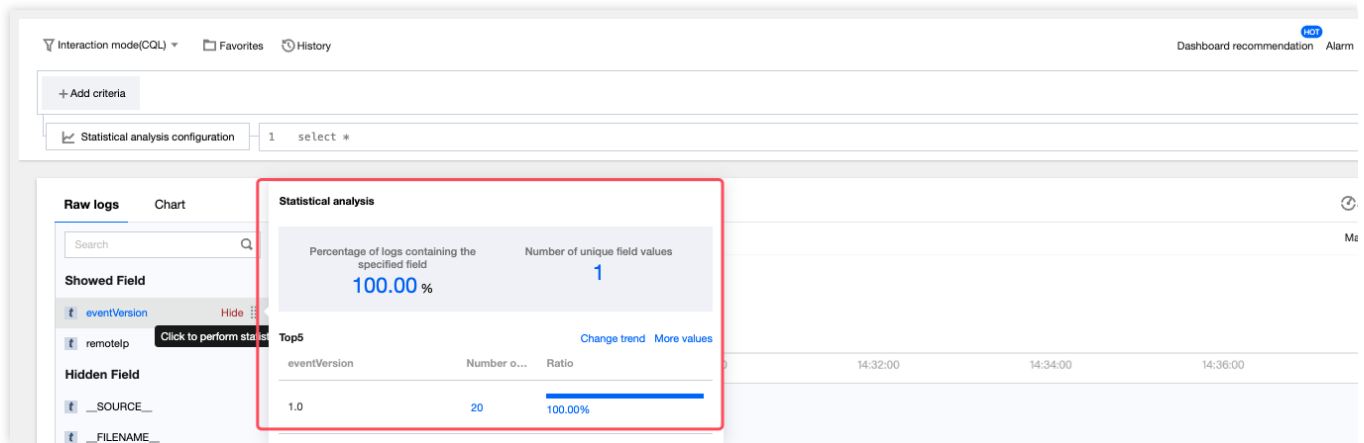
Auto Configure ⓘ

[Batch add fields](#)

Enter a

Field Name	Field Type ⓘ	Delimiter ⓘ	Allow Chinese ... ⓘ	Enable Statistics ⓘ
eventVersion	text ▼	Enter delimiter		
bucketName	text ▼	Enter delimiter		
qcsRegion	text ▼	Enter delimiter		
eventTime	text ▼	Enter delimiter		
eventSource	text ▼	Enter delimiter		
eventName	text ▼	Enter delimiter		
remotelp	text ▼	Enter delimiter		
userSecretKeyId	text ▼	Enter delimiter		

3. On the page that appears, view statistical analysis of the field. Click a number to automatically generate the corresponding retrieval and analysis statements and chart.



Entering Retrieval and Analysis Statements

Note:

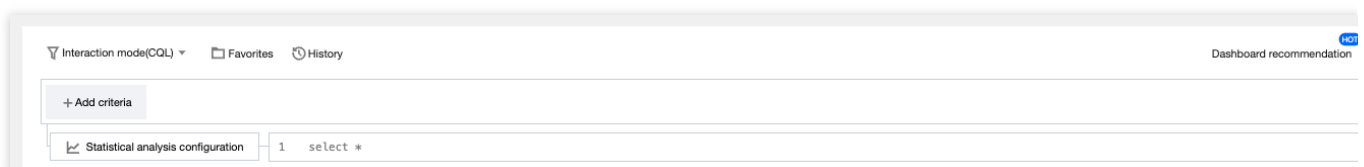
Index Configuration is a **necessary condition** for retrieval and analysis with CLS. You can perform retrieval and analysis on log data only when the index configuration function is enabled. Index configuration is complex, so it's recommended that you use the suggested configurations in [Modifying index configuration](#) to fulfill most use cases. For more information, see [Configuring Indexes](#).

For the prerequisites and user guide of retrieval and analysis statements, see [Syntax and Rules](#). For analysis methods of bucket access logs, see [COS Access Log Analysis](#).

A retrieval and analysis statement consists of **Criteria** and **SQL statements**. Enter the retrieval and analysis statement to retrieve and statistically analyze access logs.

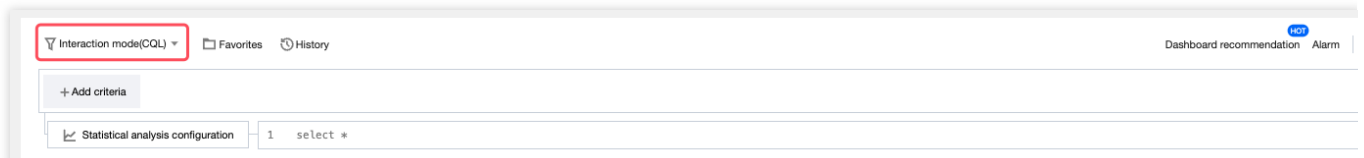
Criteria: Specify the conditions that the logs need to match, so that logs that meet the conditions are returned. For example, use `status:404` to retrieve application request logs with a response status code of 404. If the criteria are empty or `*`, all logs are displayed. For more information about syntax rules and examples, see [Syntax and Rules](#).

SQL statement: Statistically analyze logs that meet the criteria, so that the analysis results are returned. For example, use `status:404 | select count(*) as logCounts` to count the number of logs with a response status code of 404. For more information about syntax usage and examples, see [SQL Statement Syntax Rules](#).

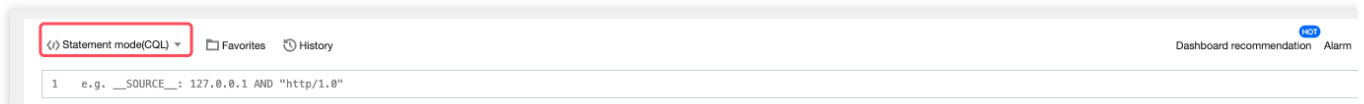


1. On the **Log Retrieval** page, select Interaction mode(CQL) or Statement mode(CQL) for retrieval and analysis statements.

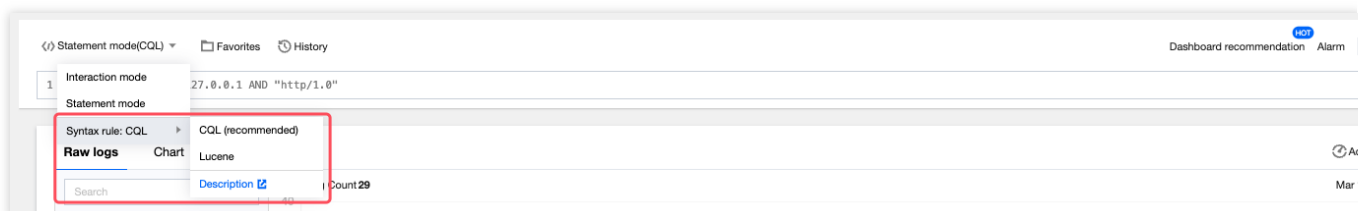
****Interaction mode(CQL)**:** In this mode, you can click specified retrieval criteria and statistical analysis rules to automatically generate retrieval and analysis statements. This mode is highly user-friendly.



****Statement mode(CQL)**:** In this mode, you can directly enter retrieval and analysis statements following the syntax rules. This mode is highly flexible.



2. Click the drop-down list to switch to Syntax rule: CQL. The options are CQL (recommended) and Lucene. For more information about syntax rules and examples, see [Search Condition Syntax Rules](#).



3. Enter the retrieval and analysis statement, select the time range, and click the **Search** button to retrieve the access logs reported by the bucket to CLS.

Viewing Log Retrieval and Statistical Analysis Results

After a successful retrieval, you can view the retrieval and statistical analysis results of access logs on the Log retrieval page. The results are respectively displayed on the **Raw logs** and **Chart** tab pages, which can be quickly switched. Details of the two tabs are as follows:

Raw logs: When a retrieval and analysis statement only contains criteria, you can view the logs matching the criteria on the Raw logs tab page. The logs are sorted by time in descending order.

Chart: When a retrieval and analysis statement contains SQL statements, you can view the analysis results on the Chart tab page and the logs matching the criteria on the Raw logs tab page. In this case, you can compare and analyze the statistical results and raw logs.

Raw Logs

Raw logs Chart

Search

Shown Field

- eventTime
- eventName

Hidden Field

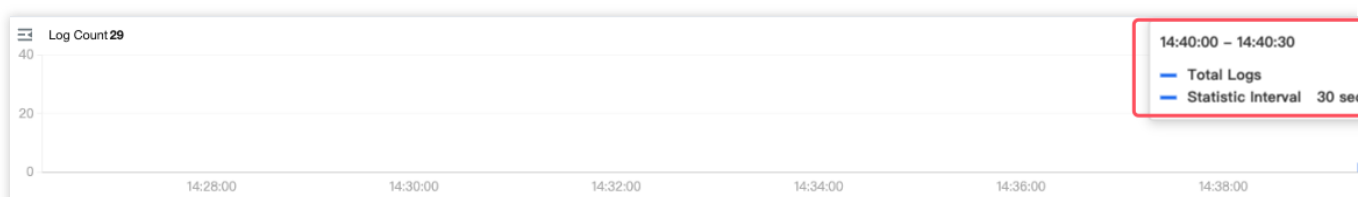
- __SOURCE__
- __FILENAME__
- __HOSTNAME__
- __INDEX_STATUS__
- bucketName
- qcsRegion
- eventSource
- userSecretKeyId
- reqBytesSent
- deltaDataSize
- reqPath
- reqMethod
- userAgent
- resHttpCode
- resErrorCode
- resErrorMsg
- resBytesSent

Log Count 29

Original Table ☐ Line Break ☒ Line No. ☒ Log Time ☐ Format JSON

Lin...	Log Time	Log Data
1	03-14 14:40:42.000	eventTime: 2024-03-14T06:40:42Z eventName: GETBucketlogginganalysis
2	03-14 14:40:35.000	eventTime: 2024-03-14T06:40:35Z eventName: GETBucket
3	03-14 14:40:34.000	eventTime: 2024-03-14T06:40:34Z eventName: ListMultipartUploads
4	03-14 14:40:34.000	eventTime: 2024-03-14T06:40:34Z eventName: GETBucketversioning
5	03-14 14:40:34.000	eventTime: 2024-03-14T06:40:34Z eventName: GETBucketreplication
6	03-14 14:40:24.000	eventTime: 2024-03-14T06:40:24Z eventName: GETBucketpolicy
7	03-14 14:40:23.000	eventTime: 2024-03-14T06:40:23Z eventName: GETBucketacl
8	03-14 14:40:19.000	eventTime: 2024-03-14T06:40:19Z eventName: GETBucket
9	03-14 14:40:18.000	eventTime: 2024-03-14T06:40:18Z eventName: ListMultipartUploads
10	03-14 14:40:18.000	eventTime: 2024-03-14T06:40:18Z eventName: GETBucketreplication
11	03-14 14:40:18.000	eventTime: 2024-03-14T06:40:18Z eventName: GETBucketversioning
12	03-14 14:40:11.000	eventTime: 2024-03-14T06:40:11Z eventName: GETObject

1.1 You can view the statistics information of logs within a specified time range under the current criteria in a bar chart.



1.2 By default, log data is displayed in original form. The display form can be customized.

Original Table ☐ Line Break ☒ Line No. ☒ Log Time ☐ Format JSON

Lin...	Log Time	Log Data
1	03-14 14:40:42.000	eventTime: 2024-03-14T06:40:42Z eventName: GETBucketlogginganalysis
2	03-14 14:40:35.000	eventTime: 2024-03-14T06:40:35Z eventName: GETBucket
3	03-14 14:40:34.000	eventTime: 2024-03-14T06:40:34Z eventName: ListMultipartUploads

1.3 Only the fields with **Show** next to them are displayed in the Log Data column. You can view or hide more fields associated with logs in the following three ways:

List Operation: In the left panel on the Raw logs tab page, locate the target field and click **Show** or **Hide** to complete the configuration.

Raw logs | **Chart** | [Add to dashboard](#)

Search | Log Count **29** | Mar 14, 2024 @ 14:26:1

Showed Field

- eventTime
- eventName

Hidden Field

- __SOURCE__
- __FILENAME__
- __HOSTNAME__
- __INDEX_STATUS__
- bucketName
- qcsRegion
- eventSource
- userSecretKeyId
- reqBytesSent
- deltaDataSize
- reqPath

Log Time: 14:28:00, 14:30:00, 14:32:00, 14:34:00, 14:36:00, 14:38:00

Log Data

Lin...	Log Time	eventTime	eventName
1	03-14 14:40:42.000	2024-03-14T06:40:42Z	GETBucketlogginganalysis
2	03-14 14:40:35.000	2024-03-14T06:40:35Z	GETBucket
3	03-14 14:40:34.000	2024-03-14T06:40:34Z	ListMultipartUploads
4	03-14 14:40:34.000	2024-03-14T06:40:34Z	GETBucketversioning
5	03-14 14:40:34.000	2024-03-14T06:40:34Z	GETBucketreplication
6	03-14 14:40:24.000	2024-03-14T06:40:24Z	GETBucketpolicy
7	03-14 14:40:23.000	2024-03-14T06:40:23Z	GETBucketacl

Log Details: Expand details of a log, and click the view icon to quickly hide or show a certain field. You can also view data of each log in JSON format and quickly copy the data. In addition, you can click a field value for custom redirection.

Original | Table | Line Break | Line No. | Log Time | Format JSON

Lin... | Log Time | Log Data

1 | 03-14 14:40:42.000 | eventTime: 2024-03-14T06:40:42Z | eventName: GETBucketlogginganalysis

Table | **JSON**

reqQcsSource

bucketName

referer

reqMethod

eventVersion

eventSource

range

deltaDataSize

storageClass

userSecretKeyId

qcsRegion

requestId

Copy

Add to Search | Open in New Tab

Exclude from Search | Open in New Tab

New Search | Open in New Tab

Custom redirect | +

You can redirect to the performance monitoring page or the specified URL.

Layout: Click "Layout: Default configuration" on the right, and select **Manage configuration**. You can show fields in batches, and click **Application** to complete the configuration.

Original | Table | Line Break | Line No. | Log Time | Format JSON

Lin... | Log Time | Log Data

1 | 03-14 14:40:42.000 | eventTime: 2024-03-14T06:40:42Z | eventName: GETBucketlogginganalysis

2 | 03-14 14:40:35.000 | eventTime: 2024-03-14T06:40:35Z | eventName: GETBucket

Layouts

Create

Default Configurati...

Configuration NameDefault Configuration

Sort byDescending by log timeAscending by log time

Field Setting ?

Select

Field

Line No.

Log Time

Context Search

__SOURCE__

__FILENAME__

__HOSTNAME__

Supports multiple selection by holding the Shift key, and the field display order is determined by the selection order.

Selected(2)

Field

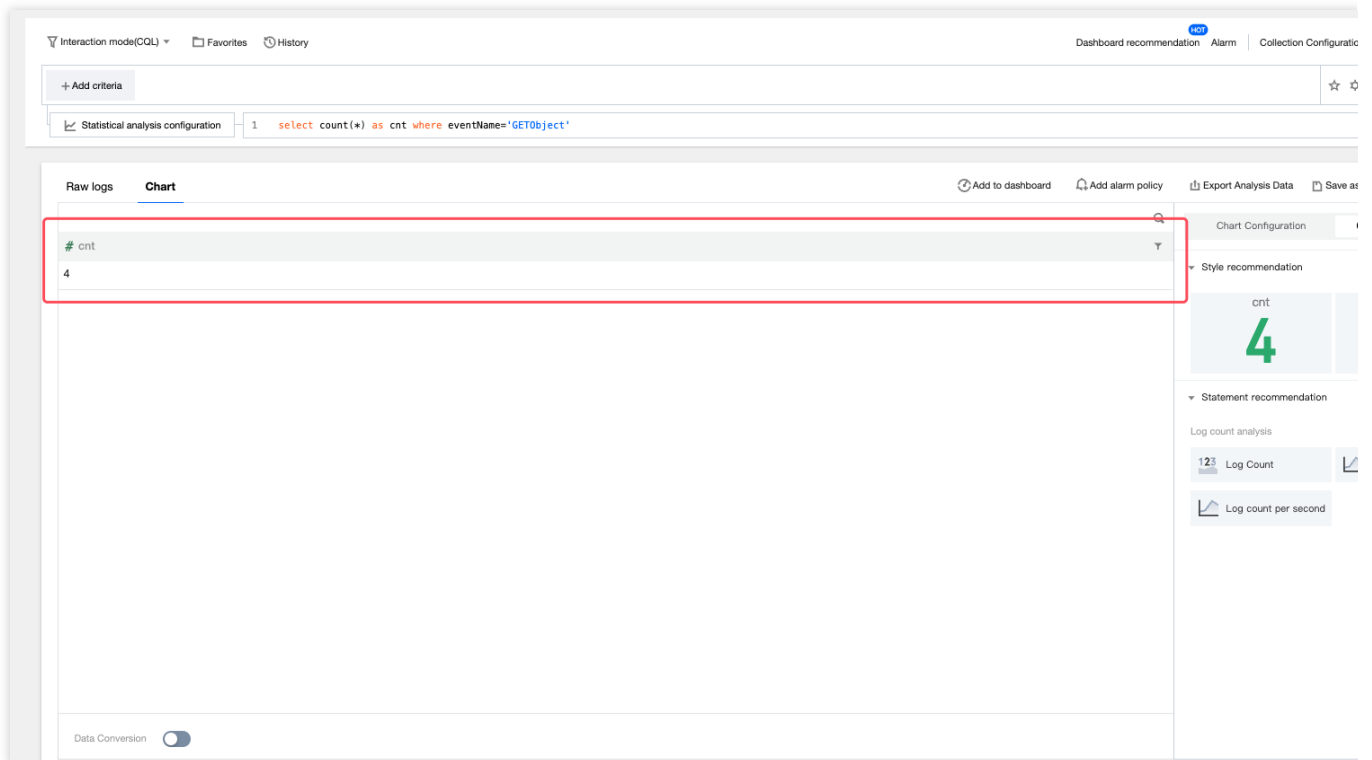
eventTime

eventName

ApplicationCancel

Chart

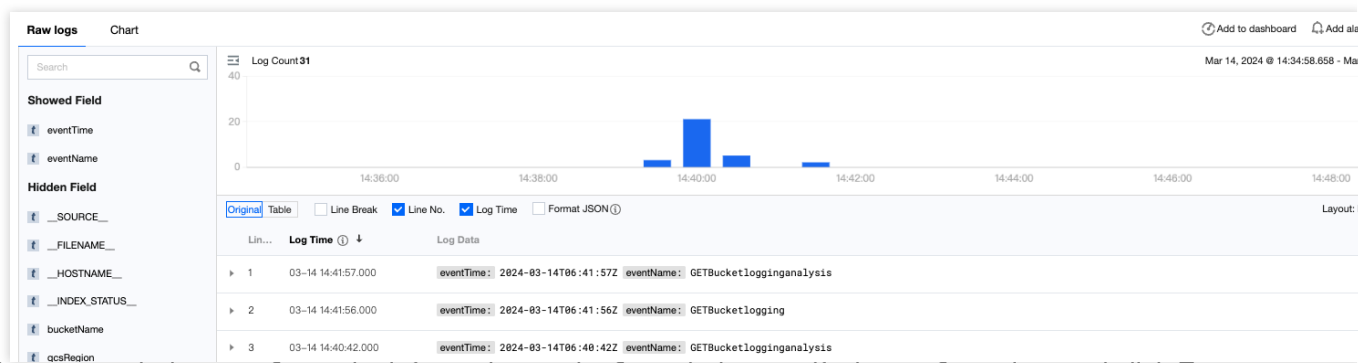
The Chart tab page shows analysis results in tables by default. You can customize the chart type and related information in **Chart Configuration** on the right. For further visualization and alarm configuration of bucket access logs, go to the [CLS console](#).



Downloading Logs and Exporting Analysis Results

Downloads Logs

1. Click **Download** on the right and select **Download Logs**.



2. In the popup window, configure the information on the figure below, verify the configuration, and click Export.

Download Logs

ⓘ

Log download consumes public network read traffic. For billing details, see [Product Pricing](#)

Time Range

2024-03-14 14:34:58.658 ~ 2024-03-14 14:49:58.658

Search Statement

*

Data Format

JSON

Log Sorting

☒ Descending (time)
☐ Ascending (time)

Log Quantity

☒ All (about 31 logs)
☐ Custom

Export

Cancel

3. In the Export Logs window where the new export task is displayed, view the current task progress, or delete or download the task. When the task is in the Waiting state, you can exit the window. Then you can click **Download** on the right and select **Export Logs** to enter the window again.

Back to Bucket List

Search menu item

Overview

File List

Basic Configurations

Security Management

Permission Management

Bucket ACL (Access Control List)

Permission Policy Settings

Associated CAM Policies

Domains and Transfer

Fault Tolerance and Disaster Recovery

Logging

Logging

Log Retrieval

Interaction mode (SQL)

Favorites

History

+ Add criteria

Statistical analysis configuration

1 select count(*) as cnt where eventName='GETObject'

Raw logs

Chart

Search

Shown Field

eventTime

eventName

Hidden Field

__SOURCE__

__FILENAME__

__HOSTNAME__

__INDEX_STATUS__

bucketName

qsRegion

eventSource

Export Logs

The exported logs will be retained for 3 days. Multiple export tasks will be executed in the order of their creation.

File Name/Task ID	Time Created	File Description	File Format	Status	Operation
export-3c1d7d5e-4acd...	2024-03-14 14:51:40	Time Range: 2024-03-14 14:34:58.658 ~ 2024-03-14 14:49:58.658 Search Statement: *	JSON	Waiting	Delete Download

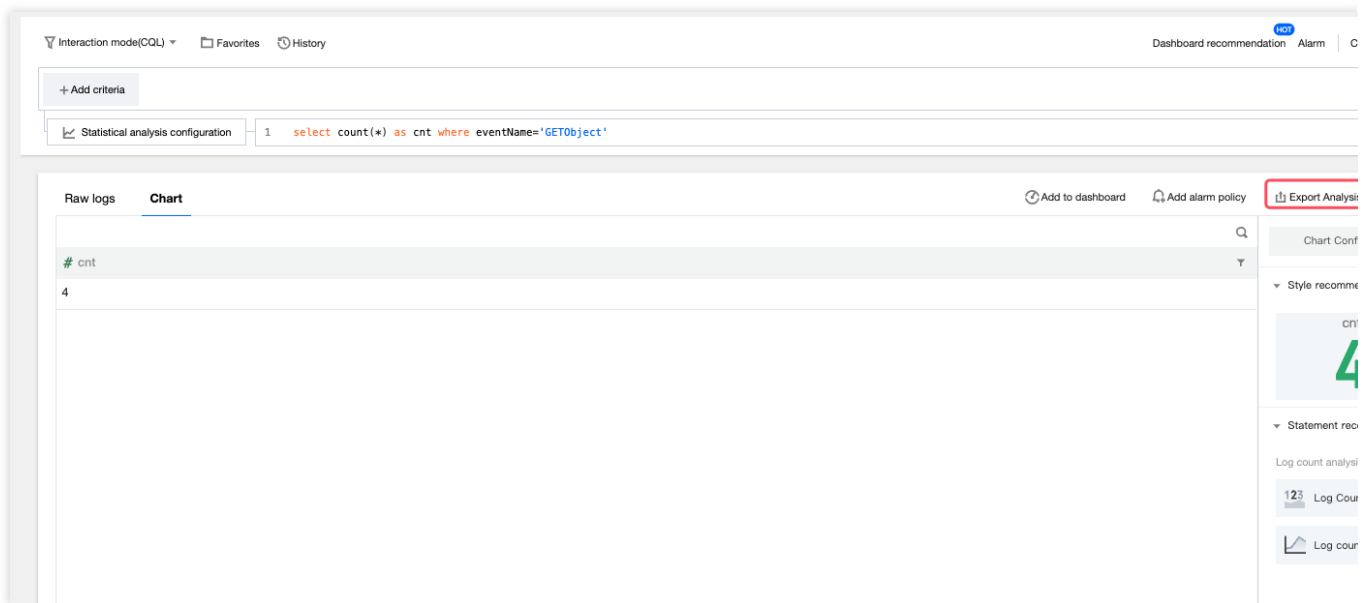
Total items: 1

10 / page

1 / 1 page

Exporting Analysis Data

Click **Export Analysis Data** on the right to download the analysis results to your local path.



Disabling Log Retrieval

If you do not want to use the log retrieval function for a bucket, disable the function.

Note:

Before disabling this function, go to the CLS console to check for empty log topics. If you do not delete them in time, extra charging will be incurred.

Log Field Description

Serial Number	Field Name	Description	Example
1	eventVersion	Record version	1.0
2	bucketName	Bucket name	examplebucket-1250000000
3	qcsRegion	Region for the request	ap-beijing
4	eventTime	Event time (end time of the request, which is a timestamp in UTC+0 time zone)	2018-12-01T11:02:33Z
5	eventSource	Domain	examplebucket-1250000000.cos.ap-

		name to be accessed	guangzhou.myqcloud.com
6	eventName	Event name	UploadPart
7	remoteIp	Source IP address	192.168.0.1
8	userSecretKeyId	Key ID for access	AKIDNYVCdoJQyGJ5brTf
9	reqBytesSent	Number of bytes in the request	83886080
10	deltaDataSize	Change in storage made by the request (in bytes)	808
11	reqPath	File path for the request	/folder/text.txt
12	reqMethod	Request method	put
13	userAgent	User agent (UA)	cos-go-sdk-v5.2.9
14	resHttpCode	HTTP return code	404
15	resErrorCode	Error code	NoSuchKey
16	resErrorMsg	Error message	The specified key does not exist.
17	resBytesSent	Number of bytes in the response	197
18	resTotalTime	Total time consumed for the request, which is the time between	4295

		the first byte of the request and the last byte of the response, in milliseconds	
19	logSourceType	Type of the log source	USER (user access request) and CDN (CDN origin-pull request)
20	storageClass	Storage class	STANDARD, STANDARD_IA, and ARCHIVE
21	accountId	Bucket owner ID	100000000001
22	requester	Requester account	The value is in the format of root account ID:sub-account ID. In case of an anonymous access, the value is shown as <code>-</code> .
23	requestId	Request ID	NWQ1ZjY4MTBfMjZiMjU4NjRfOWI1N180NDBiYTY=
24	objectSize	Object size, in bytes	808. If you use multipart upload, the objectSize field will be displayed only when the upload is completed. During the upload of each part, the field will be displayed as <code>-</code> .
25	versionId	Object version ID	Random string
26	targetStorageClass	Target storage type, which is recorded for any replication request	STANDARD, STANDARD_IA, and ARCHIVE
27	referer	HTTP referer of the request	<code>*.example.com</code> or <code>111.111.111.1</code>
28	requestUri	Request URI	"GET /fdgfdgsf%20/%E6%B5%AE%E7%82%B9%E6%95%B0 HTTP/1.1"
29	resTurnAroundTime	Time	4295

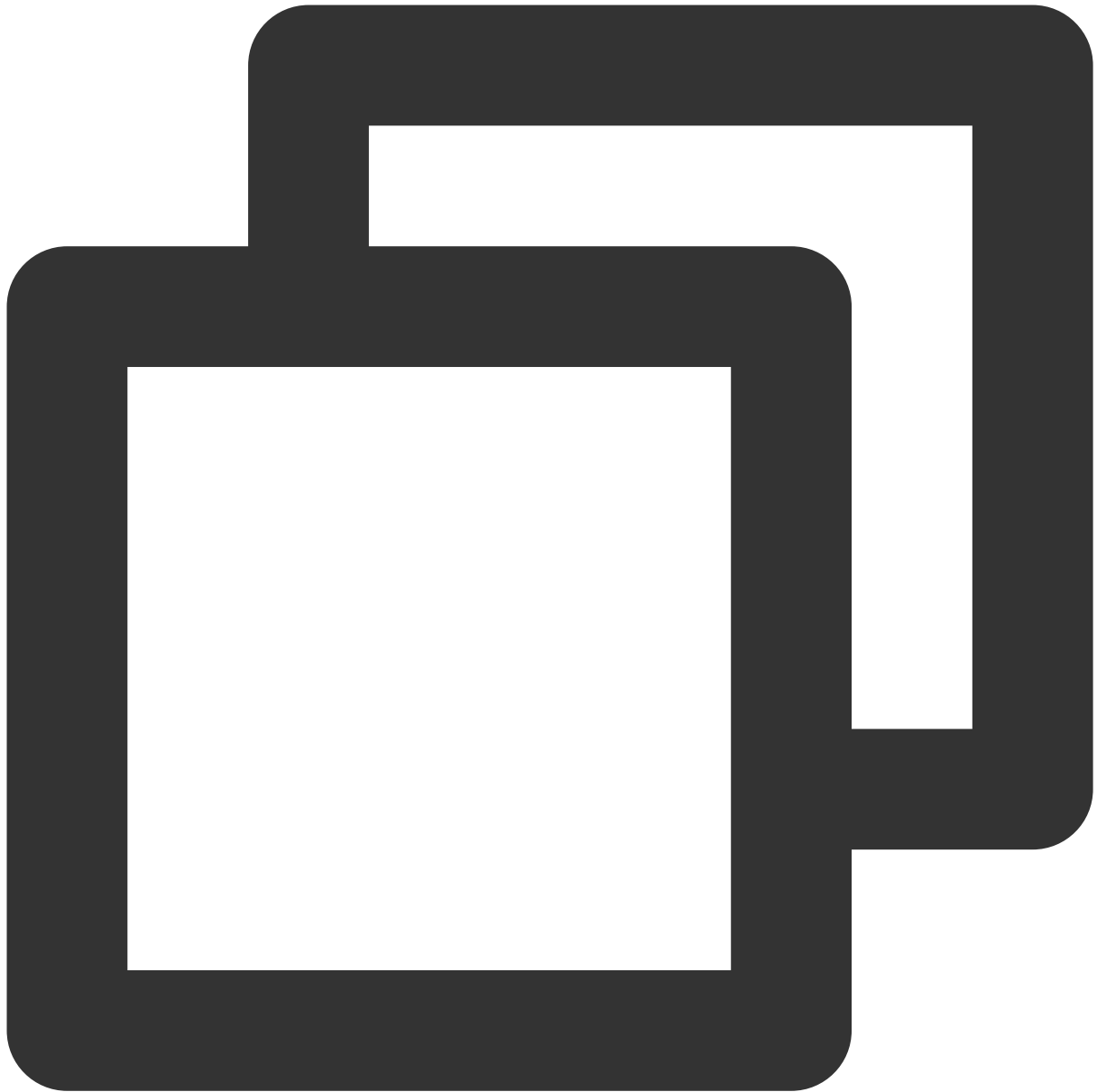
		consumed by the request server, which is the time between the last byte of the request and the first byte of the response, in milliseconds	
30	vpclId	VPC Request ID	"0": non-VPC; "12345": VPC, which is a non-zero string

Common Examples

A few commonly used examples are provided below. More cases will be added later. Please stay tuned for product updates. For more information, see [Examples](#).

Example 1: Top 50 IP Addresses by Traffic Volume

1. Select Statement mode(CQL) and enter the following SQL statement:



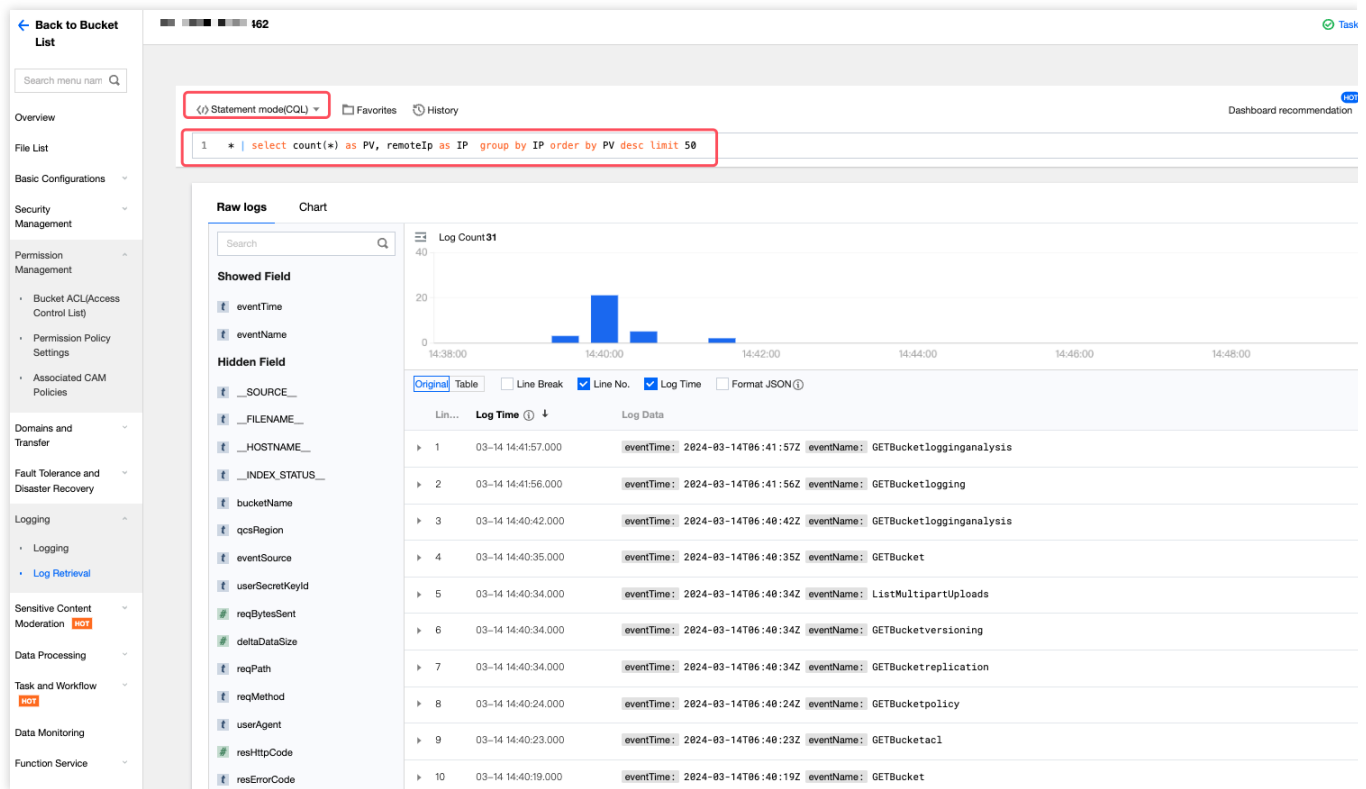
```
* | select count(*) as PV, remoteIp as IP group by IP order by PV desc limit 50
```

`count(*) as PV` : Counts all log entries, which is PV.

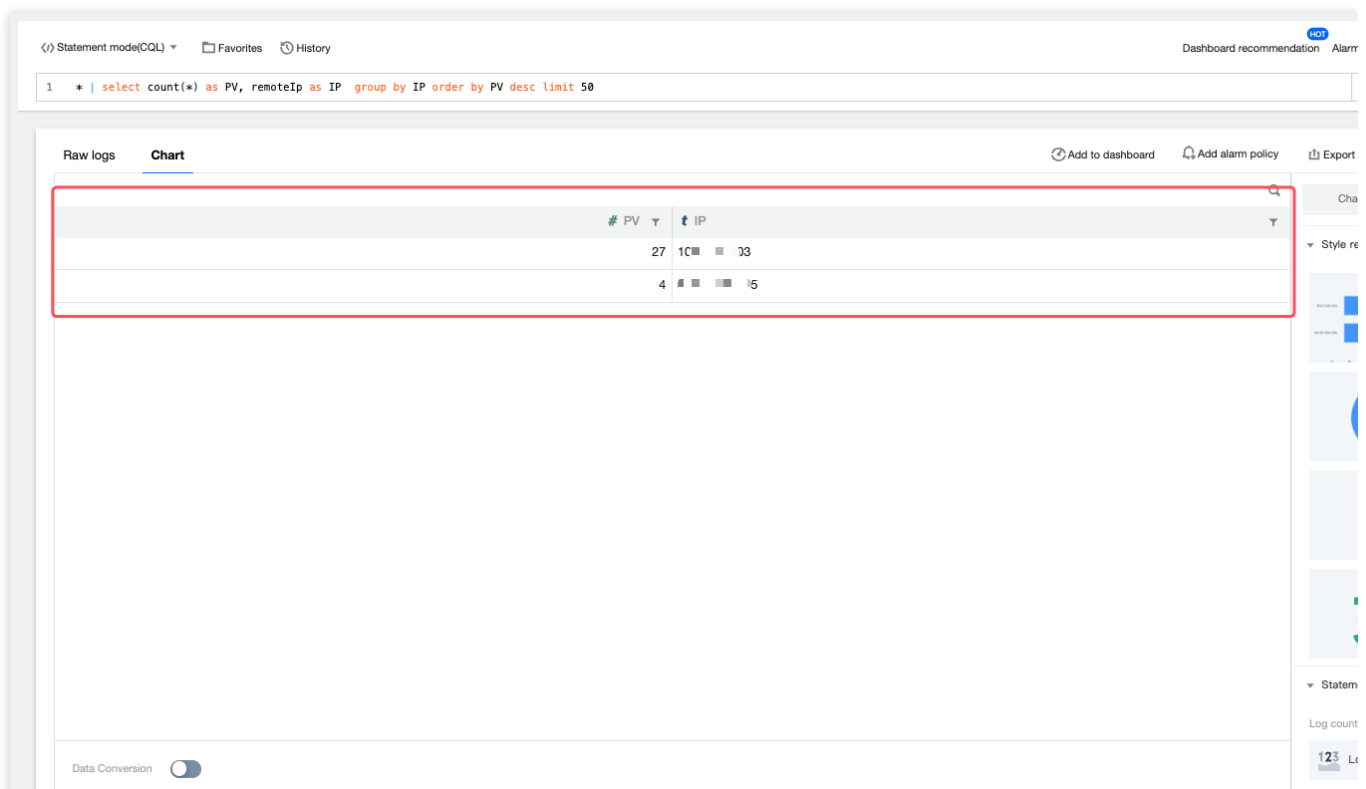
`group by IP` : Groups by IP, counting the PV for each IP.

`order by PV desc` : Sorts by PV in descending order, prioritizing IP addresses with high PVs.

`limit 50` : Only returns the top 50 query results, which are the IP addresses with the top 50 high PVs.



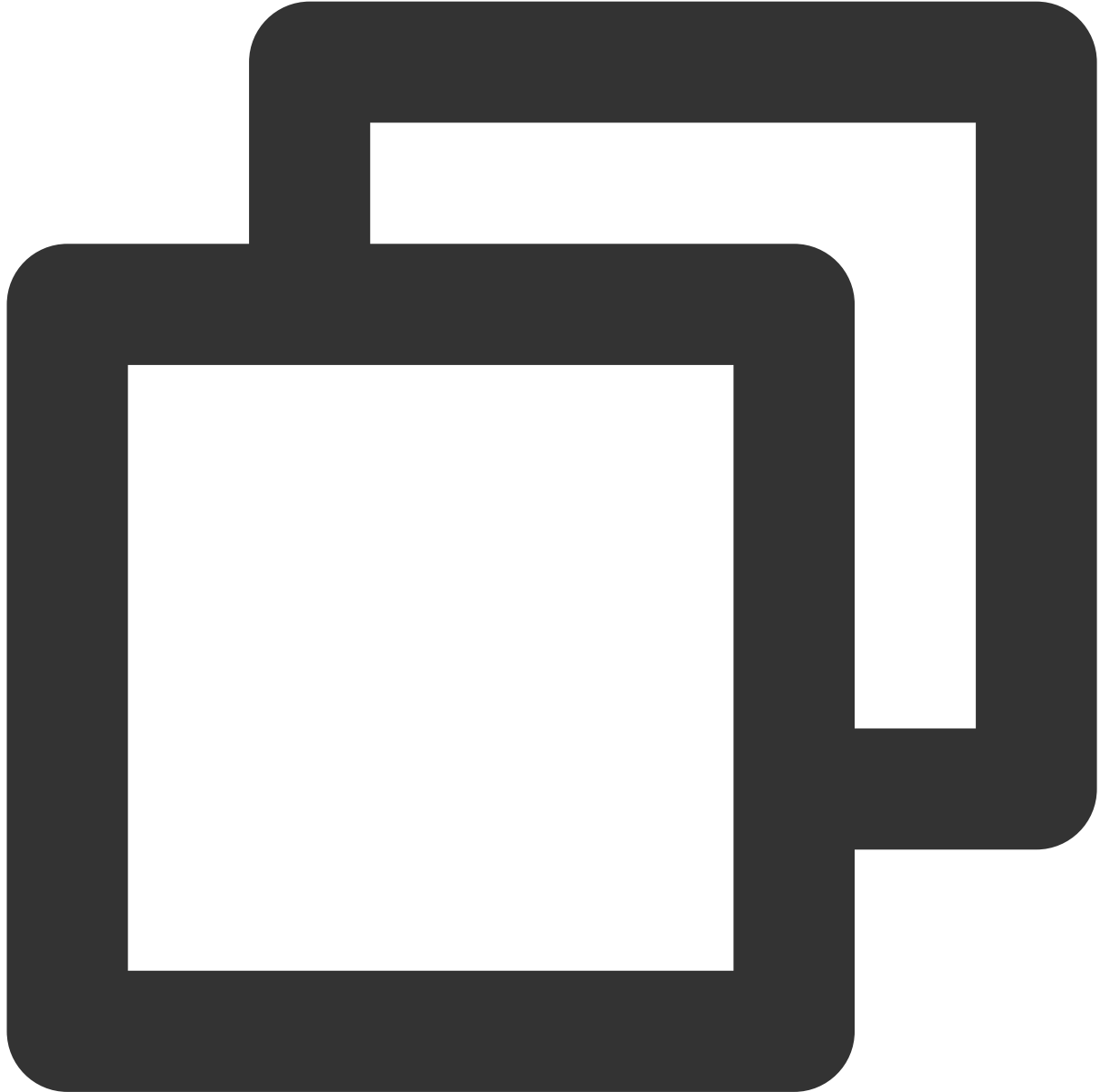
2. Select the time range and click **Search**. On the statistical analysis page, view the analysis results. You can switch chart types on the right side.



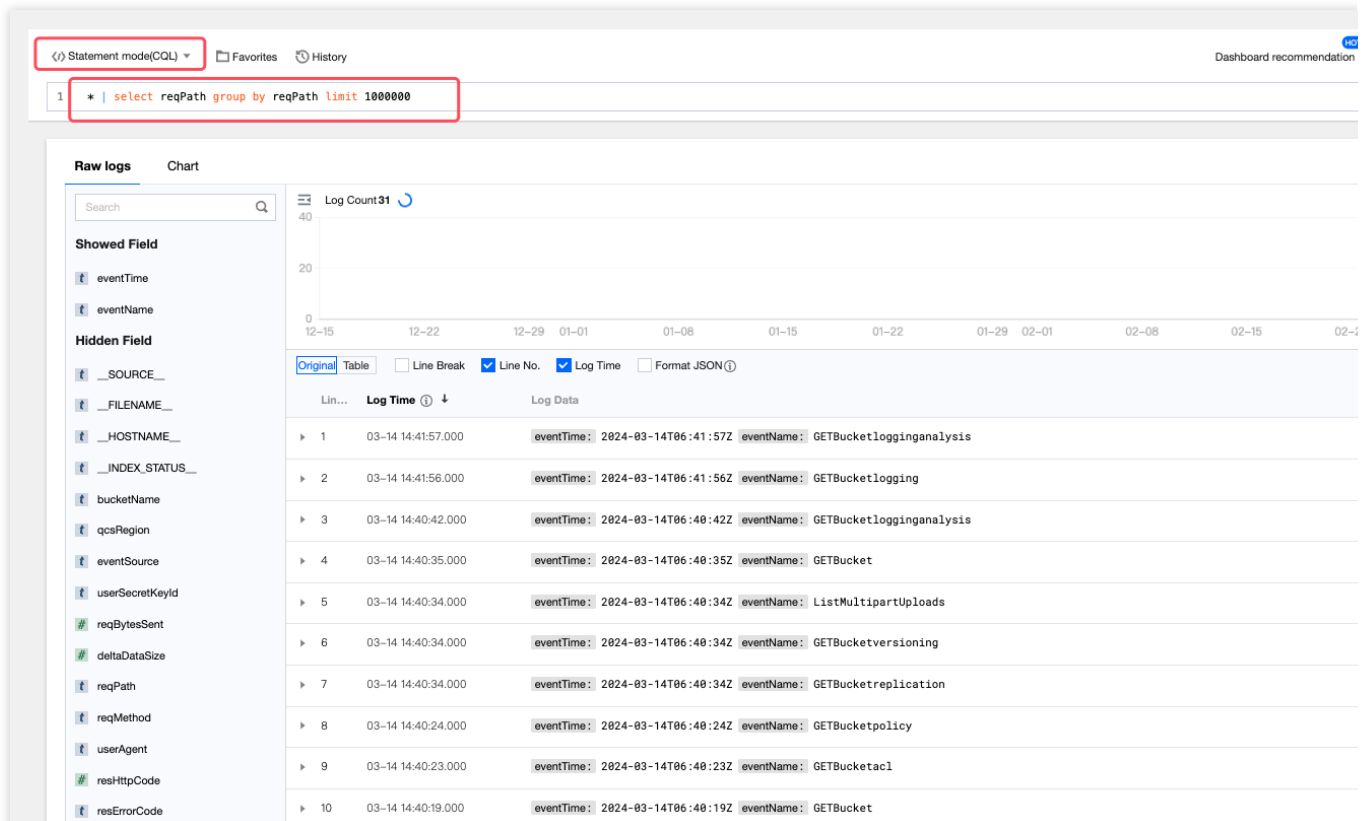
3. If the query statement fails to run, check the error location specified in the error message. For more information about error reasons, see [Search Analysis Error](#).

Example 2: Querying Files of Access Within Recent 90 Days

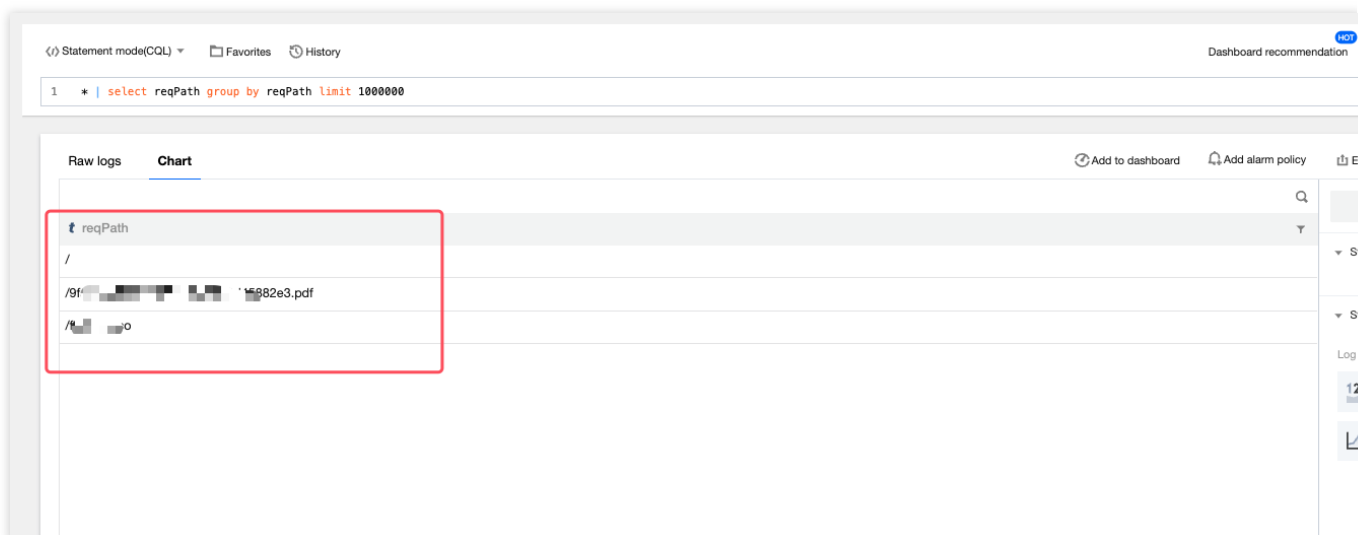
1. Select Statement mode(CQL) and enter the following SQL statement:



```
* | select reqPath group by reqPath limit 1000000
```

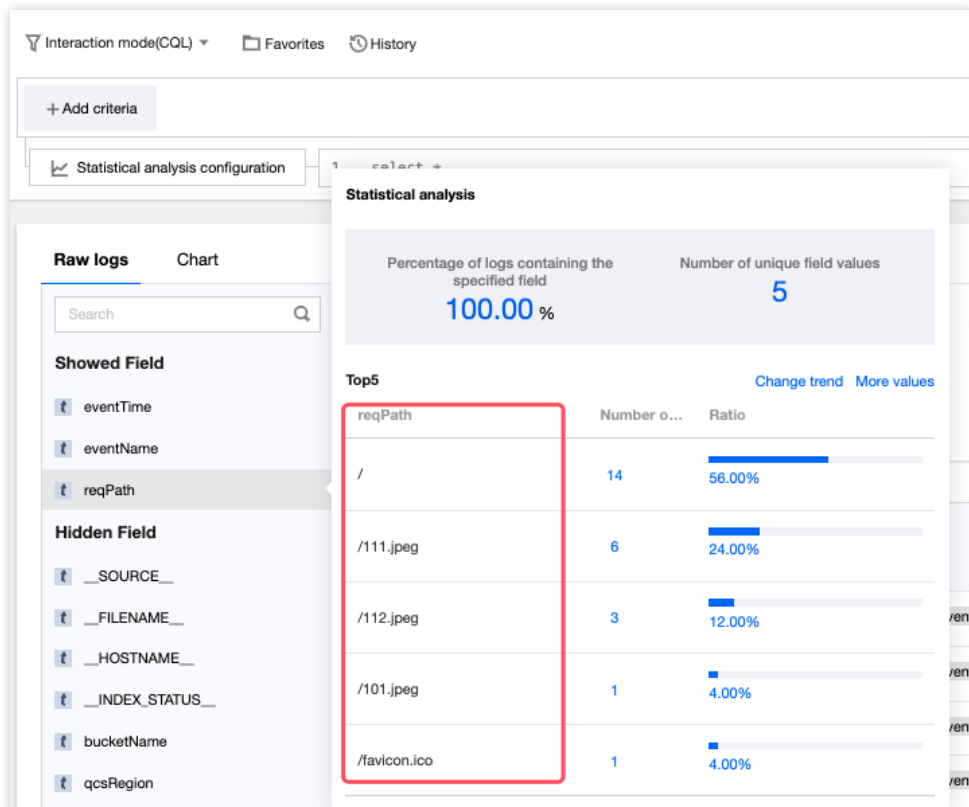


2. Set the time range to the recent 90 days and click **Search**. On the statistical analysis page, view the analysis results. You can switch chart types on the right side.



Example 3: Counting Requests, Traffic, and Storage for Specified Prefixes

For example, all the following files within the bucket generate log requests. You may desire to count the requests, traffic volume, and storage volume for objects prefixed with 1(that is, the objects with file paths "/111", "/112", and "/101").

**Note:**

Object traffic: Total number of object bytes returned for log requests.

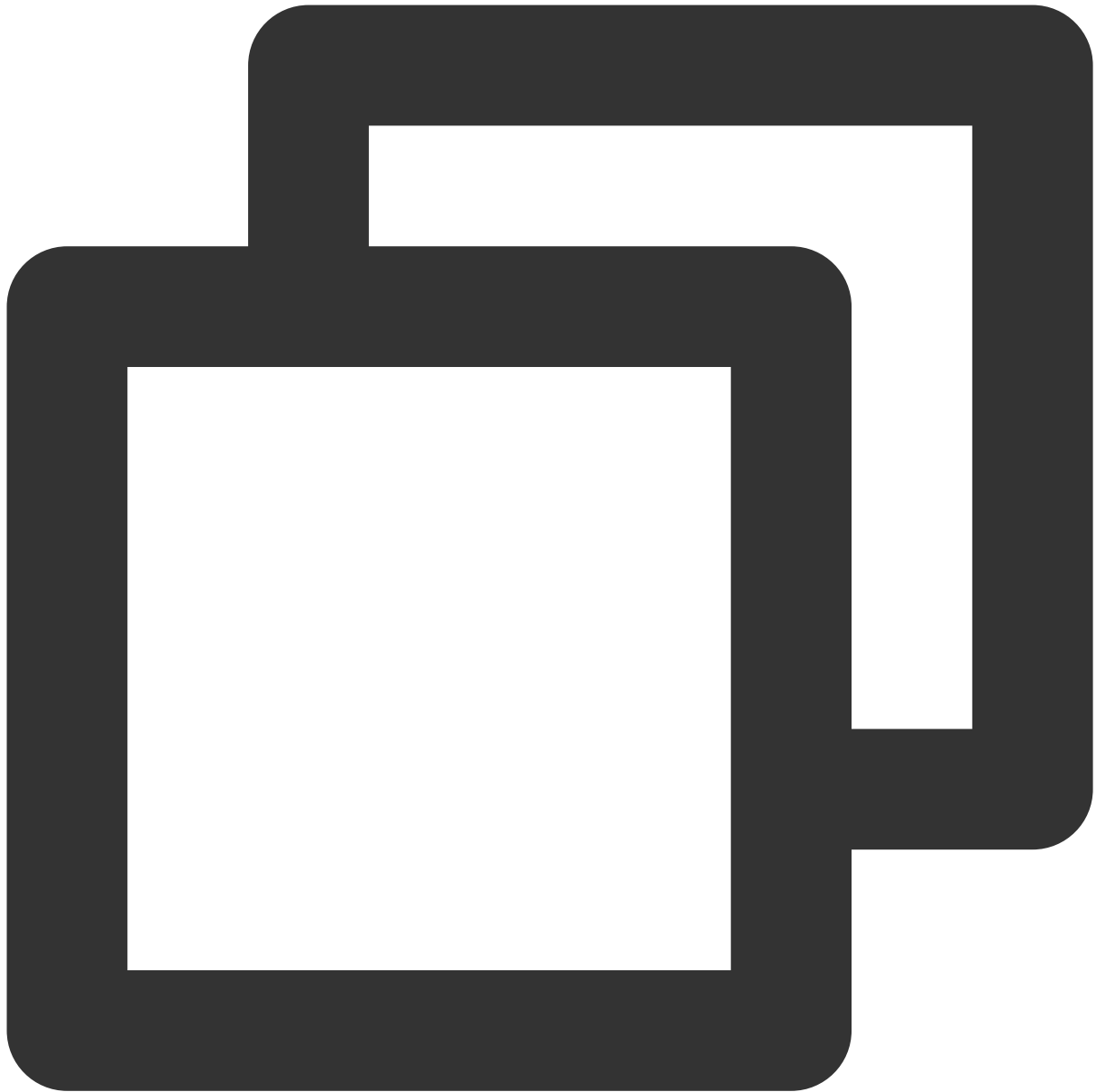
Object storage volume: Sum of object sizes (objectSize) in log requests, excluding "-". For more information, see [Log Field Description](#).

1. Select **Interaction mode(CQL)**, click **Add criteria**, specify **reqPath** to contain **/1**, and set the time range to filter object request logs prefixed with **1**, where **1** is a wildcard.

The screenshot shows the 'Add criteria' dialog box in the Tencent Cloud console. The dialog box has a search bar at the top. Below the search bar, there is a list of criteria on the left and a search results list on the right. The 'reqPath' criterion is selected in the list. The search results list shows paths like '/', '/111.jpeg', '/112.jpeg', '/101.jpeg', and '/favicon.ico'. The background shows a log table with columns for Time, eventName, and reqPath.

Time	eventName	reqPath
2024-03-14T06:59:08Z	GETObjectacl	/112.jpeg
2024-03-14T06:59:01Z	GETObject	/112.jpeg
2024-03-14T06:58:57Z	GETBucketreplication	/
2024-03-14T06:58:57Z	GETBucketversioning	/
2024-03-14T06:58:52Z	GETObject	/111.jpeg
2024-03-14T06:58:44Z	GETObject	/111.jpeg
2024-03-14T06:58:44Z	GETObject	/favicon.ico

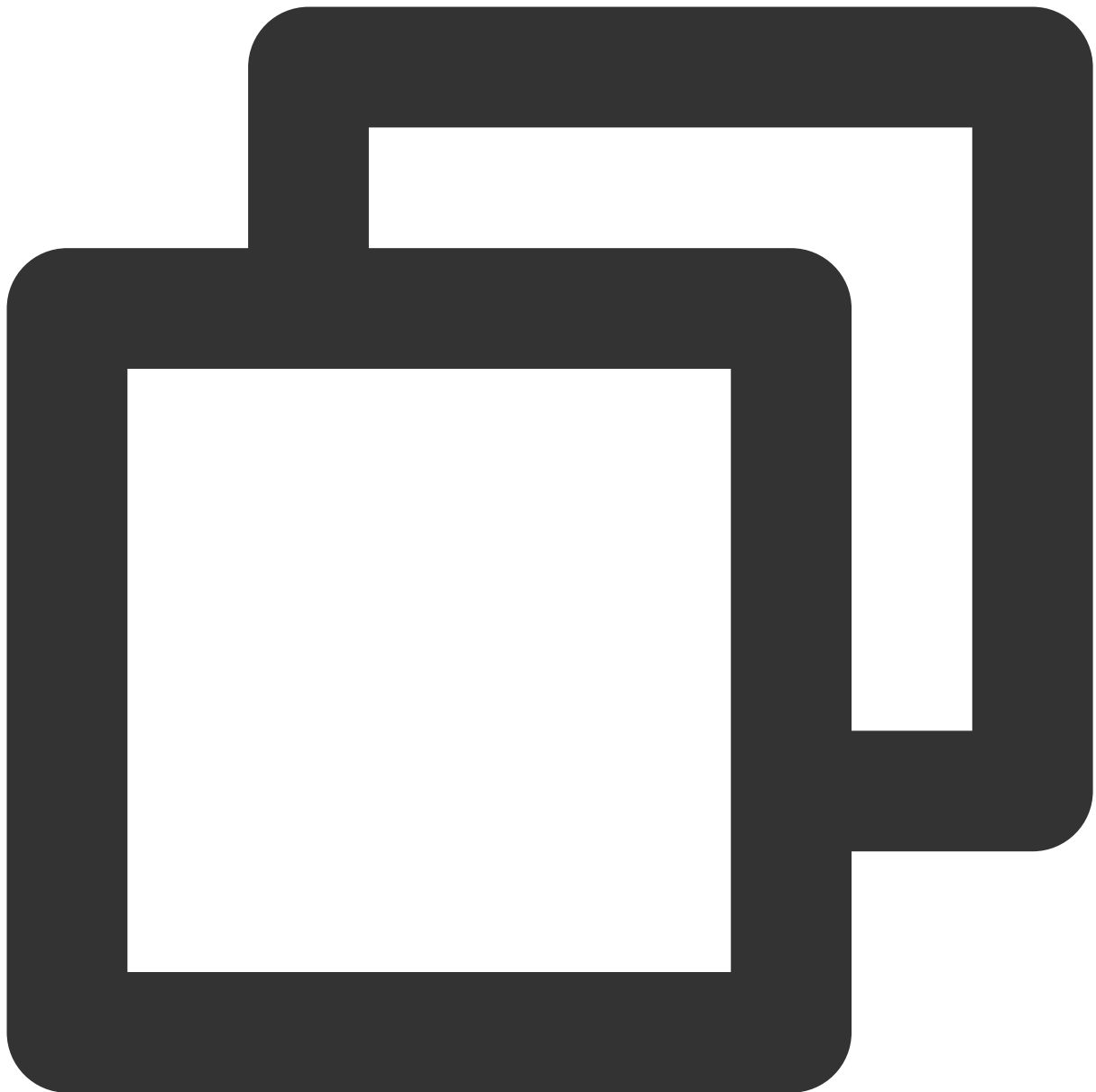
2. Enter the following statement in the input box:



```
SELECT count(*) as "Number of requests", sum(resBytesSent) as "Traffic volume", SUM
```



3. Alternatively, select **Statement mode(CQL)** in Step 1 and directly enter the following SQL statement:

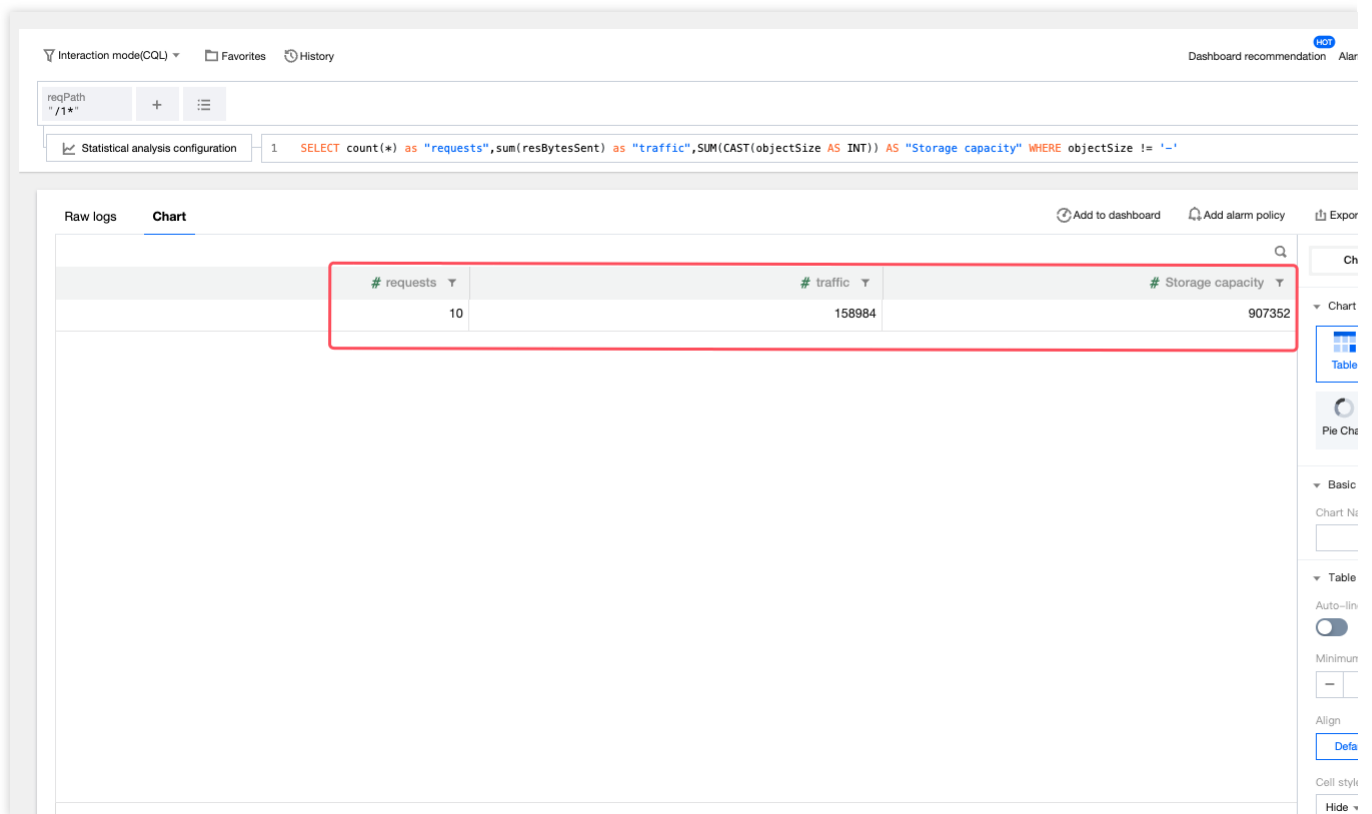


```
reqPath: "/1*" | SELECT count(*) as "Number of requests", sum(resBytesSent) as "Traf
```

Statement mode(CQL) ▾ Favorites History

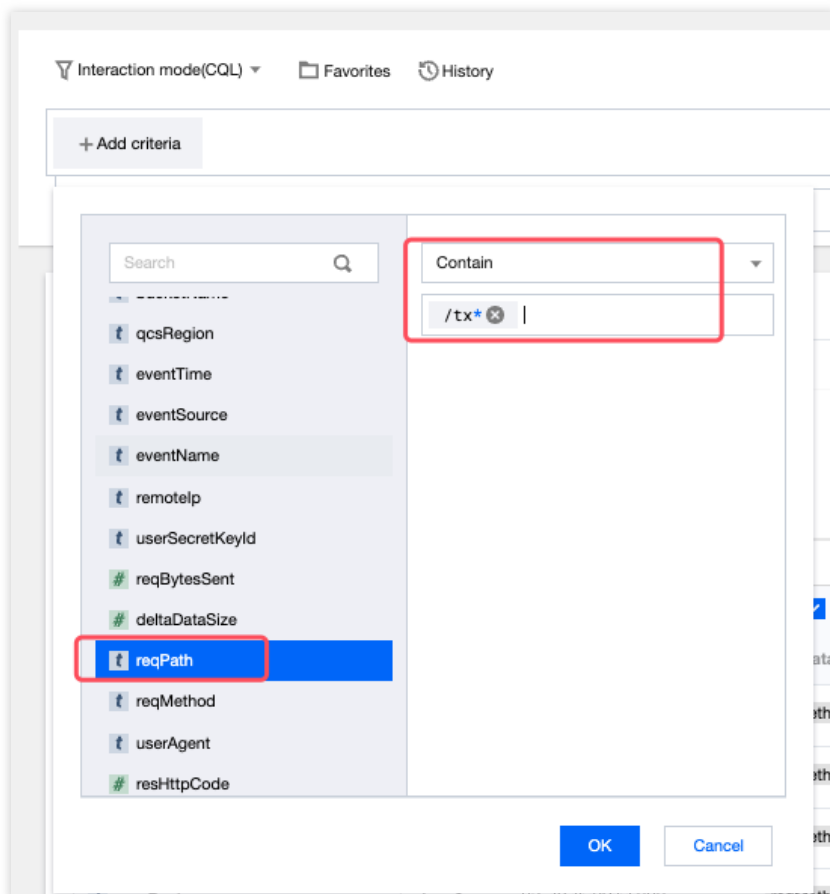
```
1 reqPath: "/1*" | SELECT count(*) as "requests", sum(resBytesSent) as "traffic", SUM(CAST(objectSize AS INT)) AS "Storage capacity"
```

4. Select the time range and click **Search**. On the statistical analysis page, view the analysis results. You can switch chart types on the right side.

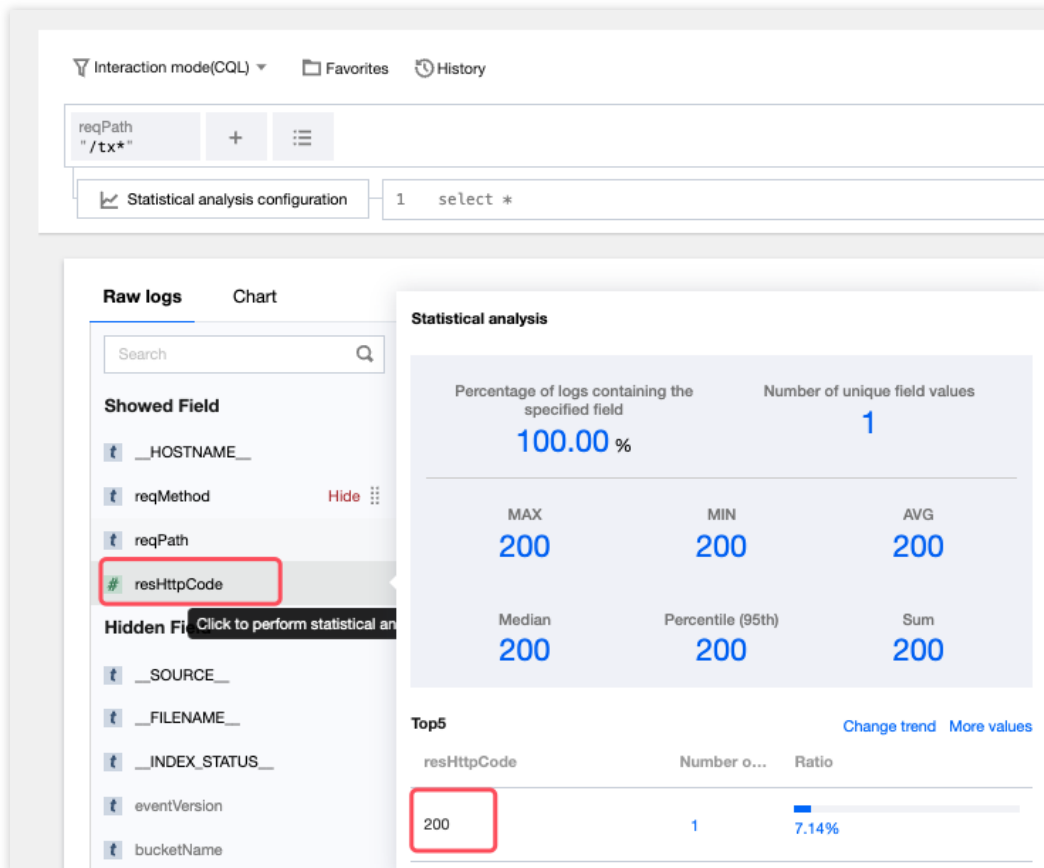


Example 4: Locating Reasons for File Access Failure

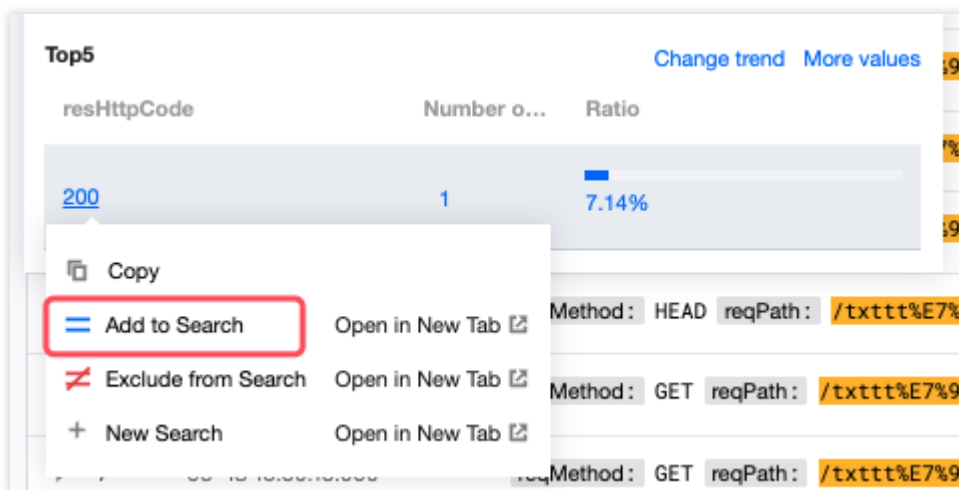
1. Select **Interaction mode(CQL)** and click **Add criteria**. Specify the target file name, select the **Time range** and click **Search**.

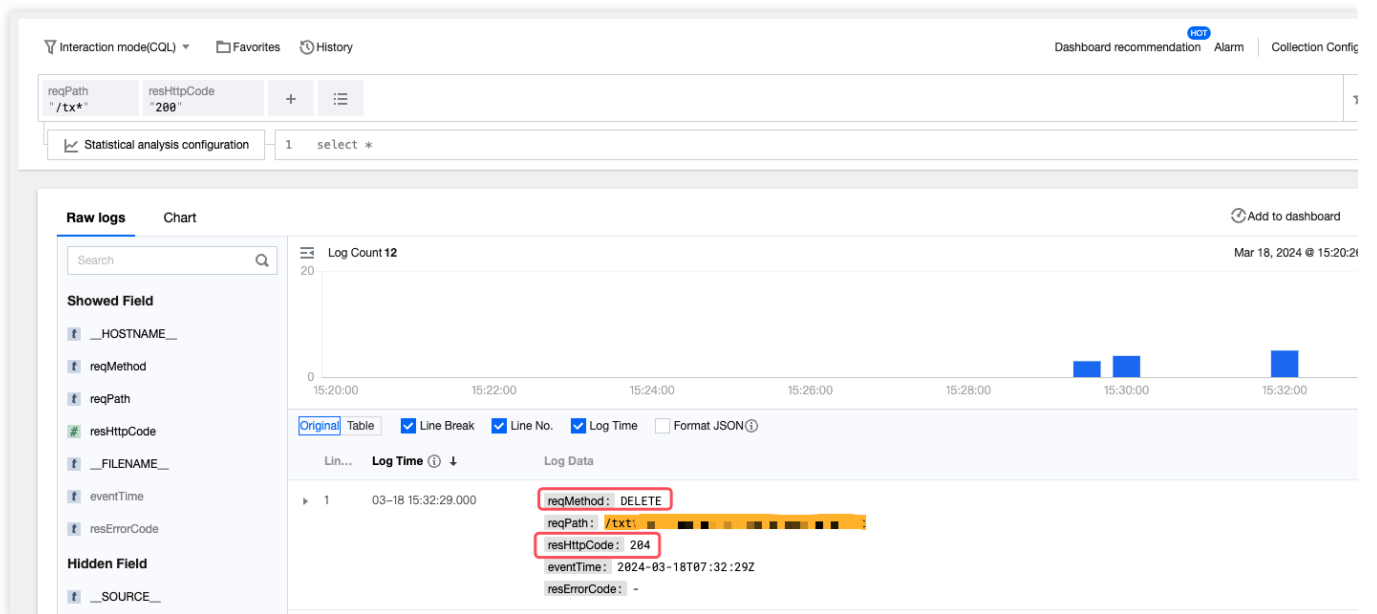


2. Click the field name on the left, enable quick analysis, and conduct statistical analysis based on the **resHttpCode** field. View log information of error codes, such as 403 and 204.



3. Click an error code and choose **Add to Search** to filter the logs. In the log details, view information about other fields, focusing on the fields such as reqMethod. The figure below shows that the delete operation is performed on the file, resulting in object access failure.





Setting Cross-Bucket Replication

Last updated : 2024-01-06 14:59:34

Overview

Cross-bucket replication enables the automatic, asynchronous replication of **incremental objects** from a source bucket to a destination bucket. During replication, COS may also automatically replicate the object operations in the source bucket, such as PUT Object or DELETE Object. You can choose to enable or disable this feature as needed. For more information, see [Overview](#).

Prerequisites

Before enabling cross-bucket replication, make sure that both the source and destination buckets have enabled [versioning](#).

Directions

Enabling cross-bucket replication

1. Log in to the [COS console](#).
2. On the left sidebar, click **Bucket List**.
3. Click the name of the source bucket that you want to set cross-bucket replication for.
4. Click **Fault Tolerance and Disaster Recovery > Cross-Bucket Replication** on the left.
5. In the **Cross-Bucket Replication** column, click **Add Rule**.

Cross Region Replication

Service Authorization You've authorized COS to access files in your bucket.

Details

Applied to	Destination Bucket	Destination Stora...	Sync Delete Marker
Add Rule			

Note: When cross replication is enabled, objects (new or deleted) in the source bucket can be automatically and asynchronously replicated to the destination bucket. Both the source and destination buckets are required to be in different region, and the versioning feature should be enabled. For more information or help, please refer to [Replication guides](#) [🔗](#)

6. In the pop-up window, configure the cross-bucket replication rule and click **OK**.

Note:

If versioning is not enabled for both the source and destination buckets, enable it first and then configure the cross-bucket replication rule.

Add Cross-replication Rule

Note: The network of the financial region and the public region are not interoperable, cross-regional replication rules cannot be configured

Source Region

Chengdu

Applied to

☒ The whole bucket ☐ Specific resources

Resource path

examplebucket-125

Destination Bucket

Beijing

ap-beijing-12

The destination bucket hasn't enabled Versioning feature so that you can not use cross-region replication.

[Learn more](#)

Enable versioning of destination bucket

Destination Storage Class

☒ Standard Storage ☐ Standard_IA Storage

Sync Delete Marker

☒ Sync ☐ Do not sync

☐ I know and agree to grant Tencent Cloud COS service access to bucket resource.

OK

Cancel

The configuration items are described as follows:

Configuration Item	Description

Source Region	The region where your source bucket resides.
Apply To	Indicates which objects will be replicated from the source bucket. The default option is **The whole bucket** . If a prefix is specified, only objects with this prefix will be replicated, such as files prefixed with <code>`logs/`</code> .
Resource Path	Path of your source bucket.
Destination Bucket	The bucket to store the replicated objects. It can be in the same region as the source bucket. You can select only one bucket under the current account in each region.
Destination Storage Class	Storage class of the replicas. The storage class will be the same as that of the source objects by default. You can also select a different storage class.
Sync Delete Marker	If you try to delete an object from a versioning-enabled bucket without specifying a version ID, COS will add a delete marker to the object. If you select this option, cross-bucket replication will copy this delete marker to the destination bucket. Regardless of whether the delete marker is copied, the object will not be deleted from the destination bucket. You can always access a noncurrent version of the object by specifying its version ID. For more information, see Overview .

Note:

Once the rule is created, you can enable/disable it under **Status**, or edit it under **Operation**.

If you set **Applied to** to **The whole bucket** in your first rule, you will be unable to add any new rules. In this case, you may choose to edit it, or simply delete it and add a new one.

If you set **Applied to** to **Specific resources** in your first rule, you can edit it and change this setting to **The whole bucket** if needed.

Disabling cross-bucket replication

You can disable a cross-bucket replication rule using either of the following two options:

Status: Switch this button off, and cross-bucket replication will be disabled temporarily. Copied data will be retained in the destination bucket but no more incremental data will be copied from the source bucket as long as replication is suspended. To re-enable cross-bucket replication, switch this button back on.

Delete Rule: Delete an existing rule by clicking **Delete** under **Operation**. Copied data will be retained in the destination bucket but no more incremental data will be copied from the source bucket. To re-enable cross-bucket replication, you need to add a new rule.

Cross Region Replication

Applied to	Destination Bucket	Destination Storage Class	State
examplebucket-125****/*	testbucket-125**** (Beiji...	Standard Storage	<input checked="" type="checkbox"/>

Note:

When cross-bucket replication is disabled, in-progress cross-bucket replication operations cannot proceed and will be aborted.

When cross-bucket replication is re-enabled for a bucket, it only applies to objects created after that time point.

Enabling Global Acceleration

Last updated : 2024-01-06 14:59:34

Overview

You can enable global acceleration for your bucket in the COS console, which accelerates uploads and downloads, so that end users around the globe can quickly access your bucket. This improves your business access success rate and business stability. For more information, see [Overview](#).

Directions

1. Log in to the [COS console](#).
2. Click **Bucket List** on the left sidebar.
3. Locate the bucket for which you want to enable the global acceleration feature. Click the bucket name to enter its details page.
4. On the left sidebar, select **Domains and Transfer** > **Global Acceleration** and click **Edit** to enable the feature.

Global Acceleration [Edit](#)

Status Off

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](#) [🔗](#)

5. After confirming that everything is correct, click **Save**.

Global Acceleration

Status



Global Accelerated Domain Name examplebucket-1250000000.cos.accelerate.myqcloud.com

Save

Cancel

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](#) [🔗](#)

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

Note:

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

Setting Object Lock

Last updated : 2024-01-06 14:59:34

Overview

COS's object lock feature allows you to set a retention period for your objects to prevent them from being overwritten or deleted for a fixed amount of time and your objects can still be accessed immediately. This document describes how to enable object lock in the COS console.

Directions

1. Log in to the [COS console](#).
2. Click **Bucket List** on the left sidebar.
3. Click the target bucket to enter the bucket list page.
4. Click **Security Management** > **Object Lock** on the left, find the **Object Lock** configuration item, click **Edit**, and toggle the feature on.
5. Enter the retention period in the configuration window and click **Save**.

Object Lock

Status

☒

Policy Type

Time Based Strategy

Retention period

days

Retention period must be a positive integer and only allow extended.

Save

Cancel

Retention period: It must be a positive integer and can only be extended but not shortened.

6. In the pop-up window, click **OK**.

After the configuration, you can click **File List** > the desired file > **Details** to view the date (local time) on which the object lock rule will expire.

Note:

The object lock feature is now only available to customers in the allowlist. To use this feature, [contact us](#).

Object Management

Uploading an Object

Last updated : 2024-01-06 15:06:14

Overview

You can upload objects to a bucket through the **File List** page in the COS console. For more information about objects, please see [Object Overview](#).

Note:

Currently, the MAZ configuration is only available in Beijing, Shanghai, Guangzhou, and Singapore regions. To upload objects to an MAZ storage class such as MAZ_STANDARD, enable [MAZ configuration](#) for the bucket in the region first.

Currently, the INTELLIGENT TIERING storage class is only available in Beijing, Nanjing, Shanghai, Guangzhou, Chengdu, Chongqing, Tokyo, and Singapore regions. To upload objects to this storage class, enable [INTELLIGENT TIERING](#) for the bucket in the region first.

Currently, the DEEP ARCHIVE storage class is only available in Beijing, Nanjing, Shanghai, Guangzhou, Chengdu, Chongqing, Tokyo, and Singapore regions. To upload objects to this storage class, select a bucket in the region first. When you upload an object in the console, the upload speed is strongly subject to the current network environment. If the object is large or the network conditions are poor, we recommend you use [multipart upload](#). In multipart upload, a file can be divided into multiple parts and uploaded separately, and the failure to upload a single part will not affect other uploaded parts. You can use the [COSCLI tool](#), [APIs](#), or [SDKs for different programming languages](#) to initiate a multipart upload request. Among them, SDKs and COSCLI support checkpoint restart, where incomplete uploads can be resumed from where left off, thereby improving the overall upload success rate.

Prerequisites

Before uploading an object, make sure that you have already created a bucket. If no bucket has been created, please see [Creating Buckets](#).

Directions

1. Log in to the [COS console](#).
2. Click **Bucket List** on the left sidebar.
3. Click the target bucket to enter the **File List** page.

4. In **File List**, click **Upload Files**.

5. In the pop-up window, click **Select Files** or **Select Folders** and select one or multiple local files (or folders) as needed.

Note:

Since some browsers do not support uploading multiple files, we recommend you use popular browsers such as Internet Explorer 10 or later, Firefox, or Chrome.

6. (Optional) Click **Configure Parameters** and set the object attributes in the **Upload Files** window.

Upload Files

✓ Select Objects

2 Set Properties

Properties Setting will be applied to all the objects to be uploaded, you can also upload directly and then modify the settings in file list page.

Storage Class

☒ STANDARD
It is suitable for business scenarios such as real-time access to a large number of hot files and frequent data interaction. Supported in all regions.

☐ STANDARD_IA
It is suitable for business scenarios with low access frequency (e.g., average access frequency is 1 to 2 times per month). Supported in all regions.

☐ ARCHIVE
It is suitable for business scenarios with very low access frequency (e.g., once every six months). Since real-time response is not supported, if you want to retrieve the archived data, please apply in advance.

☐ Deep Archive Storage
It is suitable for business scenarios with very low access frequency (for example, 1 to 2 visits per year). If you want to retrieve the data stored in deep archives, you need to apply in advance and cannot respond in real time.

Access Permissions

☒ Inherit ☐ Private Read/Write ☐ Public Read/Private Write

Server-Side Encryption

☒ None ☐ SSE-COS ⓘ

Object Tag

Enter a tag key

Enter a tag value

+

Metadata

Parameter	Value	Operati...
Select Project	Value	Delete
Add Parameters		

Notes:

Storage Class: Select the storage class for your object as needed. This field is set to `STANDARD` by default. For more information, see [Overview](#).

Note:

If your bucket has MAZ configuration enabled, you can only select an MAZ storage class, such as MAZ_STANDARD. If it also has INTELLIGENT TIERING configuration enabled, you can also select MAZ_INTELLIGENT TIERING.

Access Permissions: Select the access permission for your object as needed. This field is set to `Inherit` by default (inheriting permissions of the bucket). For more information, please see [Basic Concepts of Access Control](#).

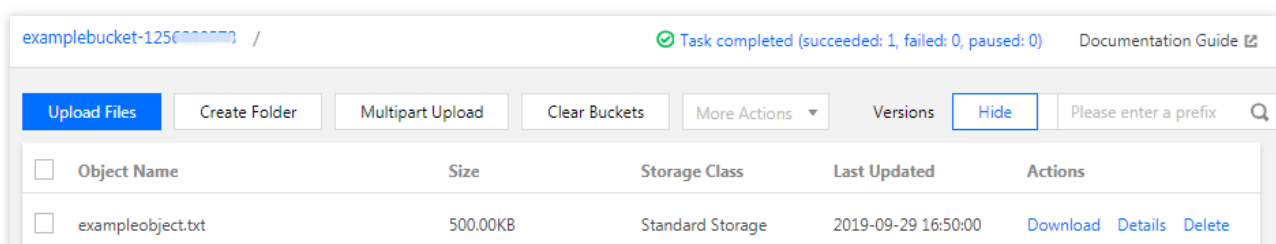
Server-Side Encryption: Configure server-side encryption for the object you want to upload. COS will automatically encrypt your data as it is written and decrypt it when you access it. Currently, COS offers two encryption types: SSE-KMS (only available in Beijing, Shanghai, and Guangzhou regions) and SSE-COS. For more information, please see [Server-side Encryption Overview](#).

Object tag: You can add tags to an object to be uploaded. The object tag is composed of a tag key, (=), and a tag value, such as `group = IT`. Each object tag is a key-value pair. For more information, see [Object Tag Overview](#).

Metadata: Object metadata, or HTTP header, is a string sent by the server over HTTP before it sends HTML data to the browser. By modifying HTTP headers, you can modify how the webpage responds as well as certain configurations, such as caching time. Modifying an object's HTTP headers does not modify the object itself. For more information, please see [Custom Headers](#).

7. Click **Upload**.

You can check the upload progress in **Task Completed** in the top-right corner of the page. Once the upload is complete, the uploaded object will appear in **File List**.



Note:

The task progress in the figure indicates the number of tasks created by the current upload operation. For example, if you perform an upload operation where all 10 files are uploaded successfully, the task progress will be displayed as "Task completed (total: 1; succeeded: 1; failed: 0)".

Downloading Objects

Last updated : 2024-01-06 15:06:14

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](#).

Directions

Downloading a single object

1. Log in to the [COS console](#).
2. Click **Bucket List** on the left sidebar.
3. Locate the bucket where the object resides and click the bucket name.
4. Click **File List** on the left.
5. Find the target object and click the corresponding **Download** button.

Click **Download** in the **Operation** column on the right of the object.

Select the object and click **More Actions > Download** at the top.

Click **Download** in the **Operation** column on the right of the object to enter the file details page, and then click **Download Object**.

You can also click **Copy Temporary Link**, paste the link into a browser, and press **Enter**.

Note:

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 1 hour from the moment you click to view the **Details**. You can refresh the validity period of the signature by clicking **Refresh**.

By default, if the downloaded object can be directly opened in the browser, then accessing the temporary URL will directly preview the object rather than downloading it.

Downloading objects or folders in batches

Note:

You can only download individual objects in the COS console. To download multiple objects or folders in batches, we recommend you install the [COSBrowser client](#). Here is how to download objects or folders in batches in the console in conjunction with the **COSBrowser client**.

1. Log in to the [COS console](#).
2. Click **Bucket List** on the left sidebar.
3. Locate the bucket where the object resides and click the bucket name.
4. Click **File List** on the left.
5. Select multiple objects and click **More Actions > Download** at the top.
6. Follow the on-screen prompts to install or launch the COSBrowser client and log in.
7. Select the file storage location, and selected files will automatically enter the download queue. You can click **Download List** to view them.

Copying Object

Last updated : 2024-01-06 15:06:15

Overview

You can use the COS console to copy a single object or multiple objects in a bucket from the source path to the destination path.

Note:

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

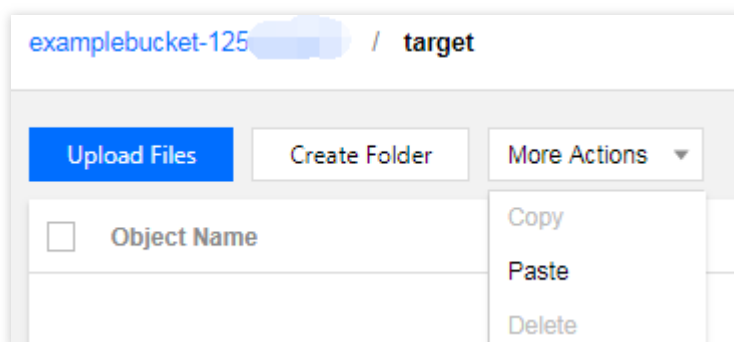
The `MAZ_STANDARD` storage class only supports replication into the exact same class rather than standard storage, low frequency, or archive storage classes.

The `MAZ_STANDARD_IA` storage class only supports replication into the exact same class rather than STANDARD, STANDARD_IA, and ARCHIVE storage classes.

A sub-account should be granted the `PutObject` , `GetObject` , and `GetObjectACL` permissions to copy objects.

Directions

1. Log in to the [COS console](#).
 2. Click **Bucket List** on the left sidebar.
 3. Click the name of the target bucket to enter its file list page.
 4. Select one or multiple objects or folders and click **More Actions** > **Copy** at the top.
 5. When prompted that the copy is successful, select the target path and click ****More Actions **** > **Paste** at the top.
- For example, you can paste to the `target` folder in the bucket `examplebucket1-1250000000` .



Note:

The destination path cannot be the same as the source path; otherwise, the paste will fail.

Previewing or Editing Object

Last updated : 2024-01-06 15:06:15

Overview

You can preview object content and edit text objects online in the COS console. For the file types supported for preview, see [File Preview Overview](#).

Directions

1. Log in to the [COS console](#).
2. Click **Bucket List** on the left sidebar.
3. Locate the bucket where the object resides and click the bucket name.
4. Click **File List** on the left.
5. Find the target object and click **Preview** in the **Operation** column on the right.
6. In the pop-up window, preview the object.

In addition, you can also preview a text file in a browser by copying the temporary preview URL (which is valid for 1 hour).

7. For a text file, you can click **Edit** in the preview window.
8. Authorize to log in to COSBrowser as prompted to edit the file.

Viewing Object Information

Last updated : 2024-01-06 15:06:14

Overview

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

Directions

1. Log in to the [COS console](#).
2. Click **Bucket List** on the left sidebar.
3. Locate the bucket where the object resides and click the bucket name.
4. Click **File List** on the left sidebar.
5. Find the target object and click **Details** in the **Operation** column on the right.

On the object details page, you can view the object size and address, obtain the signed URL, and configure the object.

Basic Information

Object Name	exampleobject.txt
Object Size	500.00KB
Last Modified	2019-09-29 16:50:00
ETag	"c939165a4566ac3eba011f641e94c519"
Specified Domain①	<div>Default Origin Domain ▾</div>
Object Address①	https://examplebucket-1250000000.cos.ap-chengdu.myqcloud.com/exampleobject.txt
Temporary Link①	<div> Copy Temporary Link Download Objects Refresh</div> <p>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) .</p> <p>Please take care of your temporary links to avoid leakage, otherwise your objects may be accessed by other users.</p>

Server-Side Encryption

Encryption ☒ None ☐ SSE-COS

Searching for Objects

Last updated : 2024-01-06 15:06:14

Overview

You can search for uploaded objects and folders in the COS console, which supports prefix and fuzzy search modes.

Prefix search: Objects are searched for by prefix, and objects and folders with the specified object prefix are displayed.

Fuzzy search: Objects are searched for by custom keyword, and objects and folders whose name contains the specified keyword are displayed.

Note:

The object prefix entered for object search is case-sensitive.

In addition, you can also use COSBrowser for fuzzy search as detailed in [COSBrowser Overview](#).

Directions

Searching for objects by prefix

1. Log in to the [COS console](#).
2. Click **Bucket List** on the left sidebar.
3. Locate the bucket where the object resides and click the bucket name.
4. Click **File List** on the left.
5. In the search box in the top-right corner of the page, enter the object name prefix and click



. Then, the system will display objects or folders with the **same name prefix** in the current bucket. For example, if you enter `img`, objects and folders with the name prefix `img` will be displayed.

Searching for objects by keyword

1. Log in to the [COS console](#).
2. Click **Bucket List** on the left sidebar.
3. Locate the bucket where the object resides and click the bucket name.
4. Click **File List** on the left.
5. In the search box in the top-right corner of the page, enter the keyword and click



. Then, the system will display objects and folders whose name contains the keyword in the current bucket. For example, if you enter `t` , objects and folders whose name contains `t` will be displayed.

Sorting and Filtering Objects

Last updated : 2024-01-06 15:06:15

Overview

This document describes how to sort/filter objects in the file list of the bucket through the COS console.

Note:

Object sorting/filtering is only available if the number of files/folders is less than 1,000.

Directions

1. Log in to the [COS console](#).
2. Click **Bucket List** in the left sidebar.
3. Click the name of the desired bucket to view its file list.
4. Click



,



, or



,



to sort/filter objects as needed.

Note:

Currently, sorting by file name/file size/modification time, and filtering by storage class are supported.

Direct Upload to ARCHIVE

Last updated : 2024-01-06 15:06:14

Overview

COS supports direct upload to the ARCHIVE storage class by using the console, APIs, SDKs, or COSCMD.

Alternatively, you can use the lifecycle feature of COS to transition your objects to the ARCHIVE or DEEP ARCHIVE storage class. For more information, see [Storage Class Overview](#).

Supported Methods

Uploading via the console

In the [COS console](#), click **Upload Files** and select the object to be uploaded. In the **Set Properties** step, set **Storage Class** to **ARCHIVE** or **DEEP ARCHIVE**. For more information, see [Uploading Object](#).

Upload Files

✓ Select Objects

>

2 Set Properties

Properties Setting will be applied to all the objects to be uploaded, you can also upload directly and then modify the file in list page.

Storage Type

☐ Standard Storage

It is suitable for business scenarios such as real-time access to a large number of hot files and frequent data interaction. Supported in all regions.

☐ Standard_IA Storage

It is suitable for business scenarios with low access frequency (e.g., average access frequency is 1 to 2 times per month). Supported in all regions.

☒ Archive Storage

It is suitable for business scenarios with very low access frequency (e.g., once every six months). Since real-time response is not supported, if you want to retrieve the archived data, please apply in advance.

Access Permissions

☒ Inherit ☐ Private (read-write) ☐ Public read & Private write

Server-Side Encryption

☒ None ☐ SSE-COS ⓘ

Metadata

Parameter	Value	Actions
Select Project ▼	Value	Delete
Add Parameters		

Previous

Upload

Uploading via APIs

You can set `x-cos-storage-class` to `ARCHIVE` or `DEEP_ARCHIVE` in the `PUT Object` , `POST Object` , or `Initiate Multipart Upload` API to implement direct upload to ARCHIVE.

Note:

The `Append Object` API does not support direct upload to ARCHIVE.

Uploading via SDKs

Currently, all COS SDKs support direct upload to ARCHIVE. You can set the `StorageClass` parameter to `ARCHIVE` or `DEEP_ARCHIVE` during the upload.

Uploading via COSCMD

You can add the header field `x-cos-storage-class` and set it to `ARCHIVE` or `DEEP_ARCHIVE` during the upload.

Restoring and downloading archived data

Unlike STANDARD/STANDARD_IA, objects in ARCHIVE or DEEP ARCHIVE can only be downloaded after being restored. The following three restoration modes are provided:

Expedited: Restores an object within 1–5 minutes (fastest).

Standard: Restores an object within 3–5 hours.

Bulk: Restores multiple objects within 5–12 hours (most cost-effective).

Note:

Objects in DEEP ARCHIVE cannot be restored in the expedited mode. An object can be restored within 12–24 hours in standard mode or 24–48 hours in bulk mode.

Note that the console, APIs, SDKs, and COSCMD all support the restoration and download of archived objects.

Restrictions

Objects in ARCHIVE or DEEP ARCHIVE need to be restored before being downloaded.

To copy an object in ARCHIVE or DEEP ARCHIVE, you need to restore it first.

Objects in ARCHIVE and DEEP ARCHIVE do not support cross-region replication.

Objects in ARCHIVE and DEEP ARCHIVE cannot be changed to a more frequently accessed storage class, such as STANDARD and STANDARD_IA.

Modifying Storage Class

Last updated : 2024-01-06 15:06:14

Overview

You can modify the storage class of your object uploaded to COS through the console at any time to meet your business needs in different scenarios. COS offers a range of storage classes, including MAZ_STANDARD, MAZ_STANDARD_IA, INTELLIGENT TIERING, STANDARD, STANDARD_IA, ARCHIVE, and DEEP ARCHIVE. For more information, see [Overview](#). The following section will guide you through how to modify the storage class of an object.

Note:

Objects in the MAZ_STANDARD or MAZ_STANDARD_IA storage class cannot be transitioned to the STANDARD_IA or ARCHIVE storage class.

To modify the storage class of an object stored in **ARCHIVE** or **DEEP ARCHIVE**, you need to restore it first into STANDARD. For more information, see [Restoring Archived Objects](#).

COS does not allow modifying the storage class of an object larger than 5 GB.

Directions

1. Log in to the [COS console](#).
2. Click **Bucket List** on the left sidebar.
3. Locate the bucket where the object resides and click the bucket name.
4. Click **File List** on the left sidebar.
5. Find the target object and click **More > Modify Storage Class** in the **Operation** column on the right.
To batch modify the storage class of multiple objects, select multiple objects and click **More Actions > Modify Storage Class** at the top.
6. Select the target storage class and click **OK** in the pop-up window.

Deleting Incomplete Multipart Uploads

Last updated : 2024-01-06 15:06:15

Overview

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 Upload** 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.

Note:

During the object upload progress, the files that are paused or canceled will be displayed in **Incomplete Multipart Upload**. Files can be viewed in **File List** only after they are completely uploaded.

Like objects, incomplete multipart uploads consume your storage space and incur storage usage costs.

Directions

Deleting incomplete multipart uploads manually

1. Log in to the [COS console](#).
 2. Click **Bucket List** on the left sidebar.
 3. Locate the bucket where the incomplete multipart upload to delete resides, and click the bucket name to go to the bucket management page.
 4. Click **File List** on the left sidebar.
 5. Click **Incomplete Multipart Upload**.
 6. View incomplete multipart uploads on the page.
 7. Click **Delete** on the right of an incomplete multipart upload to delete it.
- You can also click **Clear Incomplete Multipart Uploads** at the top to quickly delete all incomplete multipart uploads.

Multipart Upload

[Clear Incomplete Multipart Uploads](#)

Enter path prefix

Multipart Upload Name	Upload Task ID	Storage...	Time Created	Actions
file.7z	15658645104a6e0071c8b654...	Standar...	2019-08-15 18:21:50	Details Delete

After you perform the **Clear Incomplete Multipart Uploads** or **Delete** operation, the list will be empty.

Clearing incomplete multipart uploads regularly with lifecycle policy

1. Log in to the [COS console](#).
2. Click **Bucket List** on the left sidebar.
3. Locate the bucket where the incomplete multipart upload to delete resides, and click the bucket name to go to the bucket management page.
4. On the left sidebar, click **Basic Configurations > Lifecycle** to enter the lifecycle management page.

Lifecycle

Rule ID	Applied to	Rule content	State	Actions
Add rule				

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

5. Click **Add a Rule**, and you can see the configuration items as shown below. For example, you can set to delete incomplete multipart uploads across the bucket seven days after creation.

Add a Rule ✕

If an object is transitioned to the Standard_IA (Infrequent Access) Storage class or the Archive Storage class, it will be limited by the object specification. If the object size is smaller than the minimum specification, it will be calculated according to the minimum specification.

State ☒ Enable ☐ Off

Rule ID *

Applied to ☒ The whole bucket ☐ Prefix name

Managing the current version ☒ Enable ☐ Off

☐ days after the objects are modified, they will be transitioned to Standard_IA Storage.

☐ days after the objects are modified, they will be transitioned to Archive Storage

☐ days later, they will be deleted

Managing historical versions ☐ Enable ☒ Off

Removing delete markers of expired objects ⓘ ☐ Enable ☒ Off

Deleting incomplete multipart uploads ☒ After incomplete multipart uploads created days later, they will be deleted

6. Click **OK**, and you can find this new lifecycle rule in the console.

Lifecycle

Rule ID	Applied to	Rule content	State	Actions
examplerule	The whole bucket	Delete incomplete multipart uploads: 7 days	Enable	Edit Delete

Setting Object Access Permission

Last updated : 2024-01-06 15:06:15

Overview

COS allows you to set object access permissions, which have a higher priority than those for buckets.


Note:

Object access permissions take effect only when the access is made via the default endpoint. For any access made via a CDN acceleration endpoint or a custom endpoint, bucket access permissions will take effect.

There are limits on the number of ACL rules. For more information, please see [Specifications and Limits](#).

Directions

1. Log in to the [COS console](#).
2. In the left sidebar, click **Bucket List** to go to the bucket list page.
3. Locate the bucket where the object resides and click the bucket name to go to the bucket management page.
4. In the left sidebar, choose **File List** to go to the file list page.
5. Locate the object for which you want to configure the access permission, and click **Details** on the right to go to the file details page (If it is a folder, click **Permissions** on the right).

<input type="checkbox"/>	Object Name ↕	Size ↕	Storage Class ▼	modification ti... ↕	Operation
<input type="checkbox"/>	 examplefolder/	-	-	-	Permissions Statistics Delete
<input type="checkbox"/>	1.txt	0B	STANDARD	2021-01-20 14:37:01	Details Download More Actions ▼
<input type="checkbox"/>	2.txt	0B	STANDARD	2021-01-20 14:36:45	Details Download More Actions ▼

6. In the **Object ACL(Access Control List)** area, configure access permissions as needed.

For example, you can grant object permissions to a sub-account. The sub-account ID can be viewed in the [CAM console](#).

Object ACL(Access Control List)

Public permissions
☐ Inherit
☒ Private (read-write)
☐ Public read & Private write

User ACL

User type	Account ID	Permissions	Actions
Root account	10000	Full control	--
Add user			

Save
Cancel

COS supports two types of permissions for objects:

Public Permission: includes **Inherit**, **Private Read/Write**, and **Public Read/Private Write**. For more information about public permissions, please see [Access Permission Types](#).

User ACL: The root account has all object permissions (full control) by default. You can also add sub-accounts and grant them permissions including read/write, read/write ACL, and even **full control**.

7. Click **Save**.

If you need to configure or modify access permissions for multiple objects at a time, you can select the objects on the **File List** page and then click **Modify Access Permission** from the **More Actions** drop-down list at the top.

Upload Files
Create Folder
Incomplete multipart Upload
Clear Buckets
More Actions
Selected 2 / 3

<input type="checkbox"/>	Object Name	Size	Storage Class	modified	
<input type="checkbox"/>	examplefolder/	-	-	-	
<input checked="" type="checkbox"/>	1.txt	0B	STANDARD	2021-01-20 14:...	Download Restore Custom He... Modify Encr... Modify Acce... Set Tag Modify Stor...
<input checked="" type="checkbox"/>	2.txt	0B	STANDARD	2021-01-20 14:...	Download Actions Download Actions Download More Actions

Setting Object Encryption

Last updated : 2024-01-06 15:06:14

Overview

You can encrypt the objects stored in buckets using the COS console to prevent data disclosure. For more information on encryption, see [Server-Side Encryption Overview](#). The following shows you how to configure object encryption:

Caution

This operation does not support configuring encryption for objects in the ARCHIVE storage class. If encryption is required, [restore archived objects](#) first. After the restoration is complete, change the storage class to STANDARD or STANDARD_IA before configuring the encryption.

As long as you have access permission on an object, the object accessing experience is the same regardless of whether the object is encrypted.

Server-side encryption encrypts only the object data but not its metadata. Server-side encrypted objects can only be accessed with a valid signature and cannot be accessed by anonymous users.

When you list the objects in a bucket, all objects will be listed, regardless of whether they are encrypted.

Directions

1. Log in to the [COS console](#).
2. Click **Bucket List** on the left sidebar.
3. Locate the bucket where the object resides and click the bucket name.
4. Click **File List** on the left sidebar.
5. Find the target object and click **Details** in the **Operation** column on the right.
6. Select the encryption mode in the **Server-Side Encryption** column and click **Submit**.

The following two encryption methods are currently supported:

SSE-COS: Server-side encryption with a key managed by COS. For more information on SSE-COS encryption, see [SSE-COS Encryption](#).

SSE-KMS: Server-side encryption with a key managed by Tencent Cloud Key Management System (KMS). You can use the default key or create a key. For more information about keys, see [Creating a Key](#). For more information about SSE-KMS, see the **SSE-KMS Encryption** section in [Server-side Encryption Overview](#).

Note

If you use SSE-KMS encryption for the first time, you need to [enable the KMS service](#).

Currently, SSE-KMS encryption is available only in the Beijing, Shanghai, Guangzhou and Hong Kong (China) regions.

To batch encrypt multiple objects, select multiple objects and click **More Actions** > **Modify Encryption Method** at the top.

Custom Headers

Last updated : 2024-05-06 09:46:39

Feature Overview

An HTTP header (metadata header) of an object is a string sent by the server over HTTP before it sends HTML data to the browser. By modifying HTTP headers (metadata headers), you can modify how the webpage responds as well as certain configurations, such as caching time. Modifying an object's HTTP headers does not modify the object itself.

Note:

For objects of ARCHIVE and DEEP ARCHIVE, custom headers can only be set during upload. Setting custom headers for objects that have already been uploaded is not supported.

How It Works

1. Log in to the [COS console](#).
2. Click **Bucket List** on the left sidebar.
3. Locate the bucket where the object resides and click the bucket name.
4. Click **File List** on the left sidebar.
5. Locate the object for which a header is to be customized and click **More > Custom Header** in the operation column on the right. To customize headers for multiple objects, select multiple objects and click **More Actions > Custom Header** on the top.
6. In the pop-up window, select the parameter type of the metadata header to be set, enter the metadata value, and click **OK**.

COS provides the following six types of object HTTP headers for configuration:

HTTP Header	Description	Example
Content-Type	MIME information of the file	image/jpeg
Cache-Control	File caching mechanism	no-cache: Indicates that cache cannot be used directly, but whether the object has been updated must be verified first with the server. If the object has been updated, it indicates that the cache is expired, and the object must be re-downloaded from the server; if the object has not been updated, the cache is not expired, and the local cache will be used. max-age=200: Indicates the relative expiration time of the cached content, in seconds.

Content-Disposition	Extension of MIME protocol	<p>inline: Directly previews the content of the file.</p> <p>attachment: Downloads to the specified path in the browser with the original filename.</p> <p>attachment; filename="FileName": You should download it to the specified path in the browser with a custom filename. FileName defines the name of the file after download, for example, example.jpg. If the attachment name is in Chinese, it needs to be URL encoded, for example, <code>attachment; filename* = UTF-8' '%E4%B8%AD%E6%96%87.txt</code></p>
Content-Encoding	File encoding format	<p>gzip</p> <p>Note: If the Content-Encoding in the header has been modified as gzip, but the file has not been compressed with gzip, a decoding error will occur.</p>
Expires	Expiration date of the cache	Wed, 21 Oct 2015 07:28:00 GMT
x-cos-meta-[custom suffix]	User-defined content	<p>x-cos-meta-via: homepage</p> <p>Note: Header names support only hyphens (-), digits, and English letters (a-z). Uppercase letters in English will be converted to lowercase letters; other characters, including underscores (_), are not supported.</p>

License request example

Assume that a bucket named "examplebucket-1250000000" was created under account APPID 1250000000, and an object "exampleobject.txt" was uploaded to the bucket's root directory.

Non-custom HTTP header of objects

The sample below shows the headers returned for a request to download this object through a browser or client if no custom HTTP headers are specified.

Request



```
GET /exampleobject.txt HTTP/1.1
Host: examplebucket-1250000000.cos.ap-beijing.myqcloud.com
Date: Fri, 10 Apr 2020 09:35:16 GMT
Authorization: q-sign-algorithm=sha1&q-ak=AKID8A0fBVtYFrNm02oY1g1JQQF0c3JO****&q-si
Connection: close
```

Response



```
HTTP/1.1 200 OK
Content-Type: text/plain
Access-Control-Allow-Origin: *
Last-Modified: Fri, 10 Apr 2020 09:35:05 GMT
```

Custom HTTP header of objects

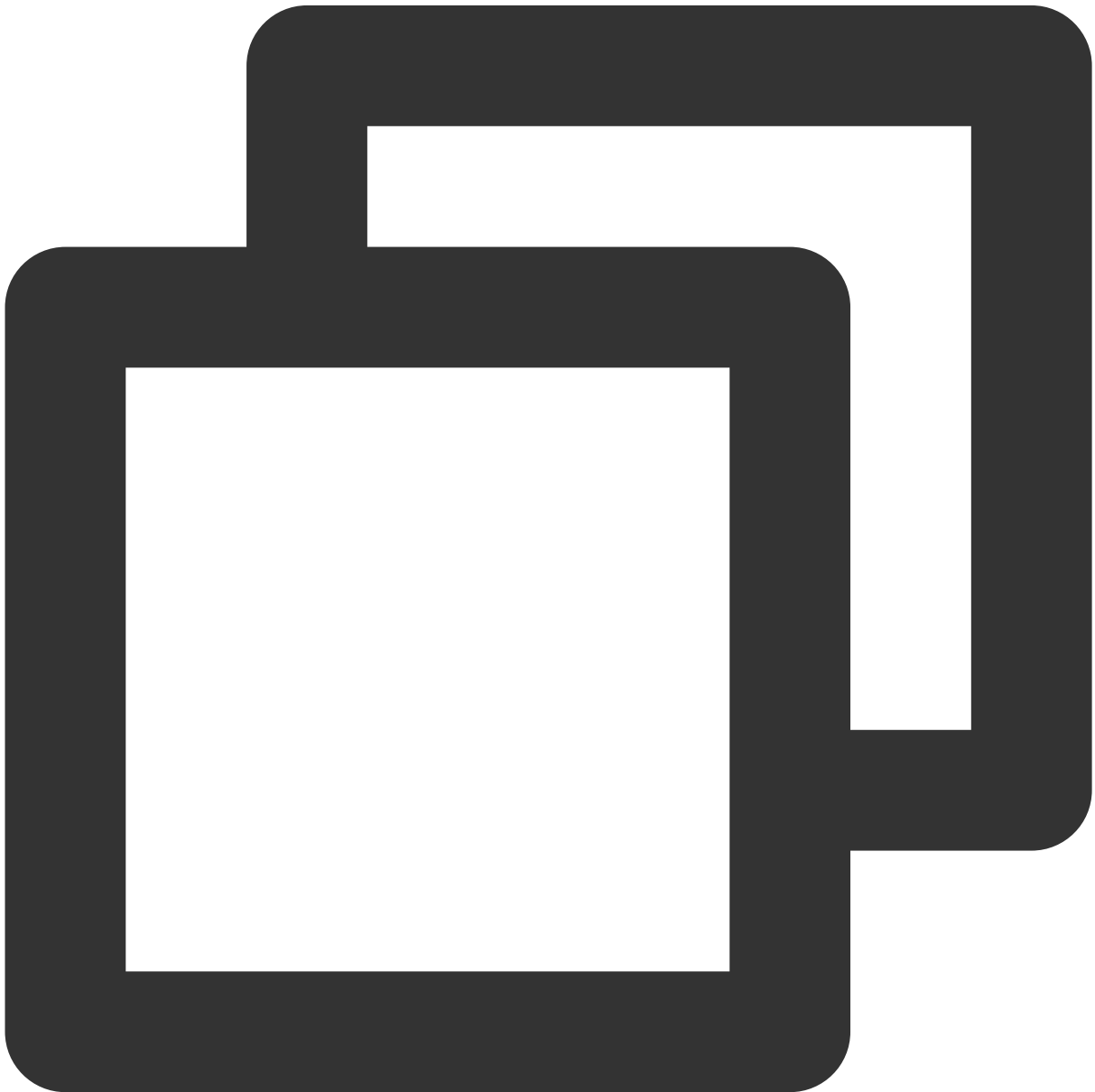
Refer to [directions](#) to add the following custom header configuration:

Parameter	Value

Content-Type	image/jpeg
Cache-Control	no-cache
Content-Disposition	attachment; filename* = UTF-8' '%E4%B8%AD%E6%96%87.jpeg
x-cos-meta-md5	1234

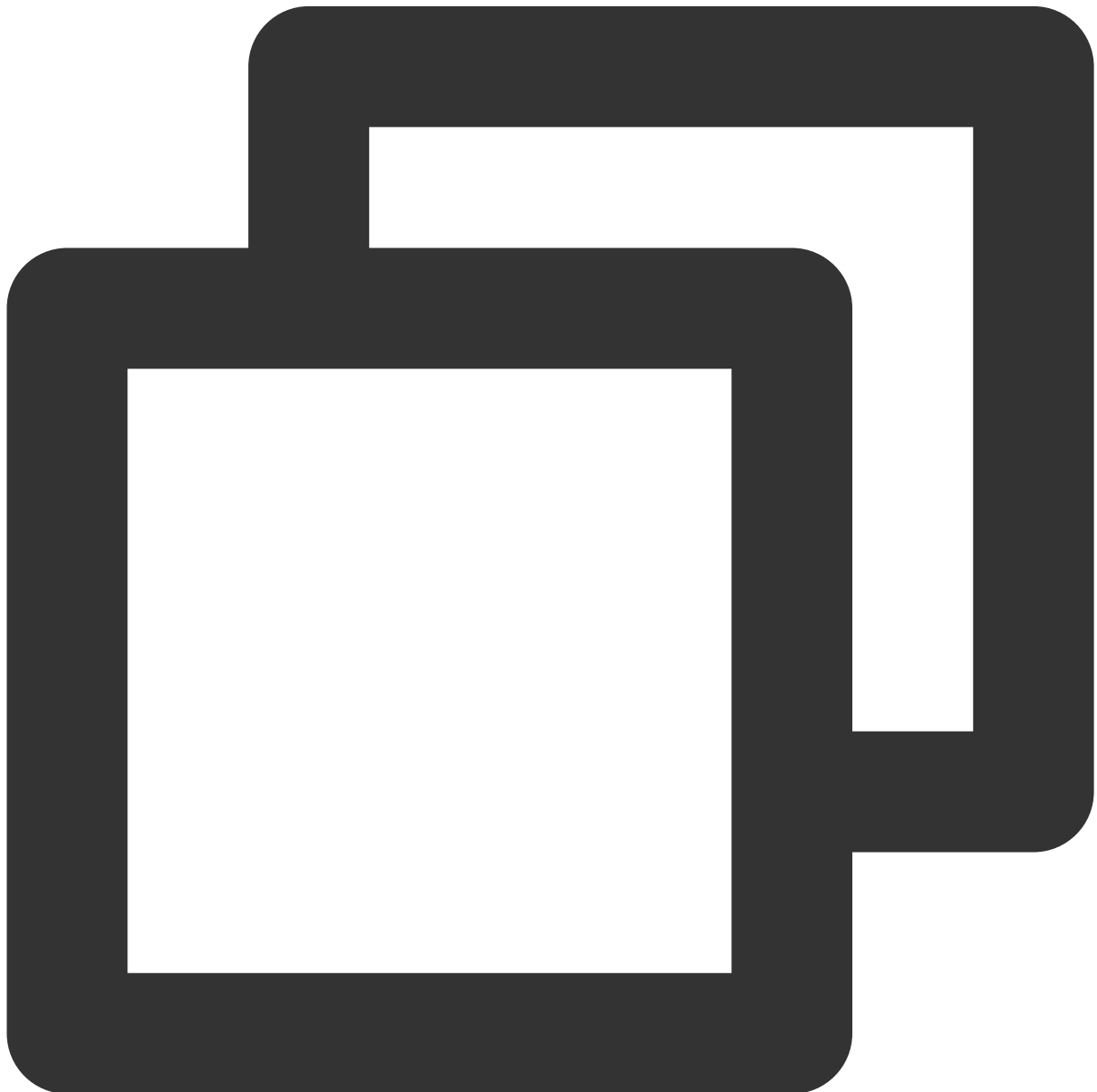
then the headers returned for new requests will be as follows:

Request



```
GET /exampleobject.txt HTTP/1.1
Host: examplebucket-1250000000.cos.ap-beijing.myqcloud.com
Date: Fri, 10 Apr 2020 09:35:16 GMT
Authorization: q-sign-algorithm=sha1&q-ak=AKID8A0fBVtYFrNm02oY1g1JQQF0c3JO****&q-si
Connection: close
```

Response



```
HTTP/1.1 200 OK
Cache-Control: no-cache
```

```
Content-Type: image/jpeg
Content-Disposition: attachment; filename* = UTF-8' '%E4%B8%AD%E6%96%87.jpeg
x-cos-meta-md5: 1234
Access-Control-Allow-Origin: *
Last-Modified: Fri, 10 Apr 2020 09:35:05 GMT
```

It can be seen that when custom headers are used, the response format of the page can be changed.

Deleting Objects

Last updated : 2024-01-06 15:06:14

Overview

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

Note:

Deleted data cannot be restored. Please proceed with caution.

Directions

Deleting a single object

1. Log in to the [COS console](#).
2. In the left sidebar, click **Bucket List** to go to the bucket list page.
3. Locate the bucket where the object resides and click the bucket name to go to the bucket management page.
4. In the left sidebar, choose **File List** to go to the file list page.
5. Locate the object to delete, and click **Delete** from the **More Actions** drop-down list in the **Operation** column.
6. In the pop-up window, click **OK**.

Deleting multiple objects

1. Log in to the [COS console](#).
2. In the left sidebar, click **Bucket List** to go to the bucket list page.
3. Locate the bucket where the object resides and click the bucket name to go to the bucket management page.
4. In the left sidebar, choose **File List** to go to the file list page.
5. Select the objects to delete and click **Delete** from the **More Actions** drop-down list at the top.
6. In the pop-up window, click **OK**.

Restoring Archived Objects

Last updated : 2024-01-06 15:06:15

Overview

You can restore an object from the ARCHIVE or DEEP ARCHIVE storage class through the COS console. The restoration operation will create a copy of the object in the STANDARD storage class. You can read, download, or perform other operations on the copy within its validity period. The copy will be deleted automatically after expiration. For more information about storage classes, see [Storage Class Overview](#).

Note:

If you restore objects from ARCHIVE, the object copy will be billed at STANDARD rates. If you restore objects from DEEP ARCHIVE, the object copy will be charged request fees at the marked unit price, and traffic fees at STANDARD rates. For more information, see [Product Pricing](#).

Directions

1. Log in to the [COS console](#).
2. Click **Bucket List** on the left sidebar.
3. Locate the bucket where the object resides and click the bucket name.
4. Click **File List** on the left sidebar.
5. Locate the object to restore and click **Restore** in the **Operation** column. To restore multiple archived objects at a time, select them all in the object list, and click **Restore** from the **More Actions** drop-down list at the top.
6. In the pop-up window, configure the restoration mode and the validity period (in days) of the copy.

Restore Archived Objects

StatusArchive Storage [Detail]

Recovery ModeStandard mode

You can download a copy after 2019-09-29 22:14:20

Validity*1

The copy will automatically expire after 2019-10-01 00:00:00

OKCancel

The parameters are described as follows:

Restoration Mode: Expedited, standard, or bulk retrieval.

Expedited retrieval: This is the fastest mode. Archived files can be restored within 1-5 minutes. If you need to access your archival data urgently, you can use this mode to greatly reduce the restoration time. **Please note that the expedited retrieval mode is not available for DEEP ARCHIVE.**

Standard retrieval: Files can be restored from ARCHIVE within 3-5 hours, and from DEEP ARCHIVE within 12 hours.

Bulk retrieval: This is the lowest-cost mode. If your need for the archival data is not urgent, this mode can usually restore massive amounts of data from ARCHIVE within 5-12 hours, and from DEEP ARCHIVE within 48 hours, both with an ultra-low cost.

Note:



The QPS of data restoration requests is limited to 100.

Validity: The number of days after which the copy will 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 copy in the pop-up window.

7. Click **OK**. The object enters the restoration process.

During this process, you can click **Details** to go to the object details page to check the restoration progress.

Basic Information

Object Name	exampleobject.zip
Object Size	13.78KB
Storage Class	Archive Storage (Restoring)
Last Modified	2019-03-21 12:05:51
ETag	"7007d843b054a0abaeb2c57a25747381"
Specified Domain①	<div>Default Origin Domain ▾</div>
Object Address①	https://examplebucket-125[REDACTED].cos.ap-chengdu.myqcloud.com/exampleobject.zip 
Temporary Link①	 Copy Temporary Link

8. After confirming that the object has been successfully restored, you can go to the object details page to perform access, download, and other operations on the object.

Restore Archived Objects ✕

Status

Restored [\[Detail \]](#)

The copy will automatically expire after 2019-10-01 00:00:00

Rescheduled *

☒

2

The copy will automatically expire after 2019-10-02 00:00:00

OK

Cancel

To modify the validity period of the copy, follow step 5 to click **Restore** again and modify the validity period in the pop-up window.

Basic Information

Object Name exampleobject.zip

Object Size 13.78KB

Storage Class Archive Storage (Restored. The copy will automatically expire after 2019-10-01 00:00:00

Last Modified 2019-03-21 12:05:51

ETag "7007d843b054a0abaeb2c57a25747381"

Specified Domain①

Object Address① <https://examplebucket-1250000000.cos.ap-chengdu.myqcloud.com/exampleobject.zip>

Temporary Link① [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 18:19:13) .

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

Folder Management

Creating Folder

Last updated : 2024-01-06 15:06:14

Overview

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. For more information, see [Folder and directory](#).

Note:

The length of the folder name cannot exceed 255 characters, and the following ASCII control characters are not supported:

Up (↑): CAN (24)

Down (↓): EM (25)

Right (→): SUB (26)

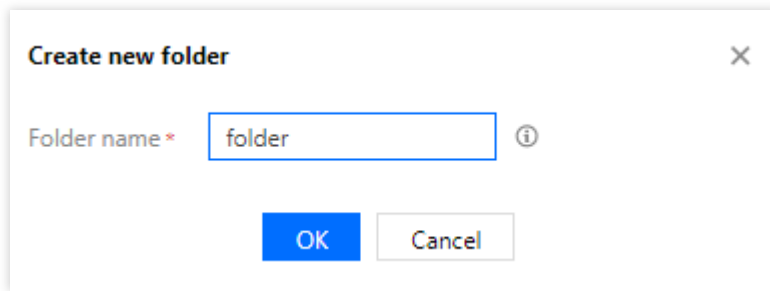
Left (←): ESC (27)

Prerequisites

A bucket is created. For operation details, see [Creating a Bucket](#).

Directions

1. Log in to the [COS console](#).
2. Click **Bucket List** on the left sidebar.
3. Locate the bucket for which a folder is to be created, and click the bucket name to go to the bucket management page.
4. Click **File List** on the left sidebar.
5. Click **Create Folder**.
6. In the pop-up window, enter the folder name and click **OK**.

**Note:**

Folders cannot be renamed. Please exercise caution when naming folders.

Folder naming rules are as follows:

The folder name can contain digits, letters, and visible characters.

A subdirectory can be created quickly by separating the path by a slash (/).

Do not start with / or use two or more / consecutively.

Do not leave the folder name empty.

Do not use . . as the folder name.

Deleting Folder

Last updated : 2024-01-06 15:06:14

Overview

You can delete a created folder in the COS console.

Note:

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

Directions

1. Log in to the [COS console](#).
2. In the left sidebar, click **Bucket List** to go to the bucket list page.
3. Locate the bucket where the folder to delete resides, and click the bucket name to go to the bucket management page.
4. In the left sidebar, choose **File List** to go to the file list page.
5. Locate the folder to delete, and click **Delete** in the **Operation** column.
6. In the pop-up window, click **OK**.

Sharing Folder

Last updated : 2024-01-06 15:06:14

Overview

You can share a created folder using the COS console.

Directions

1. Log in to the [COS console](#).
2. Click **Bucket List** on the left sidebar.
3. Click the name of a bucket where the folder to share is stored.
4. Click **File List** on the left sidebar.
5. Find the folder to share, and click **More > Share Folder** in the **Operation** column.
6. In the pop-up window, configure **Permission**, **Validity Period**, and **Password**. Then, click **OK**.
7. You can now view the generated share link in the pop-up window. Click **Copy Link and Password** and share it with others.
8. The recipient can enter the password and view the shared folder as well as the files in it.
9. On the share file page, the recipient can download the file, or view information such as the object storage class, size, and modification time.

Viewing Folder Details

Last updated : 2024-01-06 15:06:14

Overview

In the COS console, you can view the details about folders, including the number and size of objects in them. This document describes how to view folder details.

Note:

COS stores objects in a flat structure with no traditional folder concept. To make COS easy to use, we use objects whose object keys are suffixed with `/` as folders, but actually a "folder" in COS is an object occupying 0 KB.

If you want to query the number and size of all objects in the current bucket, you can get an inventory report with the inventory feature. For more information, see [Inventory Overview](#).

If the total number of objects in the current folder exceeds 10,000, we recommend that you use the inventory feature to count the objects. For more information, see [Inventory Overview](#).

Directions

1. Log in to the [COS console](#).
2. Click **Bucket List** on the left sidebar.
3. Locate the bucket where the folder is located and click the bucket name to go to the bucket management page.
4. Click **File List** on the left.
5. Locate the folder whose details you want to view, and click **Statistics** in the **Operation** column.
6. In the pop-up window, you can view the statistical information of the folder, including the total number and size of objects.

Note:

Nested folders inside a folder are counted as objects.

Example 1: If a folder contains 1 empty folder and 5 objects, 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, the total number of objects in the folder will be 8.

Setting Folder Permissions

Last updated : 2024-06-03 11:14:27

Overview

You can set access permissions for folders through the Cloud Object Storage (COS) console, allowing users to perform specified operations on them. We recommend that you follow the [principle of least privilege](#) when configuring permissions to protect your data assets.

Note:

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.

Folder permissions are essentially access permissions at the object level, which take precedence over the bucket access permissions. Unlike object access permissions, folders support setting public read and write. For more information about object access permissions, refer to [Access Permission Types](#) in the object overview.

Directions

1. Log in to the [COS console](#).
2. In the left sidebar, click **Bucket List** to go to the bucket list page.
3. Locate the bucket where the folder is located and click the bucket name to go to the bucket management page.
4. In the left sidebar, choose **File List** to go to the file list page.
5. Locate the folder for permission setting, and click **Permission**.
6. In the pop-up window, set folder permissions as required. Permission settings are described as follows:

Permission Type	Parameter	Description
Public permission	Inherit	Default value, consistent with the bucket permission.
	Private Read/Write	Only the root account has the read and write permissions on the folder. Non-root accounts (sub-accounts, the root accounts of other users, or anonymous users) cannot access the folder.
	Public Read/Private Write	The root account has the read and write permissions on the folder. Non-root accounts (sub-accounts, the root accounts of other users, or anonymous users) can read content in the folder but cannot write new data into the folder.

	Public Read/Write	Both the root account and non-root accounts (sub-accounts, the root accounts of other users, or anonymous users) have the read and write permissions on the folder.
User ACL	User Type	`Root account` indicates the root account of other users. `Sub-account` indicates the sub-account under the current root account. To grant the access permission to a sub-account of another root account, you need to grant the access permission to that root account first and then grant the access permission to the sub-account from that root account.
	Read	Permission to read data
	Write	Permission to write data
	Read ACL	Permission to read folder permission configuration. With this permission, you can obtain folder permission configuration details.
	Write ACL	Permission to modify folder permission configuration. With this permission, you can modify folder permission configuration details. Exercise caution with this configuration because it will cause permission changes.
	Full control	Includes the Reads, Write, Read ACL, and Write ACL permissions. Exercise caution with this configuration because it grants a wide range of permissions.

7. Click **Save** in the **Operation** column.

8. Click **Close**.

Data Extraction

Last updated : 2024-01-06 15:06:15

Overview

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

Note:

COS Select currently supports objects in JSON or CSV format only in public cloud regions (Chinese mainland), and objects in Parquet format only in Beijing region.

Please make sure the file to be extracted complies with COS Select specifications. For more information on COS Select specifications, please see [SELECT Overview](#).

COS Select in the console supports extraction of up to 40 MB data from a maximum of 128 MB files. To process larger files or extract more data, please use the [API](#) or SDKs.

Directions

1. Log in to the [COS console](#).
2. Click **Bucket List** on the left sidebar.
3. Locate the bucket where the object resides and click the bucket name.
4. Click **File List** on the left sidebar.
5. Find the target object and click **More > Extract** on the right.

Note:

Currently, only objects in the STANDARD, STANDARD_IA, and INTELLIGENT TIERING storage classes can be extracted.

6. Configure the fields **File Type**, **Header Field**, **Separator**, **Compression Format**, and **Export Format**.

7. Click **Select SQL Template**.

8. In the pop-up window, select the template statement you want to use for extraction and click **OK**.

9. Edit the statement in the text box based on your actual file and then click **Run SQL**.

Now you can see the first 100 results in the text box at the bottom. To obtain the complete set of data, click **Export Extraction Results**.

Setting Object Tag

Last updated : 2024-01-06 15:06:14

Overview

Object tagging is designed to help you group and manage objects in your bucket by adding a key-value pair as an object tag. An object tag consists of a `tagKey` , a `=` , and a `tagValue` , such as `group = IT` . You can set, query, and delete tags on the specified object.

Notes

Object tagging is a paid feature. For detailed pricing, see [Pricing | Cloud Object Storage](#).

You can add up to ten unique tags for an object.

Tag keys and tag values are case-sensitive. Both of them can contain 1–127 UTF-8 letters, spaces, digits, or special symbols `+ - = . _ : / @` .

For more restrictions, see [Object Tag Overview](#).

Directions

Adding tag during object upload

1. You can add a tag when [uploading an object](#) as shown below:

Upload Files

✓ Select Objects

>

2 Set Properties

Properties Setting will be applied to all the objects to be uploaded, you can also upload directly and then modify the settings in file list page.

Storage Class

☒ Standard Storage

It is suitable for business scenarios such as real-time access to a large number of hot files and frequent data interaction. Supported in all regions.

☐ Standard_IA Storage

It is suitable for business scenarios with low access frequency (e.g., average access frequency is 1 to 2 times per month). Supported in all regions.

☐ Archive Storage

It is suitable for business scenarios with very low access frequency (e.g., once every six months). Since real-time response is not supported, if you want to retrieve the archived data, please apply in advance.

Access Permissions

☒ Inherit ☐ Private Read/Write ☐ Public Read/Private Write

Server-Side Encryption

☒ None ☐ SSE-COS ⓘ

Object Tag

Group

IT

+

Metadata

Parameter	Value	Actions
Select Project ▼	Value	Delete
Add Parameters		

Previous

Upload

2. After successful upload, the object tag will be added.

You can go to the **File List** page of the bucket, find the tagged object, and click **More > Add Tags** to view, edit, or delete the added tag.

Object Tag		
Tag Key ①	Tag Value ①	Actions
group	IT	Edit Delete
Add Tags		

Adding tag uploaded object

If you did not add tags when uploading a new object, follow the steps below to add them subsequently.

1. Go to the **File List** page as instructed in [Viewing Object Information](#).
2. Find the target object and click **More > Add Tags**.
3. In the pop-up window, click **Add Tags**, enter the tag key and value, and save.

To modify or delete the tag, click **Edit** or **Delete** in this window.

Related Operations

Using object tag

After the object tag is set, you can set a lifecycle rule for objects with the same object tag. For more information, see [Setting Lifecycle](#).

Exporting Object URLs

Last updated : 2024-01-06 15:06:14

Overview

The COS console allows you to export the URLs of objects in a bucket, including objects that have been uploaded or in a folder. Batch export is supported.

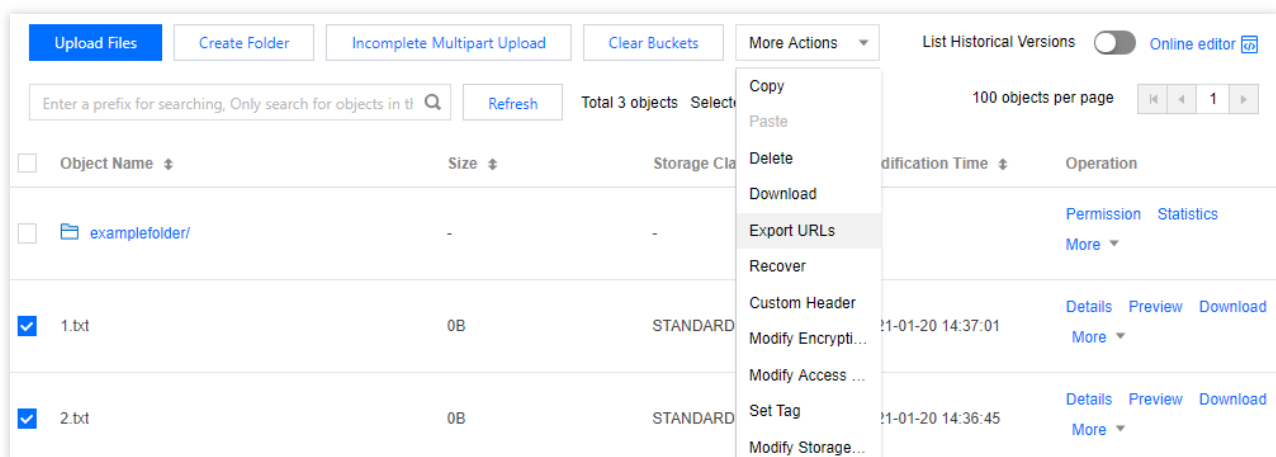
Note:

You can export up to 100 object URLs at a time, meaning you can select a maximum of 100 objects.

If you need to export more than 100 object URLs, you can use APIs or SDKs. For more information, please see [GET Bucket \(List Objects\)](#).

Directions

1. Log in to the [COS console](#).
2. Click **Bucket List** on the left sidebar.
3. Locate the bucket where the object resides and click the bucket name.
4. Click **File List** on the left sidebar.
5. Select the desired objects, click **More Actions > Export URLs**.



6. In the pop-up window, configure the following information:

Export Object URLs

Up to 100 object URLs can be exported at a time.

If the number of object URLs>100, export with APIs/SDKs. For details, see[GET Bucket \(List Objects\)](#) .

Protocol

☒ HTTPS ☐ HTTP

Specified Domain

Default Endpoint

Expiration Time ⓘ

min

Confirm

Cancel

Protocol: HTTPS is selected by default. You can select HTTPS or HTTP as needed.

Specified Domain: the default origin domain is supported.

Expiration Time: The default value is 60 minutes. You can set it to an integer ranging from 5 to 60.

7. Click **Confirm** to export the object URLs.

8. In the exported file, you can view the object names and object URLs. Note that you need to view the URLs within the validity period.

Restoring Historical Object Version

Last updated : 2024-03-25 14:38:14

Overview

This document describes how to restore a historical object version as the latest version in the COS console. For more information on versioning, see [Overview](#).

Note:

Object restoration refers to restoring a historical object version as the latest one with the historical version retained. To delete a historical version, see [Setting Versioning](#) and [Deleting Objects](#). Currently, you can only restore objects one by one instead of in batches.

Notes

The following describes the scenarios and rules for object restoration.

Scenarios	<p>A bucket with versioning enabled supports object restoration.</p> <p>A bucket with versioning enabled and then suspended supports object restoration.</p> <p>A bucket with versioning never enabled does not support object restoration.</p>
Restorage rules	<p>Historical versions can be restored.</p> <p>The latest version cannot be restored.</p> <p>Versions with delete markers cannot be restored.</p>

Prerequisites

Before you restore an object, ensure that you have enabled versioning for the bucket. If not, enable it by referring to [Setting Versioning](#).

Directions

1. Log in to the [COS console](#).
2. Click **Bucket List** on the left sidebar.
3. Locate the bucket where the object resides and click the bucket name.
4. Click **File List** on the left sidebar.

5. Click **List Historical Versions**, find the object to restore, and click **Restore** in the **Operation** column on the right.
6. In the pop-up window, check the information of the object version to be restored and click **OK**.
7. View the restored version of the object in the file list.

Batch Operation

Last updated : 2024-03-25 14:40:20

Overview

The COS batch operation feature allows you to perform large-scale batch operations on objects in a bucket. With this feature, you can now perform the following operations in batches:

Copying objects

Restoring archived objects

You can generate an inventory file for the objects on which to perform a batch operation by using either COS inventory (you need to first enable the inventory feature as instructed in [Setting Inventory](#)), or the CSV format you specify. COS will then perform this batch operation based on the inventory file. For more information on batch operations, see [Batch Operation Overview](#).

Directions

1. Log in to the [COS console](#).
2. On the left sidebar, click **Batch Operation** to enter the batch operation management page.
3. Click **Create Job** to create a batch operation job.

The configuration items are as described below:

Job Region: Select a region for the job. It must be the same as the bucket region where the objects in your inventory file reside; otherwise, the job will fail.

Note:

Currently, COS batch operation is only available in public cloud regions in Chinese mainland and Silicon Valley region.

Inventory Format: Select a format for the objects to be inventoried from the following two options:

Inventory Format	Field	Configuration Description
COS inventory report	-	You can use an inventory report generated by COS as the inventory file or create your own inventory file in CSV format.
CSV	Bucket	Bucket name
	Key	Name of the object in a bucket. The object name encoded in URL format must be decoded and then can be used properly.

	VersionId	Object version ID. If versioning is enabled for a bucket, COS will assign a version ID to each object added to the bucket. If you don't want to inventory the latest version of an object, you can specify a particular version ID.
--	-----------	---

Inventory Bucket: Select the bucket where the inventory file is stored.

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

4. Click **Next** and select the job type.

The configuration items are as described below:

Batch data copy:

Destination Bucket: Select the bucket to store the object copies.

Prefix Operation: You can choose to add, replace, or delete the prefix on the object copies.

Storage Class: Specify the storage class for object copies. Valid values: STANDARD; STANDARD_IA; ARCHIVE.

Server-Side Encryption: Specify whether to encrypt the object copies. Valid values: None; SSE-COS.

Access Permission: Set access permissions to the object copies. Valid values: Copy all permissions; Replace all permissions; Add new permissions.

Object Metadata: Configure metadata for the object copies. Valid values: Copy all metadata; Replace all metadata; Add new metadata.

Object Tag: Configure tags for the object copies. Valid values: Copy all tags; Replace all tags; Add new tags.

Restored archived objects in batches:

Restoration Mode: You can select either standard or bulk mode. For more information on restoration modes, see [Restoring Archived Objects](#).

Validity: Specify the number of days after which the object copies will expire and be automatically deleted. Value range: 1-365.

5. Click **Next** and configure the following options.

Job Description (optional): Description of the job. This field can be empty.

Job Priority: A job of a higher priority will be performed first. The value must be a positive integer. A larger value indicates a higher priority.

Job Report: Select whether to generate a job report.

CAM Role: You can create a CAM role or select an existing role to grant operation permissions to COS.

Note:

For COS to perform batch operations, you need to use a CAM role to grant permissions. For more information on CAM roles, see [Role Overview](#).

6. Click **Next**, check the batch operation job configuration you set, and select **If you select this option, the job will be directly started after creation. Make sure that the above configuration information is correct.** as needed. To modify the information, click **Modify** or **Previous**.

7. After confirming that everything is correct, click **Create** or **Create and Start**.

Once completed, you can find the new job in the job list. If you want to cancel the job, click **Cancel Job** under **Operation**.

Monitoring Reports

Viewing Data Overview

Last updated : 2024-01-06 15:14:56

Overview

You can go to the **Statistic** page in the COS console to view the number of buckets/objects/requests, storage usage, traffic, and other data.

Note:

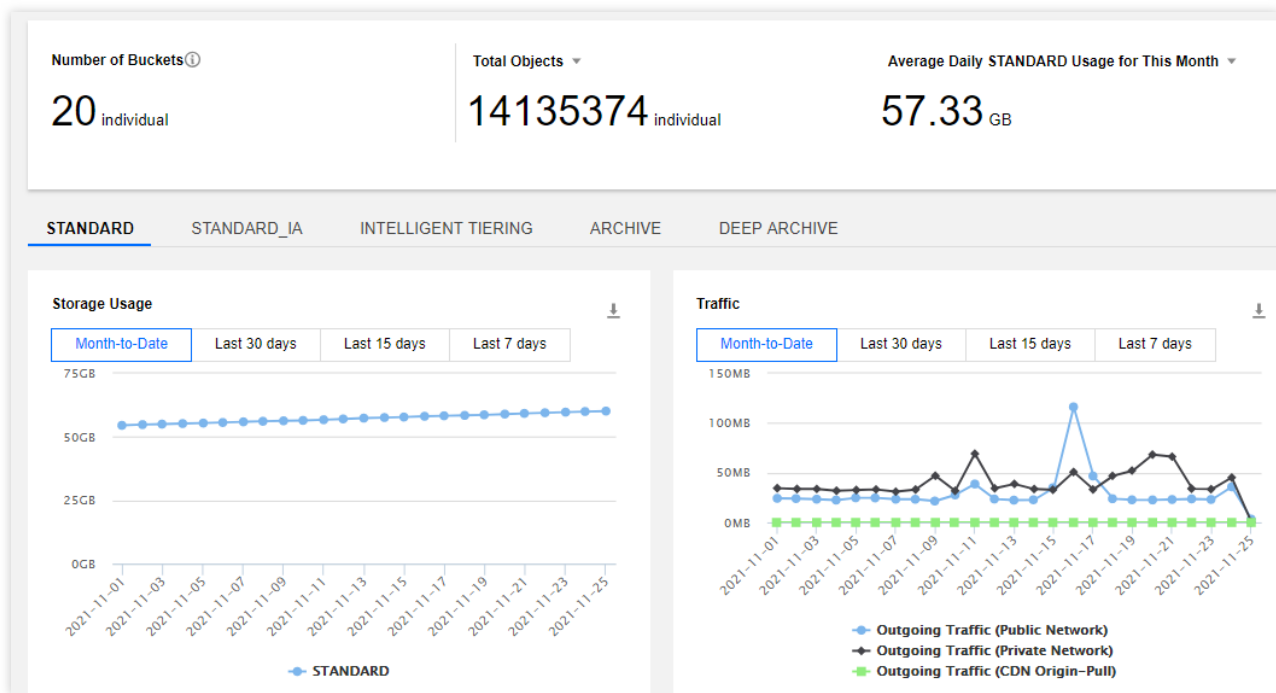
If a sub-account needs to view the statistics, it needs to have permission to **access the bucket list**. For more information, see **Adding a Preset Policy** in [Accessing Bucket List Using Sub-Account](#).

Except for the **number of buckets**, other data is not real-time and has a delay of about 2 hours. The data is for monitoring purposes only. To view the accurate billing data, go to [Billing Center](#).

Viewing Line Charts

Directions

1. Log in to the [COS console](#) and click **Statistic > Basic Statistic** on the left sidebar.
2. On the **Basic Statistic** page, you can view the following information:



Number of Buckets: number of buckets that have been created

Total Objects: number of objects that have been created in all buckets. You can view the number of objects by storage class.

Average Daily Usage for This Month: The average daily usage by storage class (i.e., STANDARD, MAZ_STANDARD, STANDARD_IA, MAZ_STANDARD_IA, INTELLIGENT TIERING, MAZ_INTELLIGENT TIERING, ARCHIVE, and DEEP ARCHIVE). Daily storage usage = sum of the "5-minute usage"/288 (number of statistical points). Average daily storage usage for this month = sum of the daily storage usage in this month/number of days in this month.

Storage Usage: Storage usage for STANDARD, MAZ_STANDARD, STANDARD_IA, MAZ_STANDARD_IA, INTELLIGENT TIERING, MAZ_INTELLIGENT TIERING, ARCHIVE, and DEEP ARCHIVE. You can view the data for the past 93 days, and the time range for each query cannot exceed 31 days.

Traffic: Public/private downstream traffic and CDN origin-pull traffic for STANDARD, MAZ_STANDARD, STANDARD_IA, MAZ_STANDARD_IA, INTELLIGENT TIERING, and MAZ_INTELLIGENT TIERING. You can view the data for the past 93 days, and the time range for each query cannot exceed 31 days.

Request Count: Number of read/write requests for STANDARD, MAZ_STANDARD, STANDARD_IA, MAZ_STANDARD_IA, INTELLIGENT TIERING, and MAZ_INTELLIGENT TIERING. You can view the data for the past 93 days, and the time range for each query cannot exceed 31 days.

Request Success Rate: Request success rate for STANDARD and MAZ_STANDARD. You can view the data for the past 93 days, and the time range for each query cannot exceed 31 days.

Data Retrieval: The amount of data retrieved for STANDARD_IA, MAZ_STANDARD_IA, INTELLIGENT TIERING, MAZ_INTELLIGENT TIERING, ARCHIVE, and DEEP ARCHIVE. For ARCHIVE, the amount is classified into

expedited retrievals, standard retrievals, and bulk retrievals. You can view the data for the past 93 days, and the time range for each query cannot exceed 31 days.

3. You can click the download button in the upper-right corner of each chart to download the data.

Viewing Bucket-Level Data

Directions

1. Log in to the [COS console](#), click **Bucket List** on the left sidebar, and click **Statistical Data**.
2. On the **Statistical Data** page, you can view the bucket data such as storage usage, data retrievals, traffic, and request count within a specified period of time.

Querying Monitoring Data

Last updated : 2024-01-06 15:14:56

Overview

COS allows you to monitor your stored data. The COS data monitoring window displays information regarding request quantity, traffic, return code, data retrieval, etc. You can also query the details and trends of data in different storage classes for different time periods. The following describes how to view the monitoring data of a single bucket with a root account or sub-account.

Note:

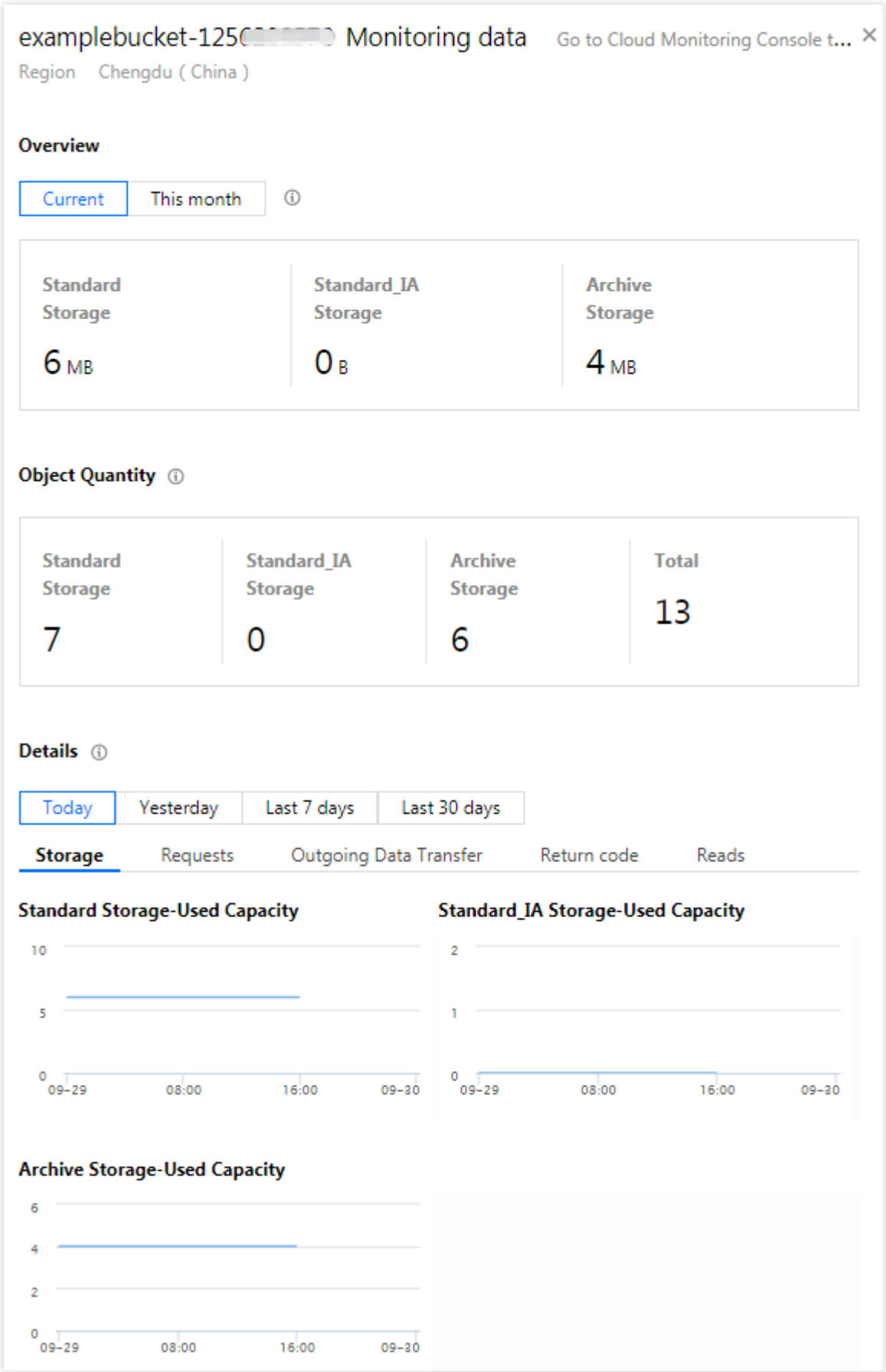
To view the summary of all data stored under your account, go to [Data Monitoring](#) in the COS console.

Querying with Root Account

1. Log in to the [COS console](#).
2. Click **Bucket List** on the left sidebar.
3. Find the target bucket and click **Monitor** on the right.

You can also select the target bucket and click **Data Monitoring** on the left sidebar on the bucket details page.

4. On the monitoring data page, view the information.



Monitoring items are as described below:

Storage: Storage usage of each storage class.

Number of Objects: Number of objects (including incomplete multipart uploads) stored in the bucket.

Number of Incomplete Multipart Uploads: Number of incomplete multipart uploads stored in the bucket. If an ongoing upload is suspended or canceled, the corresponding files will be stored in the bucket as incomplete multipart uploads.

Note:

To query the number of objects in a folder, see [Viewing Folder Details](#).

If versioning is enabled, multiple versions of an object are counted as separate objects.

Requests: Number of all requests (including GET and PUT requests), as well as read/write requests of STANDARD and STANDARD_IA.

Traffic: Public/Private network traffic, CDN origin-pull/cross-region replication traffic, and total upload traffic over public and private networks.

Return Code: Number of 2xx, 3xx, 4xx, and 5xx status codes as well as their proportion.

Data Retrieval: Statistics of data retrievals from STANDARD_IA.

Note:

Under **Details** in the **Current** section, you can query monitoring data (including storage usage, number of objects, requests, traffic, return code, and data retrieval) of different time periods, such as today, yesterday, last 7 days, last 30 days, or a custom time period.

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

Storage and **Number of Objects** show only data after March 1, 2020. For more detailed data, go to [Billing Center](#), select a time period, and export the data.

Querying with Sub-account

To query monitoring data with a sub-account in the console, you need to first grant the sub-account relevant permissions.

You can grant such permissions by using a **policy template** or **custom access policy**.

Authorizing by policy template

1. Log in to the [CAM console](#) as the root account and select **Users > User List** to enter the user list page.
2. Find the target sub-account and click **Authorize** in the **Operation** column on the right.
3. Search for and select the `QcloudMonitorFullAccess` policy in the pop-up window and click **OK** to associate it with the sub-account. Then, the sub-account can access monitoring reports.

Note:

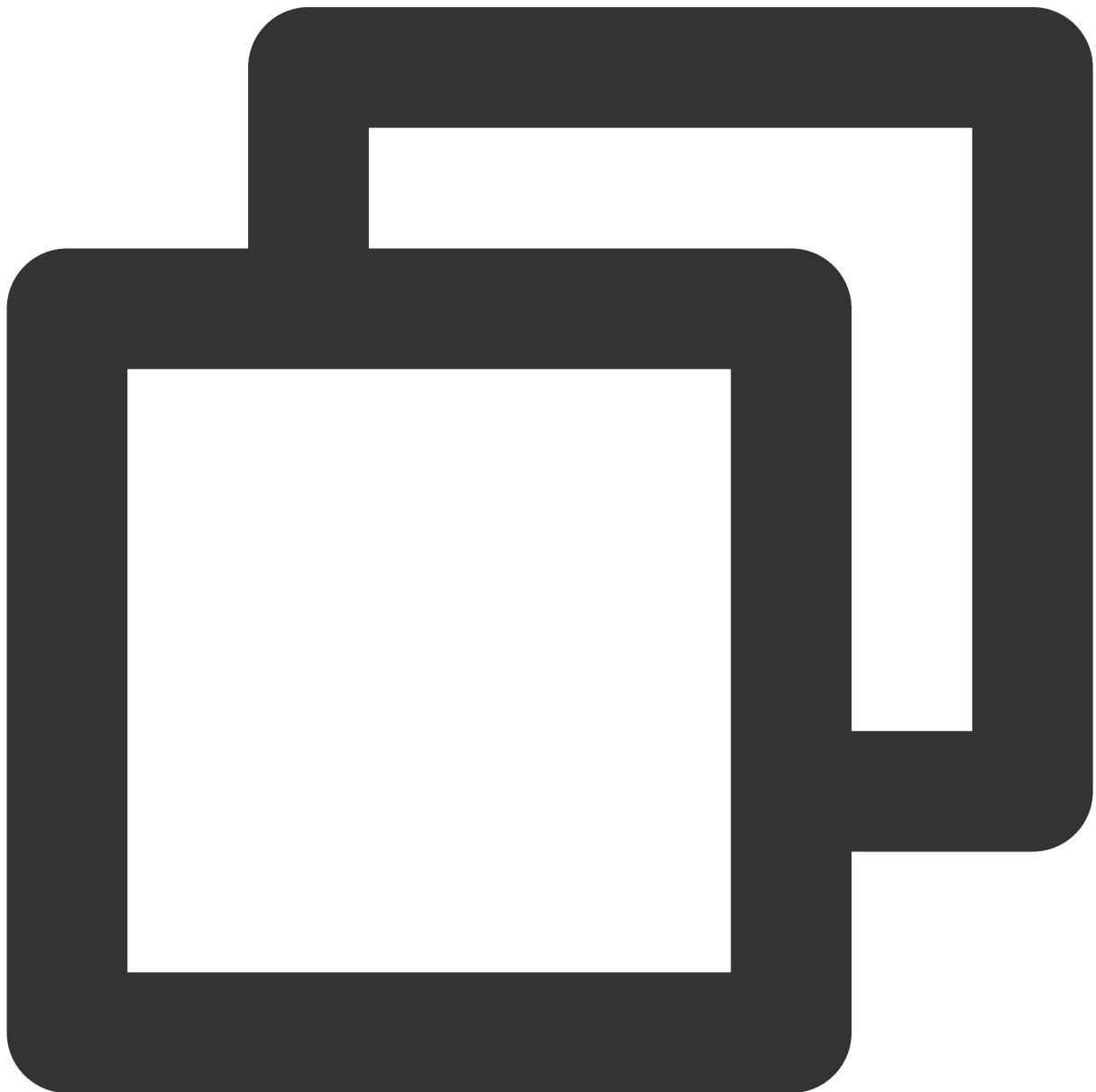
This policy template grants the sub-account the **full access** to CM. To protect the security of your account, you can customize an access policy to grant only read permissions to the sub-account.

Authorizing by custom access policy

1. Log in to the [CAM console](#) as the root account.
2. On the left sidebar, click **Policies** > **Create Custom Policy** > **Create by Policy Syntax**.
3. Select **Blank Template** and click **Next**.
4. Copy and paste the following policy syntax into the **Policy Content** input box.

You can rename the policy as needed.

Policy syntax:



```
{  
  "version": "2.0",
```

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

✓

Select policy template

>

✓

Edit Policy

Policy Name *

policygen-20190815202830

Notes

Edit Policy Content

```
1 {  
2   "version": "2.0",  
3   "statement": [  
4     {  
5       "effect": "allow",  
6       "action": [  
7         "monitor:GetMonitorData"  
8       ],  
9       "resource": "*"   
10    }  
11  ]  
12 }
```

[Policy Syntax Description](#)

[Support service list](#)

Previous

Create Policy

5. Click **OK**.

After the policy is created successfully, you can associate it with the sub-account as instructed in [Authorizing by policy template](#).

Setting Alarm Policies

Last updated : 2024-01-06 15:14:56

Overview

You can leverage the alarm policy feature of Cloud Monitor to set threshold-reaching alarms for COS monitoring metrics. An alarm policy must include the policy name, policy type, trigger condition, alarm object, and alarm notification template. You can create an alarm policy for COS as instructed below.

Note:
Tencent Cloud’s Cloud Monitor enables users to monitor cloud resources in real time and provides alarm services. Users can set alarm policies for COS monitoring metrics to query the alarm history and receive alarm notifications. For more information, please see [Creating Alarm Policy](#).

Directions

1. Log in to the [COS console](#). On the **Overview** page, click **Configure Alarm Policy** in the **Alarm Configuration** section.

Note:
Alarm Configuration can also be found on the **Overview** page of each bucket.
2. Configure a new alarm policy as shown below:

Configuration Type	Configuration Item	Description
Basic info	Policy name	A custom policy name
	Remarks	Remarks for the policy
	Monitor Type	Choose Cloud Product Monitoring.
	Policy type	Choose COS.
	Project	Setting the policy project allows you to: Manage alarm policies. Alarm policies of a project can be quickly located in the alarm policy list. Manage instances. You can choose the project as needed. Instances of the project can be quickly located in Alarm Object. You can distribute Tencent Cloud services to the desired project according to your business types. After the project is created, you can distribute resources to projects in the console of each Tencent Cloud service. Some Tencent Cloud services cannot be

		distributed to a project. If you do not have project permission, please see Cloud Access Management (CAM) for authorization.
Configure alarm rule	Alarm object	<p>If you choose Instance ID in the drop-down list, select the bucket you want to add an alarm to.</p> <p>If you choose Instance Group in the drop-down list, the alarm policy is bound to the selected instance group. If there is no instance group, you can click Create Instance Group on the right to create a group for the bucket first.</p> <p>If you choose All Objects in the drop-down list, the alarm policy is bound to all buckets the current account has permission on.</p>
	Select template	Select a configured template from the drop-down list. For more information on the configuration, see Configuring Trigger Condition Template . If the newly created template is not displayed, click Refresh on the right.
	Manual configuration(Metric alarm)	<p>Trigger condition: Consists of metric, comparison, threshold, statistical period, and the number of consecutive periods. For example, if the metric is set to `STANDARD storage read requests`, comparison to `>`, threshold to `80` times, statistical period to `5` minutes, and the number of consecutive periods to `Last 2 periods`, STANDARD storage read requests are collected every 5 minutes, and if the number of STANDARD storage read requests in a bucket is greater than 80 in 2 consecutive periods, the alarm will be triggered.</p> <p>Alarm frequency: You can set a repeated notification policy for each alarm rule. In this way, an alarm notification will be sent repeatedly at a specified frequency when an alarm is triggered.</p> <p>Frequency options: do not repeat, once every 5 minutes, once every 10 minutes, at an exponentially increasing interval, and other frequency options.</p> <p>An exponentially increasing interval means that a notification is sent when an alarm is triggered the 1st time, 2nd time, 4th time, 8th time, and so on. In other words, the alarm notification will be sent less and less frequently as time goes on to reduce the disturbance caused by repeated notifications.</p> <p>Default logic for repeated alarm notifications: The alarm notification will be sent to you at the configured frequency within 24 hours after the alarm is triggered. After 24 hours, the alarm notification will be sent once a day by default.</p>

Configure alarm notification	Alarm notification	Select a preset or custom notification template. Each alarm policy can be bound to three notification templates at most.
Advanced configuration	Auto scaling	If enabled, the auto scaling policy can be triggered when the alarm condition is met.

3. After configuring the above information, click **Complete**.

Data Processing

Image Processing

Basic Image Processing

Last updated : 2024-01-06 15:14:56

Overview

This document describes how to use COS Image Processing in the console, with the following two methods available for you. For more information on image processing, see [Image Processing Overview](#).

Adding parameters to an image URL: You can process an image by adding parameters after the object URL of the image.

Using an image style: You can save different processing results by creating styles, and use such styles to standardize your image processing. The style created is an assembled template designed to process parameters in real time when an image is downloaded.

Note:

Image Processing is available only in public cloud regions.

Image Processing is charged by CI. For detailed pricing, see **Basic image processing fee** in [Billing and Pricing](#).

Adding URL parameters

1. Log in to the [COS Console](#).
2. Locate the bucket that stores the image, and click the bucket name to enter the bucket management page.
3. Click **Details** in the **Operation** column for the image to enter its details page.
4. Copy the **Object URL** and paste it into the address bar of your browser.

Note:

To process an image, you need the write permission on objects. For object permissions setting, see [Setting Object Access Permission](#).

5. In your address bar, add parameters after the object URL using the format below. For more image processing parameters and instructions, see the Cloud Infinite API documentation [Basic Image Processing](#).



```
Object URL?processing API name/processing operation name/processing parameter
```

Note:

If the access permission on the image file is private-read, you need to add image processing parameters to the signed address.

Example: scaling an image to 50% of its original size

Suppose that the original image is displayed as below, the access permissions on the object are public read and private write, and the object URL is `https://examplebucket-1250000000.cos.ap-chengdu.myqcloud.com/sample.jpeg` .



Next, add the following parameters to the URL:

Scaling API: imageMogr2

Scaling operation name: thumbnail

Processing parameter: !50p

Now, you obtain a new URL with added parameters `https://examplebucket-1250000000.cos.ap-chengdu.myqcloud.com/sample.jpeg?imageMogr2/thumbnail/!50p`. Paste this URL to your address bar, press Enter, and you will see a scaled image as shown below:



Using an image style

Image Style can help you present different processing parameters in the format of template to standardize your image processing. The style created is an assembled template designed to process parameters in real time when an image is downloaded. Now, let's take **Image Style: width: 480px, height: 270px** as an example, and introduce how to use this feature:

1. Log in to the [COS console](#).
2. Locate the bucket that stores the image, and click the bucket name to enter the bucket management page.
3. In the left menu bar, click **Data Processing > Image Processing** to enter the **Style Management** section.

Separator: Style separators are symbols that separate filenames and processing styles, including `-`, `_`, `/`, and `!`. Select `!` here and save.

4. Click **Add Styles** and set fields as follows:

Style Name: Enter your custom style name, such as "yunstyle".

Note:

Note that style names are case-sensitive and cannot be modified once saved.

For the purpose of clarity, the separator you have enabled cannot appear in the style name.

Editing Mode: Select **Basic**.

Resize Mode: Select **Scale-only**.

Scaling: Select **Fixed height and width**.

Size: width: 480px, height: 270px.

Progressive Display: Once enabled, the images you access will be displayed progressively. It is disabled by default.

Retain the default setting here.

Output: Choose a format of the output image. Retain the default value **Original** here.

5. Once your configuration is done, You can click the **Preview** button on the right for preview.
6. After the preview, click **Save**, and you will see that an image style named "yunstyle" has been added.

Note:

Up to 100 styles can be set for a single bucket.

The settings take effect in 30 minutes on average.

Changing a separator requires clearing the cache. It takes at least 24 hours for separator changes to take effect globally.

Canceling a separator used may cause product feature malfunctions.

For more information on image styles, see [Setting Styles](#).

7. Go to the object details page, copy the object URL, and enter your separator and style name after the URL in the following format:



Object URL + Separator + Processing style name

Now, you can obtain a final object URL `https://examplebucket-1250000000.cos.ap-chengdu.myqcloud.com/sample.jpeg!yunstyle`. Paste it to your address bar, press Enter, and you will see a scaled image shown as below:



If you need to set a signature for the styled image, change the URL to `https://examplebucket-1250000000.cos.ap-chengdu.myqcloud.com/sample.jpeg!yunstyle?q-sign-algorithm=<signature>`, and use `/sample.jpg!yunstyle` as the resource to calculate the signature `<signature>`.

Setting Image Advanced Compression

Last updated : 2024-01-06 15:14:56

Overview

Image Advanced Compression is a COS feature based on Cloud Infinite. It allows you to easily convert images into formats that provide a high compression ratio, such as TPG and HEIF. This effectively reduces the transmission time, loading time, and the use of bandwidth and traffic.

Note

You can use Image Advanced Compression to convert JPG, PNG, or WebP images into TPG or HEIF.

To use the TPG format, ensure that **the environment where images are loaded supports TPG decoding**. CI provides the TPG decoder–integrated SDK for iOS, Android clients to facilitate quick integration with TPG.

Currently, iOS 11 or later and Android P have native support for the HEIF format.

Image Advanced Compression is charged by CI. For detailed pricing, please see [Billing and Pricing](#).

Directions

1. Log in to the [COS console](#).
2. Click **Bucket List** in the left sidebar.
3. Click the bucket you want to enable Image Advanced Compression for.
4. Click **Data Processing > Image Processing**.
5. Find the **Image Advanced Compression** area, click **Edit**, enable the status, and click **Save**.

Image Advanced Compression [Edit](#)

Status Enabled

- * The advanced image compression feature can convert the image in JPG/ PNG/ GIF/ WEBP formats into TPG/HEIF formats. For related settings a
- * This feature is a paid feature. For billing details, please see [Billing and Pricing](#) .
- * After the service is enabled, you can use the corresponding image compression API to convert formats for the image resources in the current b
- * Note: to use the advanced image compression feature, you need to have access permission to the processing image.

Once Image Advanced Compression is enabled, you can call the [Image Advanced Compression](#) API to convert images in the bucket into TPG/HEIF upon download.

File Processing

Setting File Processing

Last updated : 2024-01-06 15:14:56

Overview

The COS console allows you to preview documents in a bucket. This document describes how to use the document preview feature in the console. For information on document preview, see [Document Preview Overview](#).

Note:

The document preview feature is available in public cloud regions in the Chinese mainland and Silicon Valley, Virginia, Frankfurt, and Singapore. Currently, only document-to-image conversion preview is supported in Singapore and Silicon Valley.

Document preview is charged by CI. For detailed pricing, see [Billing and Pricing](#).

Directions

1. Log in to the [COS console](#).
2. Click **Bucket List** on the left sidebar, and then click the bucket for which you want to enable the document preview feature.
3. Click **Data Processing** > **Document Processing**. In the **Document Preview** area, click **Edit** and toggle on the status
4. To preview a document, add parameters to the document URL. The parameters are described as follows:



```
<BucketName-APPID>.cos.<Region>.myqcloud.com/<objectkey>?ci-process=doc-preview&pag
```

objectkey: Object key, which can be understood as a file path.

ci-process: CI's processing capability, which is fixed at `doc-preview` for document preview.

page: Number of the page to be converted, which is counted from 1.

srcType: Source data type. Currently, the file conversion feature determines the source data type according to the file extension of the COS object. If the object has no extension, you can set this value.

Note:

If you use the URL mode, only a single-page document or the first page of a multi-page document can be processed.
If you want to preview more content, use [Document Preview API](#).

Media Processing

Enabling Media Processing

Last updated : 2024-01-06 15:14:56

Overview

This document describes how to enable the media processing feature in the COS console. After enabling, you can create workflows or tasks to perform media processing operations. For more information, see [Media Processing Overview](#).

Note:

To use the media processing feature, first enable Cloud Infinite (CI). Media processing fees incurred will be charged by CI. For detailed pricing, see [CI Media Processing Fees](#).

Directions

1. Log in to the [COS console](#).
2. Choose **Bucket List** on the left sidebar.
3. Click the name of the bucket that you want to operate.
4. On the left sidebar, click **Data Processing > Media Processing**.
5. Click **Edit** and set the status to **enabled**.
6. Click **Save**.

Subsequent Operations

After enabling media processing, you can perform the following operations:

For the specified files in a bucket: You can create a media processing task to perform media processing on them. For details, see [Creating a Task](#).

For incremental files in a bucket: You can create a workflow to automatically process and save the files after they are uploaded to the bucket. For details, see [Creating a Workflow](#).

Function Service

Setting CDN Cache Purge

Last updated : 2024-03-25 14:58:45

Overview

CDN cache purge is a data purge feature provided by COS based on the [SCF](#) service. It can automatically purge the data cached on CDN edge nodes. After you add a trigger rule for a bucket, when a file is updated to the bucket, the SCF function preconfigured by COS will be automatically triggered to purge the cached data.

Note:

If you added a cache purge rule for your bucket in the COS console, the resulting purge function will also appear in the [SCF console](#). **Do not** delete this function; otherwise, your rule may not take effect.

Regions where SCF is available support CDN cache purge, including Guangzhou, Shanghai, Beijing, Chengdu, Hong Kong (China), Singapore, Mumbai, Toronto, and Silicon Valley. For more supported regions, see [Serverless Cloud Function](#).

CDN cache purge may fail due to factors such as unstable network connection. In these cases, you can click **View Log** for the function created in the COS console to enter the SCF console and view the error log details for troubleshooting.

The CDN cache purge feature depends on the SCF service, which provides a [free tier](#). Excessive usage will be billed at SCF prices. For more information, see [Pricing](#). For this feature, the more often you purge the cache, the more invocations you will need to use.

Directions

1. Log in to the [COS console](#).
2. Click **Bucket List** on the left sidebar and click the name of the target bucket.
3. Click **Function Service > CDN Cache Purge Function** on the left sidebar.

CDN Cache Refresh Function

[Add Function](#)

Function Name	Event Type	Trigger Scope	Authorize Roles	Specified Domain
---------------	------------	---------------	-----------------	------------------

No data to display

Note:

If you haven't activated SCF, go to the [SCF console](#) to activate it and authorize the service as instructed.

4. Click **Add Function** and configure the following in the pop-up window:

CreateCDN Cache Refresh Function

Function Name

Enter the prefix of function

-cdn-6def149cefd5a26e9fab68e2d492149

Beginning with a letter, support a-z, A-Z, 0-9, -, _, up to 10 characters, and at least 1 character

Event Type ⓘ

Please select

Trigger Condition ⓘ

☒ Specified Range ☐ The whole bucket

Prefix

Enter content

Suffix

Enter content

Specified Domain ⓘ

Please select

SCF Authorization

☐ Authorize SCF Service

To decompress files using SCF, you need to authorize SCF a third party role for accessing COS for you. Click above to authorize.

Confirm

Cancel

Function Name: It uniquely identifies a function and cannot be modified after being set. You can view the function in the [SCF console](#).

Event Type: An event is an operation that triggers SCF. Take upload as an example. You can initiate an upload by calling the [PUT Object](#) or [Post Object](#) API. If you select `PUT` as the event type, only uploads through the `PUT Object` API can trigger the function to purge the cache on CDN edge nodes.

Trigger Condition: You can specify the file source scope of the triggered files, such as all buckets, specified prefix, or specified suffix. After you specify a prefix or suffix, the rule only applies to the matched file sources.

Specified Domain: Specify the CDN domain name to be purged.

SCF Authorization: CDN cache purge requires authorizing SCF to call the CDN API `PurgeUrlsCache`. In this way, SCF can replace your CDN cache with the latest data CDN pulls from the COS origin.

5. Click **Confirm**.

Click **Log** to view the historical operations of CDN cache purge.

Click **Delete** to delete an unwanted CDN cache purge rule.

Content Moderation

Moderation Details

Last updated : 2024-01-06 15:31:10

Overview

The COS content moderation service intelligently moderates the multimedia content of images, videos, audios, documents, and text. It helps you effectively identify non-compliant content such as pornographic, vulgar, illegal, disgusting, and offensive information to avoid operational risks.

After files are moderated successfully, you can view the moderation results by condition and manually process them on the **Moderation Details** page.

Directions

Filtering results

1. Log in to the [COS console](#).
2. Click **Bucket List** on the left sidebar.
3. Click the name of the target bucket to go to the configuration page.
4. On the left sidebar, select **Sensitive Content Moderation** > **Moderation Details** to enter the **Moderation Details** page.

5. Select the conditions as needed.

Scope: You can view the results of moderation through API calls, automatic moderation, and historical data moderation.

File type: You can view the moderation results of images, videos, audios, and text.

Level-1 category of moderation result: It refers to the level-1 label of the moderation result. You can specify it to filter the results.

Level-2 category of moderation result: It refers to the level-2 label of the moderation result, which is more specific than the level-1 category. You can specify it to filter the results.

Moderation Result: Moderated files are categorized into three types: sensitive, suspected, and normal files. You can view a type of file or all files.

Sensitive: Images whose score falls within the range of [91,100].

Suspected: Images that are suspected to be sensitive and whose score falls within the range of [61,90]. For such images, the system cannot determine whether they are sensitive, so we recommend you determine it through human moderation.

Normal: Images whose score falls within the range of [0,60].

Block Status: You can view the moderation results of blocked, normal, or all files.

Moderation Status: You can filter the moderation status, including **under review**, **succeeded**, and **rejected**.

Moderation Policy: You can filter moderation results by moderation policy (`BizType`).

Moderation time: You can view the moderation results in the specified time period.

Note:

If you rename a file or modify its metadata, the file will be considered a newly uploaded file and have a new moderation result.

Image Score: If you select **All** for **Moderation Result**, you can filter files by customizing the file moderation score interval.

Object Name: You can enter a filename to view the moderation result of the specified file.

6. Click **Query** to view the moderation results.

Note:

The **Moderation Details** page only displays the details of moderations called in the console but not those called through an API or SDK.

Exporting results

After [filtering results](#), click **Export** to export the results as a .csv or .xlsx file.

The fields in the moderation result file are as detailed below:

Field	Description
Moderation record ID	Unique ID of the moderation job (also known as job ID), through which you can query the moderation result.
Object name	Name of the moderated file. Note: This field is empty if you use the API to directly moderate text content.
Moderation result type	Moderation result type of the file such as Porn or Ad . If the moderation result is Normal , this field will be empty.
Moderation score	The confidence the moderation result hits the moderation scene. Value range: 0–100. The higher the value, the more likely the content hits the currently returned moderation scene. For example, <code>99</code> means that the content is very likely to be pornographic.
Moderation result subtype	Moderation subtype of the file such as Sexy . If the moderation result is Normal , this field will be empty.
Moderation result	Moderation results include Normal , Sensitive , and Suspected . The result is determined by the moderation score. Normal: The moderation score is 0–60. Sensitive: The moderation score is 91–100.

	Suspected: The moderation score is 61–90.
Blocked	Whether the moderated file is blocked. You can configure automatic blocking upon moderation in Automatic Moderation and Historical Data Moderation .
File size	Unit: B.
Moderation time	Time when the file is moderated.
File path	Location of the file in the bucket. Note: This field is empty if you use the API to directly moderate text content or a file not in COS.
Original link	File URL. Note: This field is empty if you use the API to directly moderate text content.
Moderation method	File moderation method. Valid values: <code>Notify</code> : Automatic moderation. <code>Task</code> : Historical data moderation. <code>API</code> : Moderation through API call.
File type	Data source of the moderated file. Valid values: <code>object</code> : The file is in COS. <code>objecturl</code> : The file is specified by URL, which can be an external URL. <code>API</code> : The file is moderated through API call.
Moderation status	<code>Success</code> : The moderation succeeded. <code>Failed</code> : The moderation failed.
Error code	If the moderation status is <code>Failed</code> , the error cause will be returned through an error code. For more information, see Error Codes .
Error message	Error message of the moderation failure.
bizType	Unique ID of the moderation policy, by which you can find the currently configured moderation policy.

Manually moderating results

After you [filter results](#), the **Moderation Details** page will show filtered results, and you can perform the following operations on the filtered results:

Block an image or set its status to **Normal**.

Click a moderated image to view its details.

Automatic Moderation

Setting Live Stream Moderation

Last updated : 2024-01-06 15:31:10

Overview

This document describes how to use the live stream moderation feature via the Cloud Object Storage (COS) console. Moderation scenarios for live stream moderation include **pornographic**, **illegal**, and **advertising content inspection**. After you enable the live stream moderation feature, newly generated video streams from specific live domains will be automatically moderated. You can view real-time moderation results through the console or callback information.

Prerequisites

Supported live stream duration: **less than 5 hours**.

Supported live stream resolutions: Up to 1920×1080 (1080p).

Supported live stream protocols: Mainstream protocols such as RTMP, HLS, HTTP, and HTTPS.

Operations

1. Log in to the [COS console](#). On the **Bucket List** page, select the required bucket to open the bucket management page.
2. From the left sidebar, select **Sensitive Content Moderation** and then click **Auto Audit Configuration > Live streaming moderation**.
3. Click **Add Live streaming moderation configuration** to open the live stream moderation configuration page, and set the following configuration items:

Select a moderation policy: Choose the moderation policy you have configured. Different moderation policies correspond to different categories. You can customize the policy to personalize moderation based on scenes. Pornographic, illegal and advertising content moderation is supported, and you can select one or more detection scenes. You can go to [Setting Moderation Policy](#) to see how to configure a moderation policy.

Risk library associated: Risk libraries associated with the moderation policy.

Moderation scene: You can filter scenes configured in the moderation policy, such as pornography or advertising. You can select one or multiple scenes.

Play Domain: The playback domain name used in your live stream services. We will pull out the video stream from this domain for moderation.

Authentication key: If you have configured playback authentication in your live stream services, you need to enter the corresponding authentication key for your playback domain.

Callback configuration: If callback is activated, corresponding live stream moderation results will be delivered to you. You need to choose the moderation type and content for callback while configuring the callback URL. For further details, see [Live Stream Moderation Callback Content](#).

Dedicated callback security configuration: To ensure the security of the CI callback information reception, we will generate a default moderation authentication token, which allows us to verify the source of the callback information. You can also customize and modify this token.

4. If you have an ongoing live stream services, you need to specify the corresponding configurations with existing callbacks, to ensure your existing stream initiation and stream termination callbacks are unaffected. If you use the live stream service for the first time, you can skip this step:

Existing Stream Initiation Callback: Specify your existing Live Stream Initiation Callback. We will forward the callback information to you.

Existing Stream Termination Callback: Specify your existing Live Stream Termination Callback. We will forward the callback information to you.

5. Click **Save**. The system will generate a callback address dedicated for live stream moderation. Specify this dedicated callback address for both your live stream initiation and termination callback in your CSS product. We will trigger the moderation automatically according to the stream initiation callback, and cease the moderation in line with the stream termination callback.

[Click to go to the CSS console](#)

6. After the preceding operations are completed, initiate a live stream to automatically commence the moderation process.

Setting Image Moderation

Last updated : 2024-01-06 15:31:10

Overview

This document describes how to use the image moderation feature in the console. After you enable image moderation, new images uploaded to a bucket will be automatically moderated, and the identified non-compliant content can be automatically blocked (by denying public read access to the content).

You can also scan **historical** image files in COS to detect pornographic, illegal, and advertising content. For more information, see [Single Image Moderation](#).

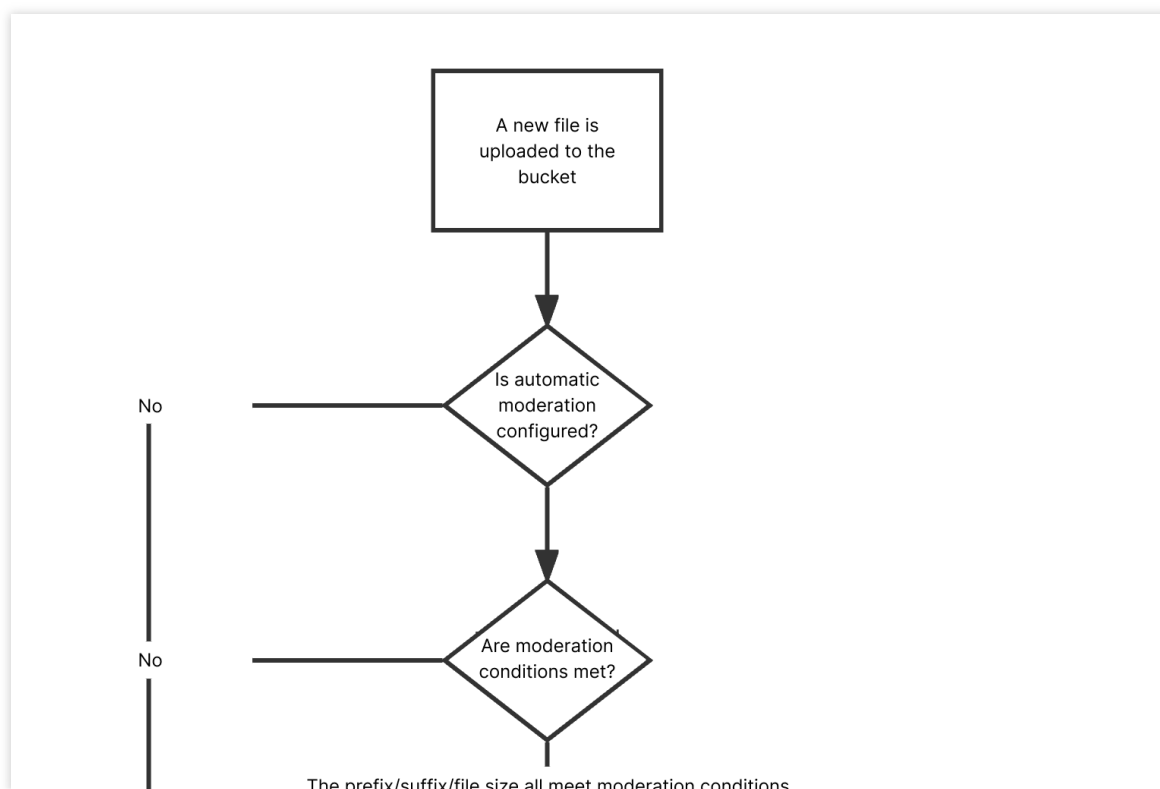
Note:

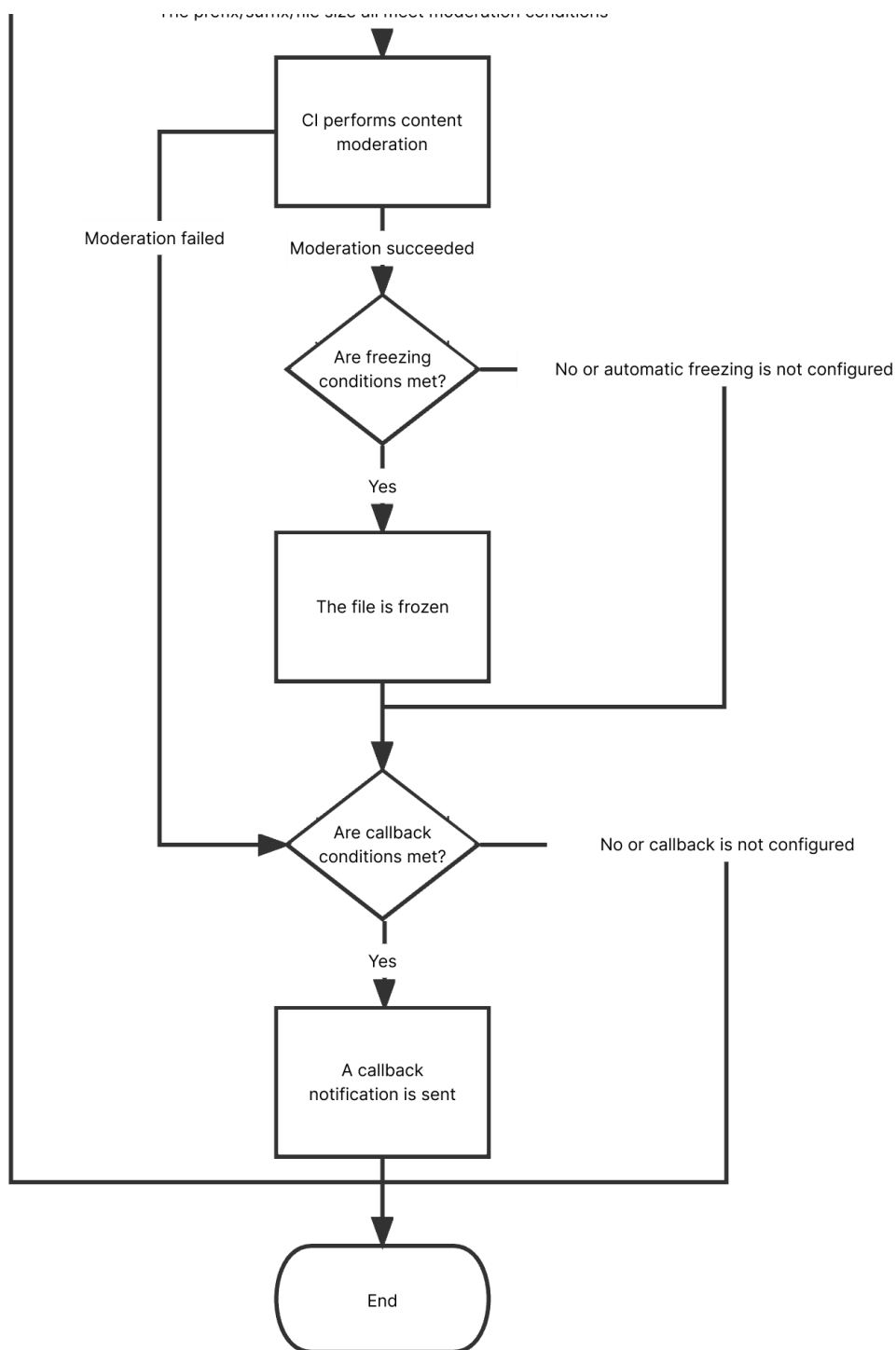
Supported image formats: PNG, JPEG, JPG, BMP, WEBP, GIF.

Supported image file size: < 32 MB. To moderate images larger than 5 MB in size, you need to enable the large image moderation feature.

Supported image dimensions: > 20 * 20 px (width * height).

Flowchart





Directions

1. Log in to the [COS console](#). On the **Bucket List** page, click the target bucket to enter the bucket details page.
2. On the left sidebar, select **Sensitive Content Moderation** > **Automatic Moderation Configuration** and click **Image Moderation**.
3. Click **Add Automatic Image Moderation Configuration** and set the following configuration items:

Moderation Scope: You can select **The whole bucket** or **Specified Range**.

Path: If you select **Specified Range**, enter the path of the images to be moderated.

Example 1: To moderate files in the test directory, set this field to `test/` .

Example 2: To moderate files prefixed with `123` , set this field to `123` .

Note:

You can add multiple moderation configurations, but the paths cannot be duplicate or have inclusion relationships. If you have configured to moderate the entire bucket, you cannot add a moderation configuration for a specific path in the bucket.

Moderation Suffix: The following image formats can be moderated: JPG, JPEG, PNG, BMP, WEBP, and GIF. Two options are supported: **Smart** and **Without suffix**.

Note:

Smart: After you select this option, the system will intelligently determine whether a file is an image based on its file extension and content.

Large Image Moderation: The image moderation feature can moderate images below 5 MB in size. For larger images, you can enable the large image moderation feature. Then, the backend will compress images (up to 32 MB) first before moderating them.

Moderation Policy: Select a moderation policy. You can create different policies for refined moderation. Moderation scene options include **Pornographic**, **Illegal**, and **Advertisement**, and you can select one or multiple options. For detailed directions on how to configure a moderation policy, see [Setting Moderation Policy](#).

Moderation Scene: It displays the default scene or the scene that you configure in the moderation policy. You can select the target scene as needed.

File block configuration: You can enable this service to authorize CI to perform automatic or human moderation and block the identified non-compliant files by denying public read access to them.

Block mode: The following two block modes are supported:

Change the file ACL to private read: Doing so actually blocks the file. Then, a 403 status code will be returned when the file is accessed again, indicating that access is denied. For more information on file permissions, see [ACL](#).

Transfer the file to the backup directory: Doing so actually blocks the file. Then, a 404 status code will be returned when the file is accessed again, indicating that the file does not exist. The backup directory is automatically generated by the backend at `audit_freeze_backup/increment_audit` in the current bucket.

Block Type: You can select a block type and mechanism. **Machine moderation and block** is selected by default. If you select **Human moderation and block**, Tencent Cloud security team will review suspiciously sensitive images identified during machine moderation. You can select the image score range for blocking (by specifying an integer between 60 and 100; the greater the score, the more sensitive the image).

Callback: After callback is enabled, you will receive image moderation results. You need to select the moderation type, callback content, callback URL, and image domain name. If you select **Custom Callback Threshold**, you need to set the score range of the images for callback. After the callback URL is set, CI will send the default callback message to the set URL to check whether it can receive callback messages normally. For more information on callback, see [Image Moderation Callback Content](#).

4. After completing the configuration, click **Save**. Images uploaded subsequently will be moderated.

Notes

1. Image moderation adopts a scoring mechanism, with a score between 0 and 100 returned for each image.
2. The **confirmed part** refers to the images that are confirmed to be normal or sensitive (with a score in the range of [0,60] or (90,100]). For such images, no manual intervention is required.
3. The **uncertain part** refers to the images that are suspected to be sensitive (with a score in the range of (60,90]). For such images, human moderation is recommended.

Setting Video Moderation

Last updated : 2024-01-06 15:31:10

Overview

This document describes how to use the video moderation feature in the COS console. Detection scenarios include **pornographic**, **illegal**, and **advertising** information detection. After you enable video moderation, **new** videos uploaded to a bucket will be automatically moderated, and the identified non-compliant content can be automatically blocked (by denying public read access to the content).

You can also moderate **historical** videos stored in COS. For more information, see [Submitting Video Moderation Job](#).

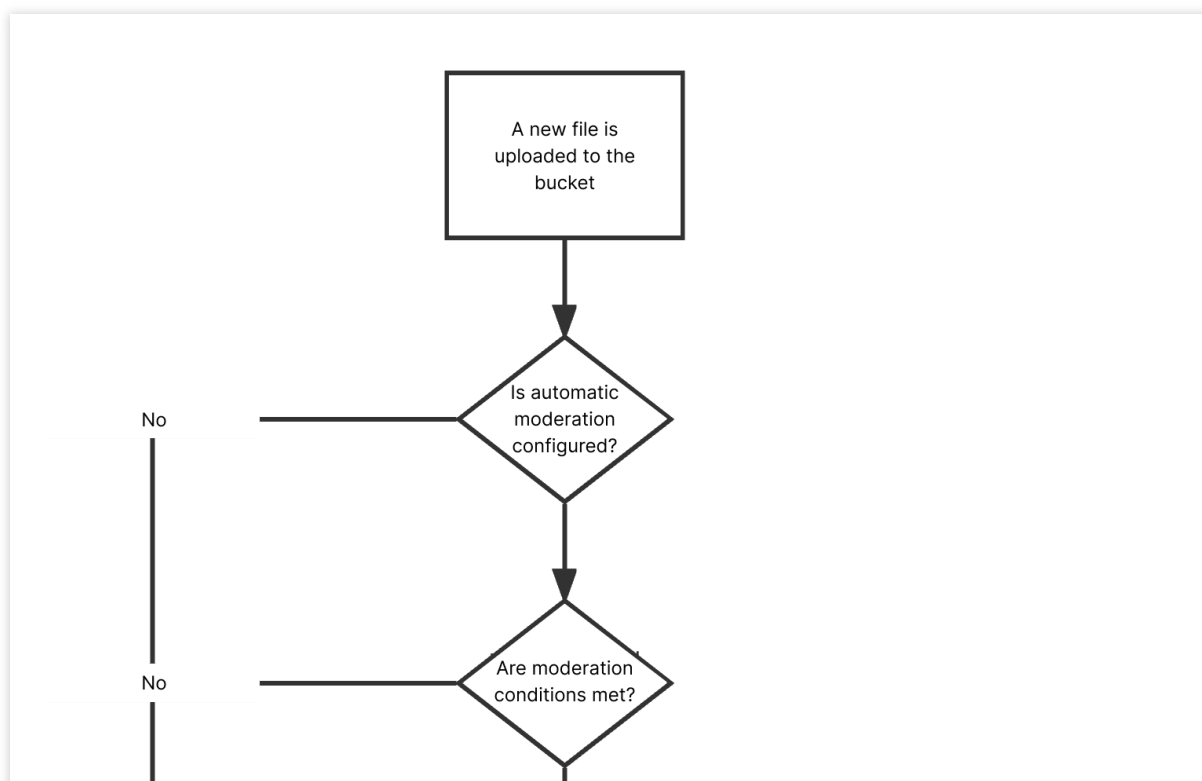
Note:

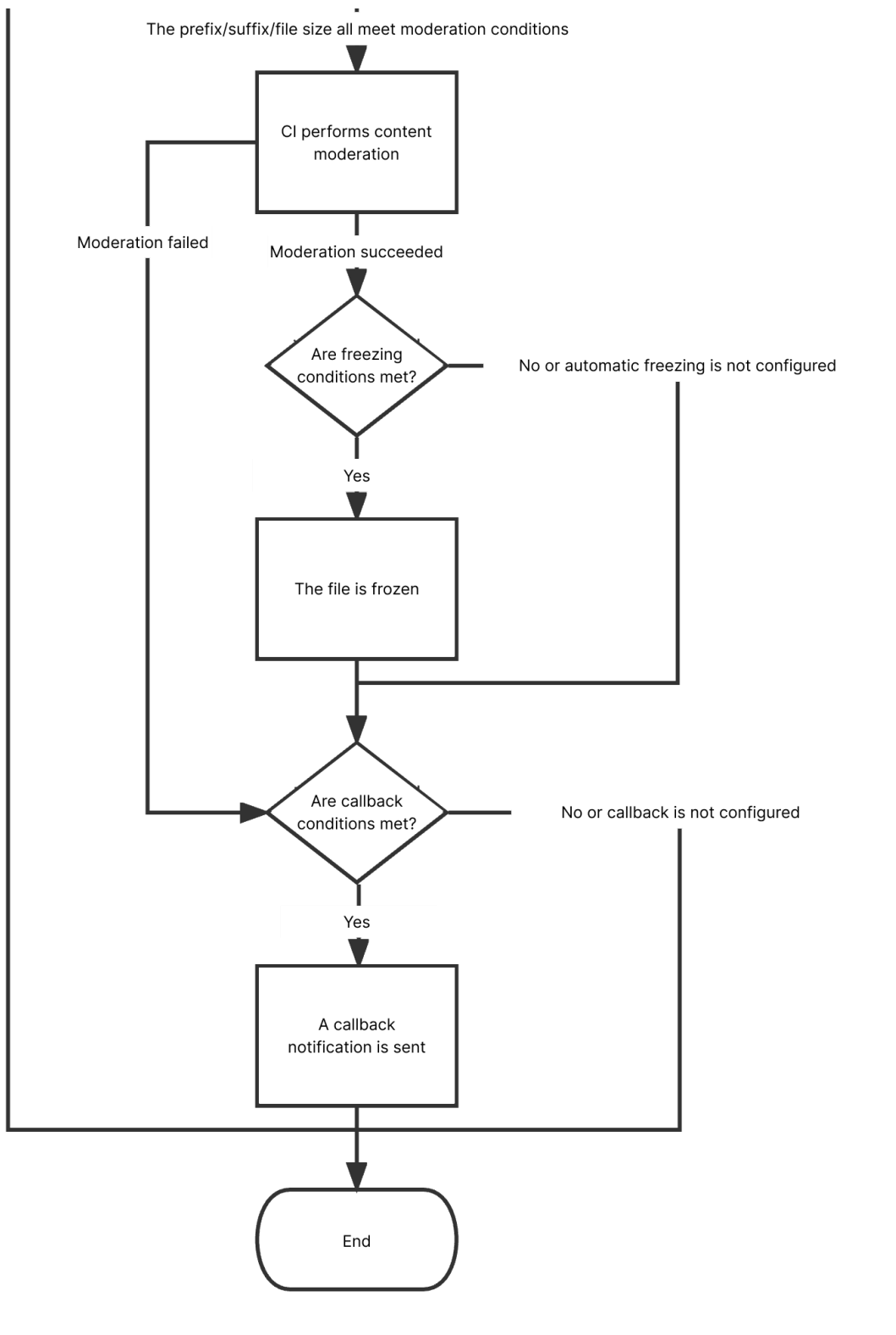
Video moderation is conducted by **capturing video frames** and checking screenshots. You can select the frame capturing method when you enable video moderation. For more information, see the directions below.

The following video formats can be moderated: MP4, AVI, MKV, WMV, RMVB, FLV, M3U8, MOV, M4V, and 3GP.

The video size cannot exceed 5 GB, and the number of captured frames cannot exceed 10,000.

Flowchart





Directions

1. Log in to the [COS console](#). On the **Bucket List** page, click the target bucket to enter the bucket details page.

2. On the left sidebar, select **Sensitive Content Moderation > Automatic Moderation Configuration** and click **Video Moderation**.

3. Click **Add Automatic Video Moderation Configuration** and set the following configuration items:

Moderation Scope: You can select **The whole bucket** or **Specified Range**.

Path: If you select **Specified Range**, enter the path of the videos to be moderated.

Example 1: To moderate files in the test directory, set this field to `test/`.

Example 2: To moderate files prefixed with `123`, set this field to `123`.

Note:

You can add multiple moderation configurations, but the paths cannot be duplicate or have inclusion relationships. If you have configured to moderate the entire bucket, you cannot add a moderation configuration for a specific path in the bucket.

Moderation Suffix: Supported video formats are MP4 (including other formats under the same MP4 format source: MPG, MPEG, MPE, DAT, VOB, 3GP), WMV (including other formats under the same WMV format source: ASF), RMVB (including other formats under the same RMVB format source: RM), and FLV (including other formats under the same FLV format source: F4V). If you select the **Without suffix** option, the system will check the Content-Type header of files without extensions to determine whether they are videos. Multiple options can be selected.

Moderation Policy: Select a moderation policy. You can create different policies for refined moderation. Moderation scene options include **Pornographic**, **Illegal**, and **Advertisement**, and you can select one or multiple options. For detailed directions on how to configure a moderation policy, see [Setting Moderation Policy](#).

Moderate: Video image and video sound can be moderated. To moderate video sound, you need to select it in the moderation policy.

Note:

The **Moderate** option should be used together with the moderation policy. If video sound is not set in the policy, you cannot select **Video sound** here.

Moderation Scene: Moderation scene options include moderation for pornographic, illegal, and advertising content, and you can select one or multiple options.

Frame Capturing Rule: Video moderation is conducted by **capturing video frames** and checking screenshots.

You can select **Fixed Time**, **Fixed Frame Rate**, or **Fixed Quantity** for video frame capturing.

Fixed Time: This option indicates to capture images at fixed intervals to moderate. You can set the time interval and the maximum number of frames per video.

Fixed Frame Rate: This option indicates to capture a fixed number of frames per second to moderate. You can set the number of frames captured per second and the maximum number of frames per video.

Fixed Quantity: This option indicates to moderate a fixed number of captured images for the entire video according to the average percentage.

File block configuration: You can enable this service to authorize CI to perform automatic or human moderation and block the identified non-compliant files by denying public read access to them. After enabling this service, you need to select the block type.

Block mode: The following two block modes are supported:

Change the file ACL to private read: Doing so actually blocks the file. Then, a 403 status code will be returned when the file is accessed again, indicating that access is denied. For more information on file permissions, see [ACL](#).

Transfer the file to the backup directory: Doing so actually blocks the file. Then, a 404 status code will be returned when the file is accessed again, indicating that the file does not exist. The backup directory is automatically generated by the backend at `audit_freeze_backup/increment_audit` in the current bucket.

Block Type: You can select a block type and mechanism. **Machine moderation and block** is selected by default. If you select **Human moderation and block**, Tencent Cloud security team will review suspiciously sensitive videos identified during machine moderation.

Callback: After callback is enabled, you will receive video moderation results. You need to select the moderation type and callback content and set the callback URL. For more information, see [Video Moderation Callback Content](#).

4. After completing the configuration, click **Save**. Videos uploaded subsequently will be moderated.

Notes

1. Video moderation adopts a scoring mechanism, with a score between 0 and 100 returned for each captured video frame.
2. The **confirmed part** refers to the videos that are confirmed to be normal or sensitive (with a score in the range of [0,60] or (90,100]). For such images, no manual intervention is required.
3. The **uncertain part** refers to the videos that are suspected to be sensitive (with a score in the range of (60,90]). For such images, human moderation is recommended.

Setting Audio Moderation

Last updated : 2024-01-06 15:31:10

Overview

This document describes how to use the audio moderation feature in the console to check audio content for **pornographic**, **illegal**, and **advertising** information.

After you configure automatic audio moderation, **new** audios uploaded to a bucket will be automatically moderated, and the identified non-compliant content can be automatically blocked (by denying public read access to the content). You can also moderate existing audios stored in COS. For more information, see [Audio Moderation](#).

Note:

Audio moderation is billed by CI.

Supported audio formats: MP3, WAV, AAC, FLAC, AMR, 3GP, M4A, WMA, OGG, APE.

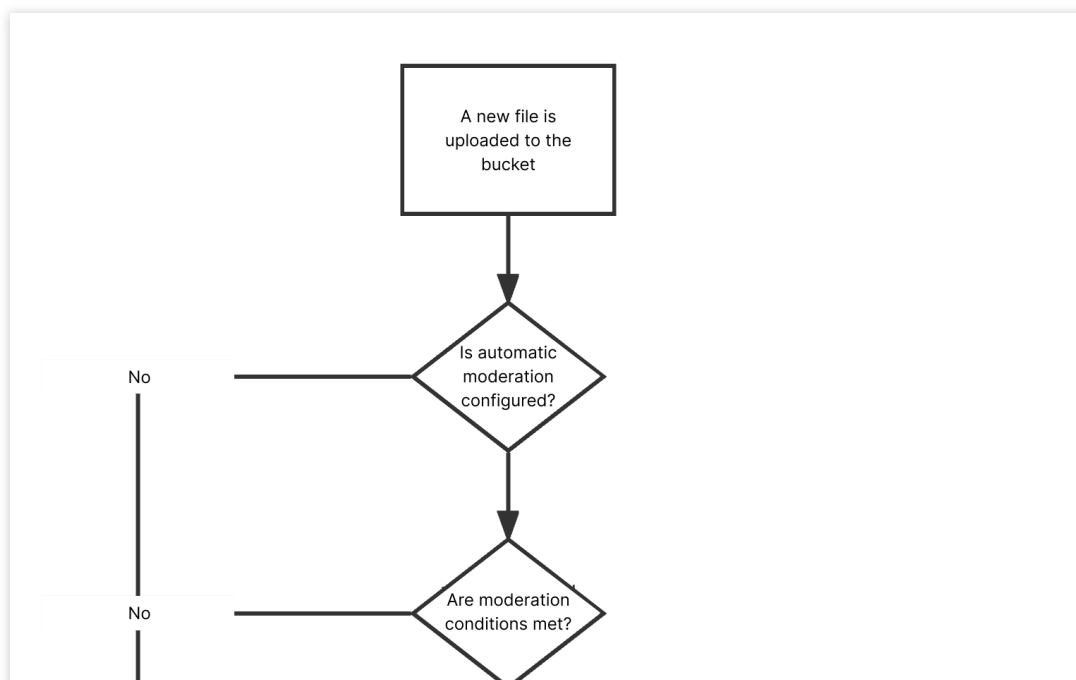
Supported audio bitrate: 128–256 Kbps.

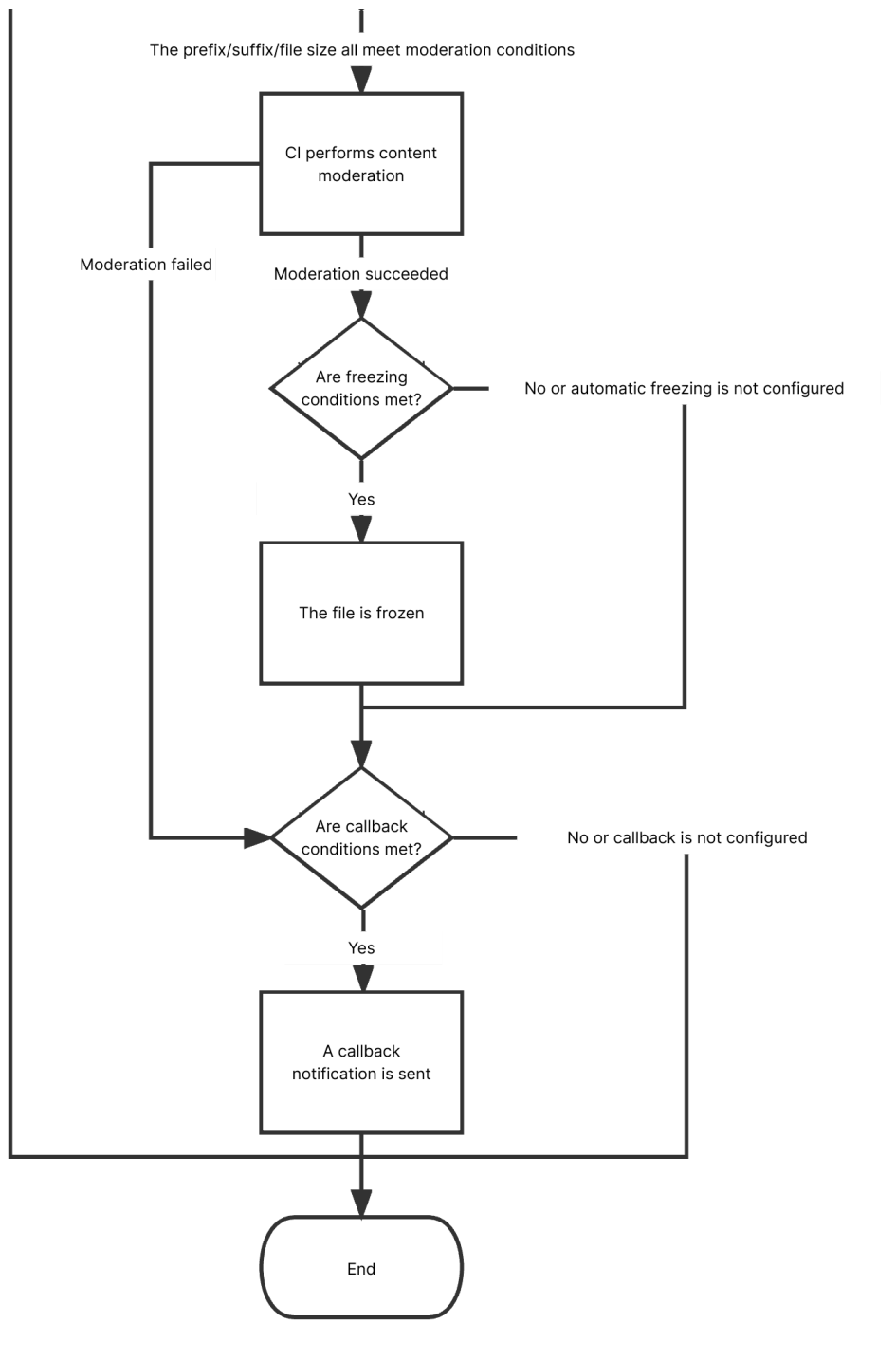
Supported audio size: < 600 MB.

Maximum duration: 3 hours.

Audio moderation can recognize Mandarin and English.

Flowchart





Directions

1. Log in to the [COS console](#). On the **Bucket List** page, click the target bucket to enter the bucket details page.
2. On the left sidebar, select **Sensitive Content Moderation** > **Automatic Moderation Configuration** and click **Audio Moderation**.
3. Click **Add Automatic Audio Moderation Configuration** and set the following configuration items:

Moderation Scope: Select the scope of audio files to be moderated, which can be the entire bucket, a specific directory, or a specific file prefix.

Moderation Suffix: The following audio formats can be moderated: MP3, WAV, AAC, FLAC, AMR, 3GP, M4A, WMA, OGG, and APE. You can select multiple formats.

Moderation Policy: Select a moderation policy. You can create different policies for refined moderation. If no policies have been configured, the default policy will be used. Moderation scene options include **Pornographic**, **Illegal**, and **Advertisement**, and you can select one or multiple options. For detailed directions on how to configure a moderation policy, see [Setting Moderation Policy](#).

Moderation Scene: It displays the scene that you configure in the moderation policy. You can select the target scene as needed.

File block configuration: You can enable this service to authorize CI to perform automatic or human moderation and block the identified non-compliant files by denying public read access to them. After enabling this service, you need to select the block type and score range of audios to be blocked.

Block mode: The following two block modes are supported:

Change the file ACL to private read: Doing so actually blocks the file. Then, a 403 status code will be returned when the file is accessed again, indicating that access is denied. For more information on file permissions, see [ACL](#).

Transfer the file to the backup directory: Doing so actually blocks the file. Then, a 404 status code will be returned when the file is accessed again, indicating that the file does not exist. The backup directory is automatically generated by the backend at `audit_freeze_backup/increment_audit` in the current bucket.

Block Type: You can select a block type and mechanism. **Machine moderation and block** is selected by default. If you select **Human moderation and block**, Tencent Cloud security team will review suspiciously sensitive audios identified during machine moderation. You can select the audio score range for blocking (by specifying an integer between 60 and 100; the greater the score, the more sensitive the audio).

Callback: After callback is enabled, you will receive moderation results. You need to select the moderation type and callback content and set the callback URL. For more information, see [Callback Content](#).

4. After completing the configuration, click **Save**. Audios uploaded subsequently will be moderated.

Callback Content

If you enable callback, after audio moderation is completed, the system will send the following callback message to the callback URL:



```
{
  "code":0,
  "message":"success",
  "data":{
    "url":"",
    "result":1,
    "forbidden_status":1,
    "trace_id":"",
    "porn_info":{
      "hit_flag":1,
      "score":91,
```

```

        "label": ""
    },
    "ads_info": {
        "hit_flag": 0,
        "score": 0,
        "label": ""
    }
}

```

Parameter	Description	Type	Required
forbidden_status	Block status. Valid values: <code>0</code> (normal); <code>1</code> (blocked).	Int	Yes
porn_info	Porn detection information, including moderation result, score, and detailed tags.	json	Yes
ads_info	Ad detection information, including moderation result, score, and detailed tags.	json	Yes
result	Recognition result for reference. Valid values: <code>0</code> (normal), <code>1</code> (sensitive), <code>2</code> (suspiciously sensitive).	Int	Yes
trace_id	<code>jobid</code> of the submitted moderation job.	String	Yes
url	The URL of the uploaded resource, including the domain name.	String	Yes

The moderation information (`porn_info` and `ads_info`) has the following sub-nodes:

Parameter	Description	Type	Required
hit_flag	Whether the moderation type is hit. Valid values: <code>0</code> (miss), <code>1</code> (hit), and <code>2</code> (suspected).	Int	Yes
label	Recognized audio tag.	String	Yes
score	Moderation score. Valid value ranges: 0–60 (normal); 60–90 (suspiciously sensitive); 90–100 (sensitive).	Int	Yes

Notes

1. Audio moderation adopts a scoring mechanism, with a score between 0 and 100 returned for each audio.
2. The **confirmed part** refers to the audios that are confirmed to be normal or sensitive (with a score in the range of [0,60] or (90,100]). For such audios, no manual intervention is required.

3. The **uncertain part** refers to the audios that are suspected to be sensitive (with a score in the range of (60,90]). For such audios, human moderation is recommended.

Setting Text Moderation

Last updated : 2024-01-06 15:31:10

Overview

This document describes how to use the text moderation feature in the COS console. The feature can check text content for **pornographic**, **illegal**, **advertising**, and **abusive** information.

After you enable text moderation, **new** text files uploaded to a bucket will be automatically moderated, and the identified non-compliant content can be automatically blocked (by denying public read access to the content).

Note:

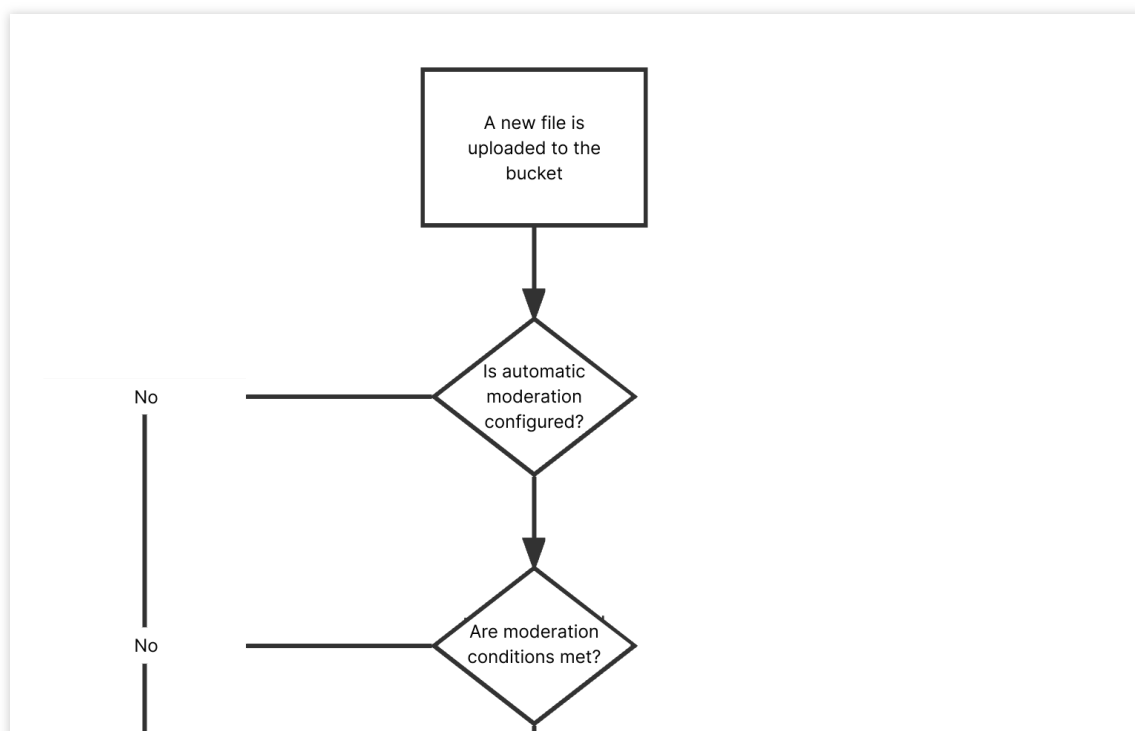
Text moderation is billed by CI.

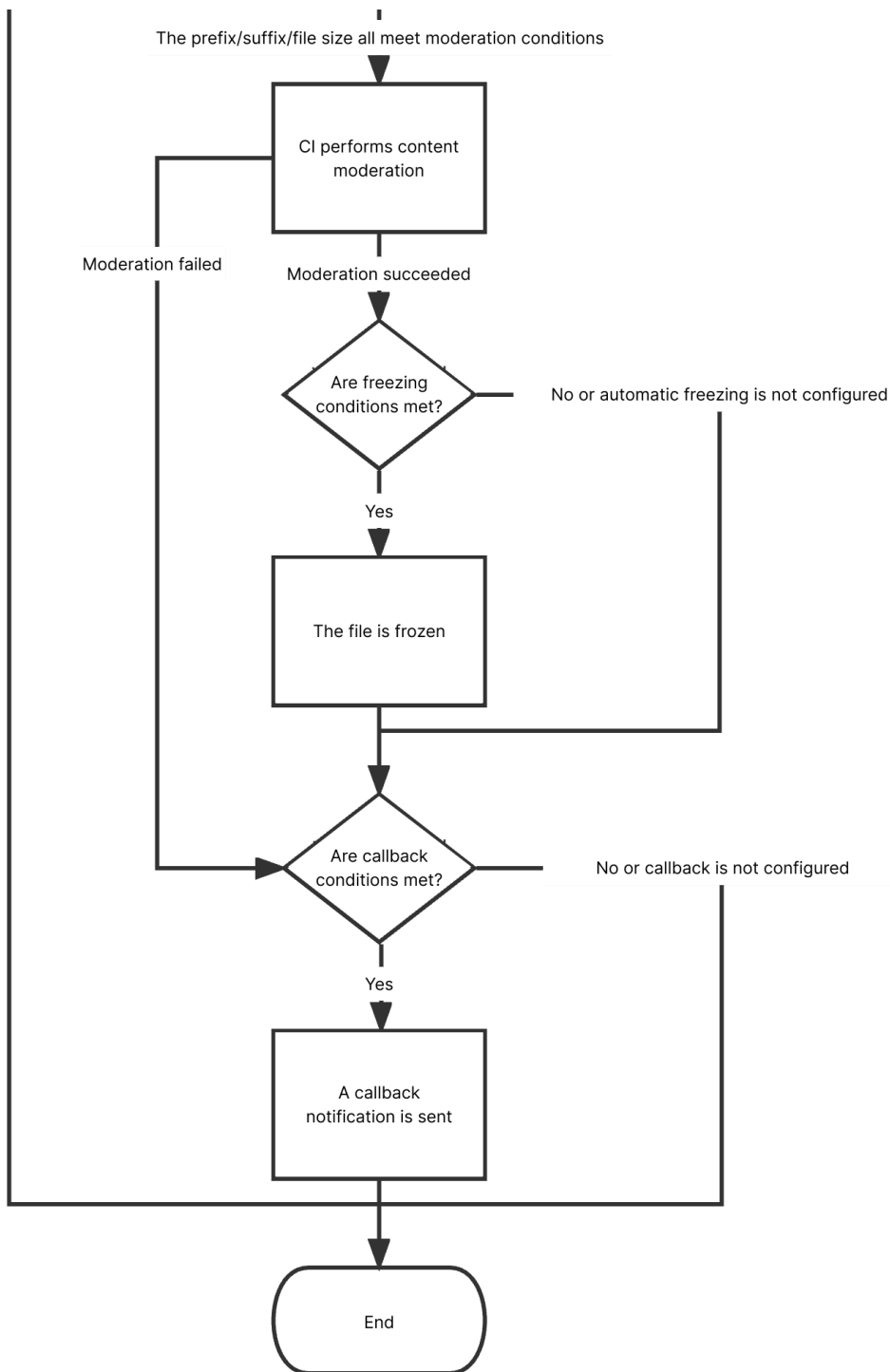
Text moderation is billed by moderation times. Every 10,000 UTF-8 characters is counted as one moderation operation, and less than 10,000 characters are counted as 10,000 characters.

Currently, the text moderation feature supports TXT files and files without extensions, and the file size cannot exceed 1 MB.

Text moderation can recognize Mandarin and English.

Flowchart





Directions

1. Log in to the [COS console](#).
2. Click **Bucket List** on the left sidebar.
3. Click the name of the target bucket to go to the configuration page.

4. On the left sidebar, select **Sensitive Content Moderation** > **Automatic Moderation Configuration** and click **Text Moderation**.

5. Click **Add Automatic Text Moderation Configuration** and set the following configuration items:

Moderation Scope: You can select **The whole bucket** or **Specified Range**.

Path: If you select **Specified Range**, enter the path of the text files to be moderated.

Example 1: To moderate files in the test directory, set this field to `test/`.

Example 2: To moderate files prefixed with `123`, set this field to `123`.

Note:

You can add multiple moderation configurations, but the paths cannot be duplicate or have inclusion relationships. If you have configured to moderate the entire bucket, you cannot add a moderation configuration for a specific path in the bucket.

Moderation Suffix: Options include **TXT**, **HTML**, and **Without suffix**.

Moderation Policy: Select a moderation policy. You can create different policies for refined moderation. Moderation scene options include **Pornographic**, **Illegal**, and **Advertisement**, and you can select one or multiple options. For detailed directions on how to configure a moderation policy, see [Setting Moderation Policy](#).

Moderation Scene: Moderation scene options include moderation for pornographic, advertising, and abusive content, and you can select one or multiple options.

File block configuration: You can enable this service to authorize CI to perform automatic or human moderation and block the identified non-compliant files by denying public read access to them.

Block mode: The following two block modes are supported:

Change the file ACL to private read: Doing so actually blocks the file. Then, a 403 status code will be returned when the file is accessed again, indicating that access is denied. For more information on file permissions, see [ACL](#).

Transfer the file to the backup directory: Doing so actually blocks the file. Then, a 404 status code will be returned when the file is accessed again, indicating that the file does not exist. The backup directory is automatically generated by the backend at `audit_freeze_backup/increment_audit` in the current bucket.

Block Type: You can select a block type and mechanism. **Machine moderation and block** is selected by default. If you select **Human moderation and block**, Tencent Cloud security team will review suspiciously sensitive text files identified during machine moderation.

Callback: After callback is enabled, you will receive moderation results. You need to select the moderation type and callback content and set the callback URL. For more information, see [Callback Content](#).

6. After completing the configuration, click **Save**. Text files uploaded subsequently will be moderated.

Callback Content

After callback is enabled, the system will send the following default callback message to the set URL to check whether it can receive callback messages normally:



```
{
  "code": 0,
  "data": {
    "forbidden_status": 0,
    "porn_info": {
      "hit_flag": 0,
      "label": "",
      "count": 9
    },
    "result": 0,
    "trace_id": "test_trace_id",
  }
}
```

```

    "url": "test_text"
  },
  "message": "Test request when setting callback url"
}

```

Note:

If the callback option is selected, text files frozen by Tencent Cloud will be returned to you, with public read access to them denied.

The callback URL must begin with "http" or "https" and return a 200 status code by default before it can be used.

Check it before saving the settings.

The callback URL will take effect in 30 minutes.

After the callback URL takes effect, when an uploaded text file hits moderation rules, the system will call back the URL by default and send a standard HTTP POST notification message to it. The HTTP packet is as follows:

Parameter	Description	Type	Required
forbidden_status	Block status. Valid values: <code>0</code> (normal); <code>1</code> (blocked).	Int	Yes
porn_info	Porn detection information, including moderation result, score, and detailed tags.	json	Yes
ads_info	Ad detection information, including moderation result, score, and detailed tags.	json	Yes
result	Recognition result for reference. Valid values: <code>0</code> (normal), <code>1</code> (sensitive), <code>2</code> (suspiciously sensitive).	Int	Yes
trace_id	<code>jobid</code> of the submitted moderation job.	String	Yes
url	The URL of the uploaded resource, including the domain name.	String	Yes
illegal_info	Illegal information detection information, including moderation result, score, and detailed tags.	json	No
abuse_info	Abuse detection information, including moderation result, score, and detailed tags.	json	No

The moderation information (`porn_info` , `ads_info` , `illegal_info` , and `abuse_info`) has the following sub-nodes:

Parameter	Description	Type	Required
hit_flag	Whether the moderation type is hit.	Int	Yes
label	Recognized text tag.	String	Yes

count	Text file callback parameter, which is the number of sensitive text segments that hit the moderation scene.	Int	Yes
-------	---	-----	-----

Below is a sample callback:



```
{
  "code":0,
  "message":"success",
  "data":{
    "url":"xxxxxxxxxxxxxxxx",
    "result":1,
```

```
    "forbidden_status":1,  
    "trace_id":"xxxxxxxxxxxxxxxx",  
    "porn_info":{  
        "hit_flag":1,  
        "label":"Obscene",  
        "count":3  
    },  
},  
}
```

Setting Document Moderation

Last updated : 2024-01-06 15:31:10

Overview

This document describes how to use the document moderation feature in the console to check file content for **pornographic**, **illegal**, and **advertising** information.

After you configure automatic document moderation, **new** documents uploaded to a bucket will be automatically moderated, and the identified non-compliant content can be automatically blocked (by denying public read access to the content).

You can also moderate existing documents stored in COS. For more information, see [Document Moderation](#).

Note:

The document moderation feature leverages the **document conversion** capability to convert each page of a document into an image for moderation.

Document moderation is billed by CI.

Currently, document types supported for moderation include:

Presentation files: PPTX, PPT, POT, POTX, PPS, PPSX, DPS, DPT, PPTM, POTM, PPSM.

Text files: DOC, DOT, WPS, WPT, DOCX, DOTX, DOCM, DOTM.

Spreadsheet files: XLS, XLT, ET, ETT, XLSX, XLTX, CSV, XLSB, XLSM, XLTM, ETS.

PDF.

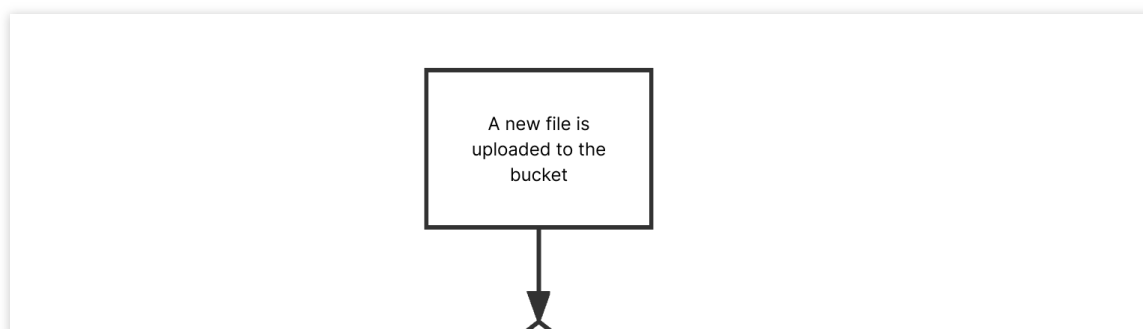
Other files: TXT, LOG, HTM, HTML, LRC, C, CPP, H, ASM, S, JAVA, ASP, BAT, BAS, PRG, CMD, RTF, XML.

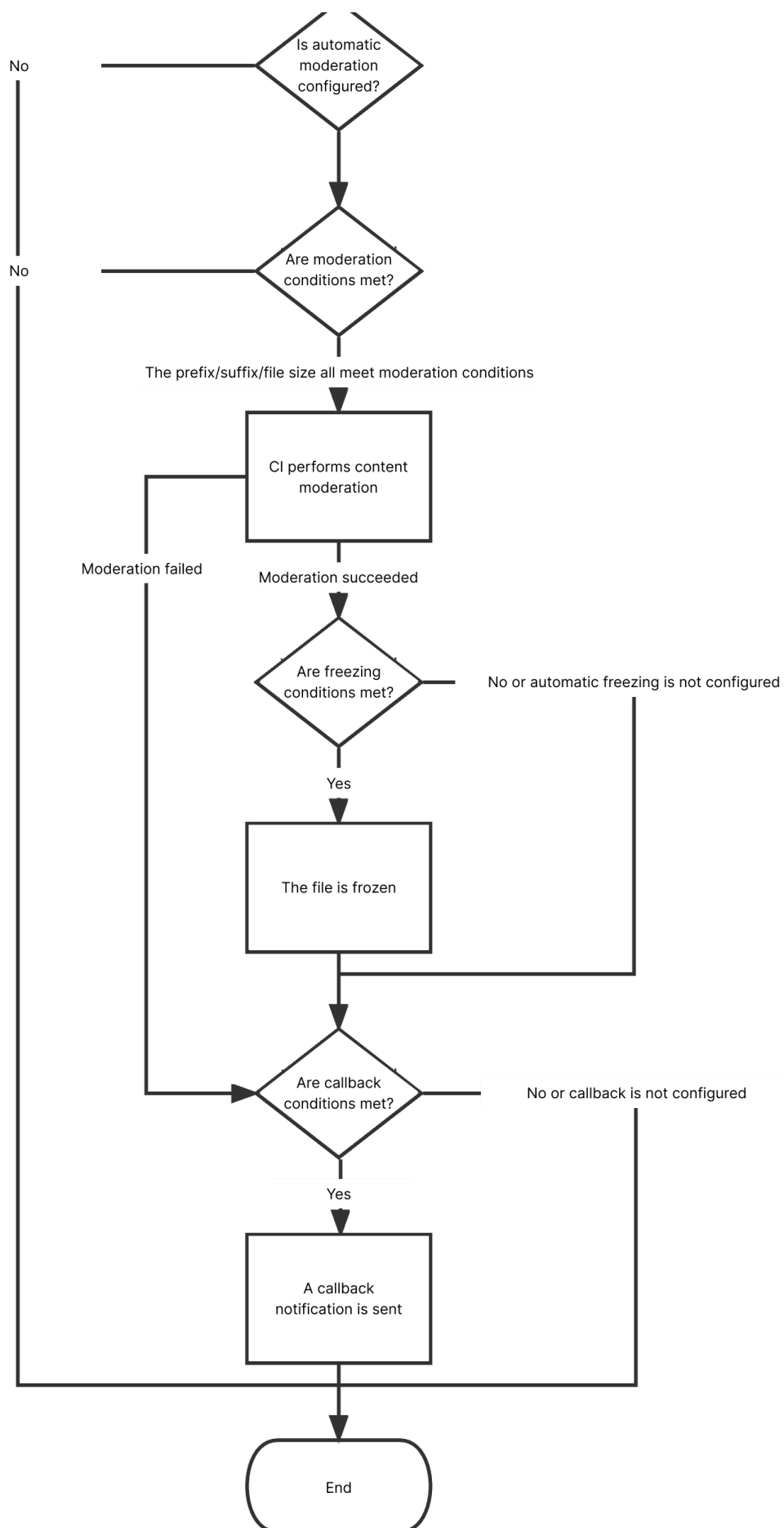
A spreadsheet file may be split into multiple pages, with multiple images generated.

The input file size cannot exceed 200 MB.

The number of pages in the input file cannot exceed 5,000.

Flowchart





Directions

1. Log in to the [COS console](#).
2. On the **Bucket List** page, click the target bucket to enter the bucket details page.
3. On the left sidebar, select **Sensitive Content Moderation > Automatic Moderation Configuration** and click **Document Moderation**.

4. Click **Add Automatic Document Moderation Configuration** and set the following configuration items:

Moderation Scope: Select the scope of documents to be moderated, which can be the entire bucket, a specific directory, or a specific file prefix.

Moderation Suffix: Select one or multiple options for **Document Format**, including presentation, text, spreadsheet, and PDF.

Moderation Policy: Select a moderation policy. You can create different policies for refined moderation. If no policies have been configured, the default policy will be used. Moderation scene options include **Pornographic**, **Illegal**, and **Advertisement**, and you can select one or multiple options. For more information on how to configure a moderation policy, see [Setting Moderation Policy](#).

Moderation Scene: It displays the scene that you configure in the moderation policy. You can select the target scene as needed.

File block configuration: You can enable this service to authorize CI to perform automatic or human moderation and block the identified non-compliant files by denying public read access to them. After enabling this service, you need to select the block type and score range of files to be blocked.

Block mode: The following two block modes are supported:

Change the file ACL to private read: Doing so actually blocks the file. Then, a 403 status code will be returned when the file is accessed again, indicating that access is denied. For more information on file permissions, see [ACL](#).

Transfer the file to the backup directory: Doing so actually blocks the file. Then, a 404 status code will be returned when the file is accessed again, indicating that the file does not exist. The backup directory is automatically generated by the backend at `audit_freeze_backup/increment_audit` in the current bucket.

Block Type: You can select a block type and mechanism. **Machine moderation and block** is selected by default. If you select **Human moderation and block**, Tencent Cloud security team will review suspiciously sensitive files identified during machine moderation. You can select the file score range for blocking (by specifying an integer between 60 and 100; the greater the score, the more sensitive the file).

Callback: After callback is enabled, you will receive moderation results. You need to select the moderation type and callback content and set the callback URL. For more information, see [Document Moderation Callback Content](#).

5. After completing the configuration, click **Save**. Documents uploaded subsequently will be moderated.

Notes

1. Document moderation adopts a scoring mechanism, with a score between 0 and 100 returned for each output image.
2. Depending on the score range, the moderation result can be a sensitive image, suspiciously sensitive image, or normal image.

The score range of sensitive images is ≥ 91 .

The score range of suspiciously sensitive images is 61–90. Such images cannot be accurately identified as sensitive, so human moderation is recommended to ensure their content security.

The score range of normal images is ≤ 60 . Such images are determined as normal by the system.

Historical data moderation

Configuring Historical Data Moderation Tasks

Last updated : 2024-03-25 15:00:04

Overview

This document describes how to use the historical data moderation feature of Cloud Object Storage (COS) via the console. You can create a historical data moderation task to conduct a batch moderation on your images, videos, audios, texts, and files all at once.

Directions

Creating a Moderation Task

1. Log in to the [COS console](#).
2. Select **Bucket List** in the left navigation bar to open the bucket management page.
3. Navigate to the target bucket and click on its name to open the bucket configuration page.
4. In the left navigation bar, choose **Sensitive Content Moderation > Existing File Moderation** to open the historical data moderation page.
5. Click **Create Moderation Task**.
6. In the Scan Range page, you can moderate your files as needed through a specified scan scope:

1 **Scan Range** > 2 Moderation Policy > 3 Block Policy > 4 moderation result > 5 Finish

Scan Scope ☒ Bucket File List ☐ COS inventory report ⓘ ☐ URL list file ⓘ

Time ☒ Not specified ⓘ ☐ Specified

Moderation Scope ☐ The whole bucket ☒ prefix matches with ☐ Wildcard matching

Moderate the content with specified prefixes ⓘ [Select](#) +

Moderate the content without specified prefixes ⓘ ☐

[Next](#)

The scan scope include Bucket File List, COS Inventory Report, and URL List File:

Bucket File List: You can select files within the current bucket for moderation. The scan range can either be the file upload time or prefix.

COS inventory report: You can choose the inventory list generated by the [COS Setting Inventory](#) feature to scan, and put the inventory list file in the current bucket.

URL list file: You can choose a designated URL list file to scan. Currently, TXT files with one URL listed per line are supported.

7. Click **Next**.

8. On the Moderation Policy page, activate the review policy as needed, configure the corresponding file type for moderation and the review scenario type, and click **Next**.

✓ Scan Range > 2 **Moderation Policy** > 3 Block Policy > 4 moderation result > 5 Finish

Review Image ☐

Review Video ☐

Review Audio ☐

Review Text ☐

Review More ☐

[Previous](#) [Next](#)

Review Image:

Moderation Suffix: Image moderation supports the following formats: JPG, JPEG, PNG, BMP, WEBP, and GIF.

Note:

Intelligent suffix recognition can recognize some special suffixes in addition to the preceding six common suffixes.

Large Image Moderation: Image moderation only supports images up to 5 MB. For images exceeding the size limit, you can enable the large image moderation feature. Then the system compresses the images before the moderation process. This feature can compress images up to 32 MB.

Note:

The large image moderation feature incurs basic image processing fees. For detailed prices, see [Basic Image Processing Costs](#).

Moderation Policy Selection: Please select the moderation policy you have configured (if no policy is configured, the system's default policy can be used). Each moderation policy corresponds to a category, and you can customize moderation scenes through policy customization. Options for moderation include pornographic content, illegal activity or non-compliant behavior, and advertising content, and you can select one or multiple scenes for moderation. For more information on how to configure a moderation policy, see [Setting Moderation Policy](#).

Daily Moderation Limit: You can configure the maximum number of images that can be moderated per day. By default, there is no upper limit.

Moderation Scene: Either the default scenes or those you have configured in your moderation policy are displayed here. You can select the scene categories you wish to moderate.

Review Video:

Moderation Suffix: Video moderation supports the following formats: MP4, AVI, MKV, WMV, RMVB, FLV, M3U8, and so on.

Moderation Policy Selection: Please select the moderation policy you have configured. Each moderation policy corresponds to a category, and you can customize moderation scenes through policy customization. Options for moderation include pornographic content, illegal activity or non-compliant behavior, and advertising content, and you can select one or multiple scenes for moderation. For more information on how to configure a moderation policy, see [Setting Moderation Policy](#).

Daily Moderation Limit: You can configure the maximum number of video files that can be moderated per day. By default, there is no upper limit.

Moderation Scene: Moderation scene options include moderation for pornographic content, illegal, and advertising content. You can select one or multiple moderation scenes.

Moderation Content: Both video images and audio can be moderated.

Frame Capturing Rule: Frame capturing is the basis for video moderation, which is implemented through the moderation of the image captured from the video. Fixed Time, Fixed Frame Rate, and Fixed Quantity are supported for frame capturing moderation.

Fixed Time: Images are captured at fixed intervals for moderation. You can set the time interval and the maximum number of frames captured per video.

Fixed Frame Rate: A fixed number of frames are captured per second for moderation. You can set the frame capture rate per second and the maximum number of frames captured per video.

Fixed Quantity: A predetermined quantity of images are captured from full-length videos, based on an average percentage. You can set the maximum number of frame captured per video.

Note:

The configuration of frame capturing rules will impact the outcome of the moderation.

Review Audio:

Moderation Suffix: Audio moderation supports the following formats: MP3, WAV, AAC, FLAC, AMR, 3GP, M4A, WMA, OGG, and APE.

Moderation Policy Selection: Please select the moderation policy you have configured (if no policy is configured, the system's default policy can be used). Each moderation policy corresponds to a category, and you can customize moderation scenes through policy customization. Options for moderation include pornographic content, illegal activity or non-compliant behavior, and advertising content, and you can select one or multiple scenes for moderation. For more information on how to configure a moderation policy, see [Setting Moderation Policy](#).

Daily Moderation Limit: You can set the maximum quantity of audio files to be moderated per day. By default, there is no upper limit.

Moderation Scene: Moderation categories display the scenes that you configured in the moderation policy, and you can select the desired categories for moderation.

Review Text:

Moderation Suffix: Text files with the suffix TXT or no suffix can be moderated.

Moderation Policy Selection: Please select the moderation policy you have configured (if no policy is configured, the system's default policy can be used). Each moderation policy corresponds to a category, and you can customize moderation scenes through policy customization. Options for moderation include pornographic content, illegal activity or non-compliant behavior, and advertising content, and you can select one or multiple scenes for moderation. For more information on how to configure a moderation policy, see [Setting Moderation Policy](#).

Daily Moderation Limit: You can set the maximum amount of text files moderated per day. By default, there is no upper limit.

Moderation Scene: Moderation categories display the scenes that you configured in the moderation policy, and you can select the desired categories for moderation.

Review More:

Moderation Suffix: The file formats supporting moderation include presentations, text files, spreadsheets, PDFs, among others. You can select multiple formats.

Moderation Policy Selection: Please select the moderation policy you have configured (if no policy is configured, the system's default policy can be used). Each moderation policy corresponds to a category, and you can customize moderation scenes through policy customization. Options for moderation include pornographic content, illegal activity or non-compliant behavior, and advertising content, and you can select one or multiple scenes for moderation. For more information on how to configure a moderation policy, see [Setting Moderation Policy](#).

Daily Moderation Limit: You can configure the maximum number of files that can be moderated per day. By default, there is no upper limit.

Moderation Scene: The scenes you have configured in your selected moderation policy are displayed here. You can select the scenes you want to moderate.

9. In the Block Policy interface, configure the block policy, and then click **Next**. Enabling the block policy authorizes Cloud Infinite (CI) services to conduct automatic moderation or manual re-moderation on certain types of files, forbidding public read access to any identified non-compliant content.

✓ Scan Range

✓ Moderation Policy

3 Block Policy

4 moderation result

5 Finish

Image blocking and human review settings ☒

Pornographic content blocking settings

Score-based blocking ☒

Human review ⓘ ☐

When the score is greater than or equal to , the moderated content will be blocked

Violence/Terrorism content blocking settings

Score-based blocking ☒

Human review ⓘ ☐

When the score is greater than or equal to , the moderated content will be blocked

Political content blocking settings

Score-based blocking ☒

Human review ⓘ ☐

When the score is greater than or equal to , the moderated content will be blocked

Ad blocking settings

Score-based blocking ☒

Human review ⓘ ☐

When the score is greater than or equal to , the moderated content will be blocked

CDN cache purge after blocking ⓘ ☐

After file block is enabled, the moderated files will be auto-blocked according to the predefined block policy. Modifications are divided into three categories based on their score: normal (scores 0–60), suspected (scores 61–90), and restricted (scores 91–100).

Block mode

☒ Change the file ACL to private read

The file ACL will be changed to private read. For more information, see [ACL Overview](#).

☐ Transfer the file to the backup directory

Previous

Next

Image blocking and human review settings: You can set values (that is, integers from 60 to 100) based on different moderation types. The images will be blocked when the set value range is reached. By default, direct blocking is selected. If you select manual re-moderation, a secondary review on the image will be carried out by a professional security team.

Note:

The moderation results are classified into confirmed sensitive, likely sensitive, and normal categories based on the moderation score.

The score range for confirmed sensitive images is ≥ 91 .

The score range for potentially sensitive images is from 61 to 90. The system may not accurately identify these images as sensitive, thus it's recommended that users should conduct manual re-moderation to ensure the anti-spam nature of the images.

The score range for normal images is ≤ 60 . The system considers these images as normal.

CDN Cache Purge after Blocking: When it is enabled, the corresponding domain's CDN cache data will be purged while the COS origin file is blocked.

Block Mode: The following two blocking modes are supported.

Change the file ACL to private: Files are blocked through the modification of the file's access permission to private read. When this mode is used, a re-attempt to access the file would return a 403 status code, indicating that access to the file is not allowed. For information about file permissions, see [ACL](#).

Transfer the file to the backup directory: Files are blocked through the move of the file to the backup directory. When this mode is used, a re-attempt to access the file returns a 404 status code, indicating that the file does not exist. The backup directory is automatically generated by the background, located in the path of the current bucket: `audit_freeze_backup/increment_audit`.

10. On the Moderation Results page, set up the callback for moderation results and click **Next**.

After enabling callback settings, we will direct the moderation results to your designated callback address. You need to set the callback type, callback content, and callback URL.

✓ Scan Range

>

✓ Moderation Policy

>

✓ Block Policy

>

4 moderation result

>

5 Finish

Callback

☒

Once callback is enabled, the file moderation results will be sent back to you.[Callback Settings Help Documentation](#)

Callback scenario

☒ Pornographic

☒ Violence/Terrorism

☒ Political

☒ Ad

Callback Mode

☒ Lite

☐ Detailed

Callback Content

☒ Non-compliance callback

☐ Block callback

☐ Custom callback

▼ More callback events

Callback URL

The callback notification will be sent as a POST request. By default, your callback URL is available only if the status code 200 is returned. The configuration

Callback URL protocol

☒ Force HTTP

☐ Force HTTPS

Previous

Next

Callback Scenario: Based on the moderation policy you have set, options include pornographic content, illegal and non-compliant content, advertisement moderation, illegal content, and verbal abuses.

Callback Mode: You have chosen either Lite or Detailed mode.

Callback Content: Options include callback only for non-compliant files, callback only for blocked files, and callback for all files. Re-moderation is also supported for files that failed the first moderation.


Callback URL: The callback URL must by default return a 200 status code.

Callback URL Protocol: You can choose either enforced HTTP or HTTPS.

11. After checking all task configurations, click **Create** to complete task creation.

Viewing Task Results

On the Existing File Moderation page, you can perform different operations based on the task status.

Overview		Task State	Progress	Oper
Task ID:	task180f6c3389d211eeb321525400553fa5			
Moderation policy:	Image Default policy (preset)			
Moderation path:	Scan range: Bucket file list ci-file-1316781462/picture Upload time range: Before 2023-11-23 15:29:53	 under review Start Time: 2023-11-23 15:29:53	Scan: 0 images 0 video(s) 0 audio(s) 0 text(s) 0 document(s) Scanning count0 file(s) Moderation: 0 images 0 video(s) 0 audio(s) 0 text(s) 0 document(s)	Task Term
Moderate the content in the specified path:	/picture			

When the task status is **under review**, you can click **Task Configuration** or **Terminate Task**.

When the task status is **Job completed**, you can view **Moderation Details** or **Result Statistics**.

Moderation Details: Only moderation details from the past one month can be viewed. After clicking this option, you will be redirected to the moderation page where you can export moderation results, conduct manual moderation, and so on. For specific operation instructions, see [Moderation Details](#).

Result Statistics: This page displays the statistical results of the moderation task. If you have any doubts about the moderation results, you can go to the Moderation Details page on the control panel to view the specific moderation contents.

Setting Moderation Policy

Last updated : 2024-01-06 15:31:10

Overview

When you use the content moderation service, you can specify a moderation category through a moderation policy to moderate content in custom scenes. For different file types, COS provides different scenes for your choice, making it easier for you to customize moderation policies that suit your business.

Currently, the file types and corresponding moderation scenes supported by COS are as follows:

Supported File Types	Moderation Scenes	Specific Moderation Categories
Image moderation policy, video moderation policy, audio moderation policy, text moderation policy, file moderation policy,Webpage Moderation policy	Pornographic content	Sexually suggestive/vulgar behaviors
		Genital nudity/Sexual behaviors
		Sex toys
		Sexy content
		Pornographic text moderation
	Advertising content	QR code and barcode recognition
		Logo detection and recognition
		Advertising text moderation
	Other non-compliant content	Fire, explosion, bloody scene, etc.

Note:

WEBP images involving advertising QR codes cannot be moderated currently.

Directions

Default policy

Each moderation type has a default moderation policy, which is configured by Tencent Cloud based on your historical moderation conditions. If you have never used the moderation service, the policy developed by algorithm experts based on models for multiple industries will be used by default, which will be suitable for most content security requirements.

Note:

The default policy can be viewed and edited but not deleted.

Custom policy

If the default policy cannot meet your business needs, or you have multiple scenes that require different moderation policies, you can create custom policies as needed.

1. Log in to the [COS console](#).
2. Click **Bucket List** on the left sidebar.
3. Click the name of the target bucket to enter the configuration page.
4. Select **Content Moderation** > **Moderation Policy** on the left sidebar.
5. Create a moderation policy based on your business needs. Currently, you can create policies for **image moderation**, **video moderation**, **audio moderation**, **text moderation**, and **file moderation**.
Take the image moderation policy as an example:
 - i. Click **Create Image Moderation Policy** and enter the policy name.
 - ii. Select the category you need to moderate under the moderation type, where OCR pornographic text moderation indicates to moderate image content based on OCR.
 - iii. Click **Save** to create the policy.
6. After the moderation policy is created, the backend will automatically generate a unique `Biztype` value.
7. You can view or edit the created moderation policy; however, you cannot change its name and `Biztype` value.

Using moderation policy

After the moderation policy is created, configure [automatic moderation](#), create a historical data moderation job, or call a [content moderation API](#). You can select the corresponding policy to moderate content in custom categories.

Automatic moderation

Create an automatic moderation configuration in the console, and you can manually select a moderation policy.

Historical data moderation

Create a historical data moderation job in the console, and you can manually select a moderation policy.

Moderation APIs

When calling an API for content moderation, you can manually pass in the `Biztype` value to the API, which you can view in the list of moderation policies in the console. If you don't pass it in, the default policy will be used.

Setting the Custom Image Risk Library

Last updated : 2024-03-25 15:01:26

Overview

The custom image risk library is designed to help you manage images or keywords that need to be moderated. With risk library customization, you can configure the images or keywords to allow or block them. This can be applied to all moderation scenes.

Image Risk Library

You can use an image risk library to manage images that need to be blocked or allowed, to address unexpected control requirements.

Six preset image risk libraries are available in the system:

Normal image library: The returned moderation result will be normal for images that match those in this library.

Pornographic and illegal image library: The returned moderation result will be the corresponding violation tag for images that match those in the library.

Creating new image risk library is not supported. You can add sample images to the existing default libraries.

Note:

The image risk library is effective by account. After you add sample images to the gallery in any bucket under the same account, these images will automatically take effect in all your buckets and all your moderation policies.

A single image library can contain a maximum of 10,000 sample images.

Some specific images may fail to be added to the image library. In this case, please [contact us](#) for assistance.

Text Risk Library

You can use the text risk library to manage text to be blocked or allowed, in order to address sudden control requirements.

The text risk library contains the following types:

Pre-defined text library: It is a text library with pre-defined policies for you, which includes:

Normal text library: If a keyword in the library is matched, the moderation result will be returned as normal.

Pornographic text library, illegal text library, and other text libraries: If a keyword in the library is matched, the moderation result will be returned as the corresponding violation tag.

Note:

The pre-defined text library takes effect by account. After you add sample keywords to any pre-defined text library for the same account, these keywords will automatically take effect in all your storage buckets and all moderation policies. Up to 10,000 sample keywords can be added to a pre-defined text library.

Custom text library: It is the text library you create, where you can add samples of various types of violations. If the text under moderation matches a keyword in the library, it will be marked with the corresponding tag based on the defined library policy.

Note:

The custom text library needs to be associated with a moderation policy and only takes effect within the associated moderation policy.

Up to 2,000 sample keywords can be added to a single custom text library.

Directions

1. Log in to the [Cloud Object Storage console](#). On the **Bucket List** page, select the required bucket to open the bucket management page.
2. On the left navigation bar, choose **Sensitive Content Moderation > Custom Risk Library**.
3. On the **Custom Risk Library** page, three tabs are displayed: **Image Risk Library**, **Text Risk Library**, and **Business Field Risk Library**. For instructions on operating the Business Field Risk Library, see [Setting the Business Field Risk Library](#).

[← Back to Bucket List](#)

Custom Risk Library

Image Risk Library

Text Risk Library

Business Field Risk Library

Search menu name

Overview

File List

Basic Configurations

Security Management

Permission Management

Domains and Transfer

Fault Tolerance and Disaster Recovery

Logging

Sensitive Content Moderation HOT

- Functional experience
- Statistics
- Moderation Details
- Auto Audit Configuration
- Existing File Moderation
- Moderation Policy
- Custom Risk Library

You can customize a image risk library to block/pass images as needed. For more information, please see [Setting a Custom Risk Library](#)

Note: This configuration is global and will take effect for **all buckets and all audit policies**.

Image Library Name	Image Library Policy	Match Type	Moderation policy associated
Normal Image Library (Default)	Normal	Exact	Take effect globally
Violent/Terrorist Image Library (Default)	Sensitive	Exact	Take effect globally
Pornographic Image Library (Default)	Sensitive	Exact	Take effect globally
Political Image Library (Default)	Sensitive	Exact	Take effect globally
Restricted Image Library (Default)	Sensitive	Exact	Take effect globally
Ad Image Library (Default)	Sensitive	Exact	Take effect globally
Total 6 items			

4. The operations on Image Risk Library and Text Risk Library are as follows:


Image Risk Library

Text Risk Library

To handle incorrect moderation, you can add image clean samples, to ensure the image moderation results return as normal:

Find the normal image library (pre-defined) in the list and click **Manage** to the right of the library to access the Image Risk Library page.

On the Image Risk Library page, you can perform the following operations:

 **Image Risk Library - Management**


Note: This configuration is global and will take effect for all buckets.


Image library name
[Normal Image Library \(Default\)](#)

Image library policy
[Normal](#)

Samples
1

Match Type [Exact](#) Status [Enable](#)

[Add Sample](#) [Delete](#) 

<input type="checkbox"/>	Thumbnail	Sample Name	Remarks	Added On
<input type="checkbox"/>		1.jpeg	-	2023-09-13 10:

Total 1 Items

Viewing the image library policy: The policy for the normal image library is normal.

Viewing samples: Check the number of samples added to the image library.


Adding samples: You can add selected images to the library as samples.

Deleting samples: You can delete sample images from your image library.

For scenarios of missed moderation, add image block samples so that the image moderation results return as sensitive:

In the list, find the image library for with the returned sensitive type is desired. If you add an image to the pornographic image library (pre-defined), the moderation result will be tagged as pornography. Click **Manage** on the right of the library to open the Image Risk Library page.

On the Image Risk Library page, you can perform the following operations:

 **Image Risk Library - Management**


Note: This configuration is global and will take effect for all buckets.

Image library name	Image library policy	Samples
Pornographic Image Library (Default)	Sensitive	0

Match Type	Exact	Status	Enable
------------	-------	--------	--------

[Add Sample](#)

[Delete](#)



<input type="checkbox"/>	Thumbnail	Sample Name	Remarks	Added On
The current list is empty				

Total 0 items

Viewing the image library policy: The policy for the pornographic image library is sensitive.

Viewing samples: Check the number of samples added to the image library.

Adding samples: You can add specific images to the library as samples.

Deleting samples: You can delete sample images from your image library.

You can directly add keywords into the pre-defined text library or create a custom text library to add keywords:

Keywords added to the pre-defined text library will take effect for all moderation policies:

← Back to Bucket List

Search menu name Q

Overview

File List

Basic Configurations ▾

Security Management ▾

Permission Management ▾

Domains and Transfer ▾

Fault Tolerance and Disaster Recovery ▾

Logging ▾

Sensitive Content Moderation **HOT**

- Functional experience
- Statistics
- Moderation Details
- Auto Audit Configuration
- Existing File Moderation
- Moderation Policy
- Custom Risk Library

Custom Risk Library

Image Risk Library **Text Risk Library** Business Field Risk Library

You can use the Text Risk Library to manage the text that need to be blocked or allowed in a targeted manner and respond to unexpected control needs. For details, please see The System Preset Text Library is globally effective and does not need to be associated with audit policies, and will be added in your **all buckets and all audit policies**. The Custom Text Library takes effect only when you associate it with audit policies.

create Custom Text Library

System Preset Text Library ▾

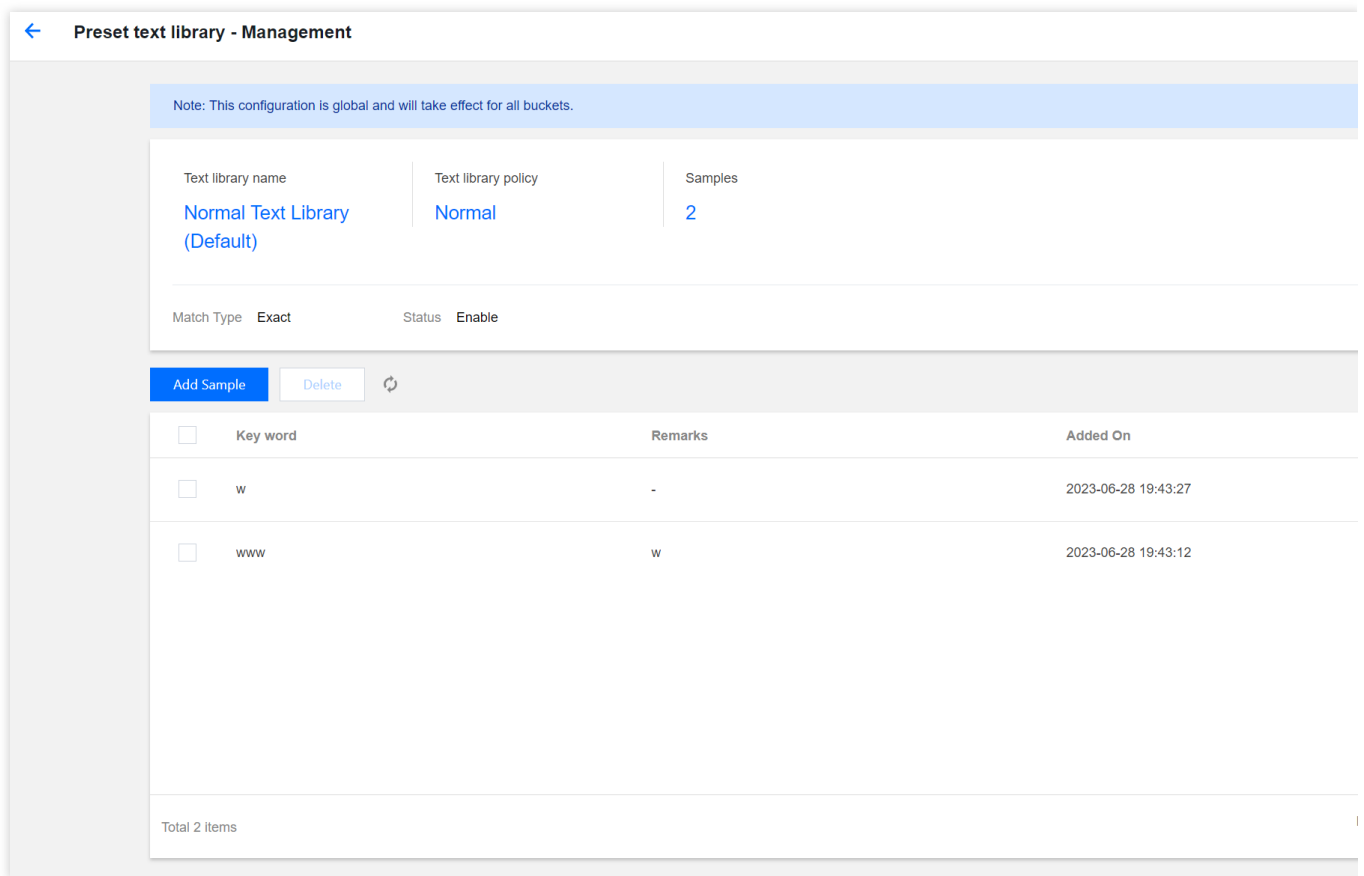
Text Library Name	Text Library Policy	Match Type	Moderation policy associated
Normal Text Library (Default)	Normal	Exact	Take effect globally
Violent/Terrorist Text Library (Default)	Sensitive	Exact	Take effect globally
Pornographic Text Library (Default)	Sensitive	Exact	Take effect globally
Political Text Library (Default)	Sensitive	Exact	Take effect globally
Restricted Text Library (Default)	Sensitive	Exact	Take effect globally
Ad Text Library (Default)	Sensitive	Exact	Take effect globally
Abuse text library (preset)	Sensitive	Exact	Take effect globally
Total 7 items			

If you want to add clean sample keywords, find the normal text library (pre-defined) in the list, and then click **Manage** on the right side of the text library to open the Text Risk Library page.

On the Text Risk Library page, you can perform the following operations:

©2013-2022 Tencent Cloud. All rights reserved.

Page 248 of 358



Viewing the text library policy: The policy of the normal text library is normal.

Viewing samples: Check the number of samples added to the text library.

Adding samples: You can add specific keywords into the text library as samples.

Deleting samples: You can delete keywords from the text library.

Creating a custom text library: The custom text library needs to be associated with a moderation policy. In moderation operations, only the text library associated with moderation policies takes effect:

Click **Create Custom Text Library**, and in the window, specify the Text Library Name, and select the Text Library Policy and Match Type:

Text Library Policy: When a keyword sample in the text library is matched, you can choose sensitive or suspected as the returned moderation result.

Match Type: You can choose an exact match or a fuzzy match. For a fuzzy match, variants of the entered keyword can be detected to match similar words. Split words, homographs, homophones, simplified or traditional forms, case differences, and numeral words are supported.

After the Custom Text Library has been created, find the newly created library in the list, and click **Manage** on the right side of the selected library to open the Text Risk Library page.

On the Text Risk Library page, you can perform the following operations:

[←](#) Custom text library - management

Text library name

defzq

Text library policy

Sensitive

Samples

0

Match Type

Add Sample

Import Sample

Delete

↻

Please enter a keyword

<input type="checkbox"/>	Non-compliance ty... ▼	Suggestions	Key word	Remarks	Added On
The current list is empty					

Total 0 items

Viewing the text library policy: The custom text library policy can be sensitive or suspected.

Viewing samples: Check the number of samples added to the text library.

Adding samples: You can add specific keywords into the text library as samples.

Deleting samples: You can delete keywords from the text library.

5. After the risk library is configured, if samples from the risk library are encountered while you use the content moderation feature, they will be automatically allowed or blocked according to the risk policy.

Setting the Business Field Risk Library

Last updated : 2024-03-25 15:01:26

Overview

Content moderation supports adding the business field `UserInfo` to tag the data for moderation, including nickname information, account details, room number, and so on. For more information, see [API Documentation](#). This allows you to manage users or IP addresses that need to be blocked or allowed. For example, you can blacklist a certain nickname so that data entries containing that nickname field will be blocked by default.

Differences between the Business Field Risk Library and the Image and Text Risk Library

The business field risk library manages the business fields that you add when you call the moderation API, while the image and text risk library manages the content of images or text.

The business fields that can be added to the risk library include:

Field Name	Description
TokenId	It usually indicates account information, limited to 128 bytes in length.

Note

Up to 10,000 fields can be added to a business field risk library.

Operations

1. Log in to the [Cloud Object Storage console](#). On the **Bucket List** page, select the required bucket to open to the Bucket List page.
2. On the left navigation bar, select **Sensitive Content Moderation > Custom Risk Library**.
3. On the **Custom Risk Library** page, select the **Business Field Risk Library** tab, and then click **create business field risk library**.

create business field risk library

library name	Match field	library type	Moderation policy associated	Creation
No data yet				

Total 0 items

create business field risk library

library name *

Enter the library name

Enter up to 32 characters of Chinese characters, letters, digits, and underscores (_)

Match field

TokenId ▼

library type ⓘ

☒ Block-library - sensitive ☐ Block-library - suspected ☐ Allow-library

Moderation policy associated

Select a moderation policy type ▼

OK

Cancel

4. Enter the related content:

Library name: Up to 32 Chinese and English characters, digits, and underscores are supported.

Match field: Select the business field to be controlled. Currently, only TokenId is supported.

Library type: Select the corresponding library type. When the content in the library is matched, the returned moderation result will be the corresponding type. The blocklist result can be sensitive or suspected, and the allowlist result is normal.

Moderation policy associated: A business field risk library requires an associated policy and is effective only for the associated policy.

5. Click **OK** to completing creating the business field risk library.

6. After the library is created, you can manage, edit, or delete the library.

7. Click **Manage** to open the management interface of the current library. You can add or delete content on this page. The content here corresponds to the business field. For example, if you choose TokenId as the matching field (TokenId usually indicates the account ID), then the content here is the specific account ID, such as 12345678 and 1008787.

[←](#) **Business Field Risk Library - Management**

library name

define

library policy

Block-library - sensitive

Content entries

2

Status

Enable

Add Content

Delete

<input type="checkbox"/>	Content	Added On
<input type="checkbox"/>	add	2023-11-29 20:14:09
<input type="checkbox"/>	test	2023-11-29 20:14:09

8. Click **Edit** to modify the account settings: The library name and associated moderation policy can be modified, but the matching field and library type cannot be modified.

Smart Toolbox User Guide

Last updated : 2024-01-06 14:48:14

Overview

The smart toolbox provides tools for processing almost all types of multimedia files, such as image watermark, image compression, and audio/video/file format conversion. It presents various capabilities of COS in the form of convenient and quick tools in the console for you to use with speed and easy.

Notes

All the capabilities in the smart toolbox are implemented based on the data processing APIs of COS. Using them is equivalent to calling such APIs. You need to keep the following in mind during use:

When you use the smart toolbox for the first time, the **CI** service will be activated for you free of charge.

Whenever a processing operation is completed through the toolbox, it is equivalent to calling a data processing API once and incurs processing fees as detailed below:

Tool	Fees
Image compression (WebP or JPEG format), image editing, image watermark, and image information	Basic image processing
Image compression (AVIF or HEIF format)	Image advanced compression
Audio/Video processing	Media processing
AI processing	Content recognition
Online file preview	File preview

Tools

The smart toolbox currently contains the following tools:

Category	Tool
Image processing	Image compression
	Image editing

	Image watermark
	Image information
Audio/Video processing	Audio/Video format conversion
	Top speed codec transcoding
	Video frame capturing
	Video-to-animated image conversion
	Intelligent thumbnail
	Digital remastering
AI processing	Image tagging
	Vehicle and license plate detection
File processing	Online file preview

Image processing

1. Image compression

The image compression tool implements the process of downsizing an image as much as possible without sacrificing quality so that it can be stored at a lower cost and accessed more quickly.

Directions

1. Log in to the [COS console](#) and click **Smart Toolbox** on the left sidebar.
2. On the **Smart Toolbox** page, select **Image Processing > Image Compression**.
3. In the image upload area, select an existing image in the bucket and add it to the tool.
4. After the image is added, the tool will automatically process it, and you can see the size of the compressed image on the left. You can also download the compressed image.

2. Image editing

The image editing tool offers capabilities of image cropping, rotation, scaling, sharpening, brightness adjustment, and contrast adjustment.

Directions

After adding an image as instructed in steps 1–3 in the [Image compression](#) section, use tools on the left to make corresponding adjustments.

3. Image watermark

The image watermark tool allows you to add an image or text to another image in the form of watermark.

Directions

Image watermark: After adding an image as instructed in steps 1–3 in the [Image compression](#) section, click **Image Watermark** on the left, select an existing image in the bucket, adjust the margins, and click **Generate Watermark**.
Text Watermark: Click **Text Watermark** on the left, enter the watermark text, adjust the margins, font, and font size, and click **Generate Watermark**.

4. Image information

The image information tool lists the format, size, and MD5 information of an image.

Directions

After adding an image, click **Information** on the left to view the information of the image.

Audio/Video processing

1. Audio/Video format conversion

The audio/video format conversion tool can convert your audio/video files into MP4, MP3, MOV, AVI, MKV, and other formats. It allows you to set different parameters such as video resolution and audio bitrate during conversion to adapt to different terminals and network environments.

Directions

1. Log in to the [COS console](#) and click **Smart Toolbox** on the left sidebar.
2. On the **Smart Toolbox** page, select **Audio/Video Processing > Audio/Video Format Conversion**.
3. Select an audio/video file and add it to the tool. You can select existing files in the bucket or local files, but if you select local files, you need to upload them to the bucket, as the tool can convert files in the bucket only.
4. After selecting an audio/video file, you need to select the conversion parameters as detailed below:
The following is an example of converting a video with parameters of **MP4 format, H.264 codec, 720 * proportional height resolution, and 1024 Kbps bitrate**:
Video format: MP4
Video codec: H.264
Video resolution: 720 (width) * proportional height of the input video
Video bitrate: 1024 Kbps
5. After selecting parameters, select the name and location of the output video in the bucket and click **Finish**.
6. Click **Start Transcoding** and wait for the transcoding to complete.

7. After transcoding is completed, the input and output videos are displayed in the left and right of the video display area respectively for you to directly compare and check the transcoding effect. You can copy the output video link or directly download the output video by clicking buttons in the bottom-right corner.

2. Top speed codec transcoding

Top speed codec transcoding leverages deep learning algorithms to convert an input video to an output video with higher definition, lower noise, and higher frame rate by reducing the compression and texture distortion of the input video.

Directions

The steps of top speed codec transcoding are similar to those of audio/video file conversion, except that the output video transcoded by top speed codec is smaller and clearer.

3. Video frame capturing

With the video frame capturing tool, you can capture any frame in a video and save it as an image.

Directions

1. Add a video to the tool as instructed in steps 1–3 in the [Audio/Video format conversion](#) section and select frame capturing parameters.
2. After the video is added, the tool will automatically start capturing frames and display the captured frames on the right.

4. Video-to-animated image conversion

The video-to-animated image conversion tool can convert your video into a GIF or WebP animated image.

Directions

1. Add a video to the tool as instructed in steps 1–3 in the [Audio/Video format conversion](#) section and select video-to-animated image conversion parameters.
2. After the video is added, the tool will automatically start converting and display the output animated image on the right.

5. Intelligent thumbnail

By intelligently recognizing and analyzing the characteristics of motions, events, and faces in the video, the intelligent thumbnail tool can automatically identify, capture, and save highlight frames as video thumbnails.

Directions

1. Add a video to the tool as instructed in steps 1–3 in the [Audio/Video format conversion](#) section.
2. After the video is added, the tool will automatically start analyzing the video and capturing highlight frames and display the captured frames on the right.

6. Digital remastering

The digital remastering tool has video noise cancellation, super resolution, SDR to HDR, sharpening, and other capabilities. Through the combination of different capabilities, it can meet your needs for remastering old and low-quality videos.

Directions

1. Add a video to the tool as instructed in steps 1–3 in the [Audio/Video format conversion](#) section.
2. After adding the video, select the target resolution and click **Start Remastering**.

AI processing

1. Image tagging

The image tagging tool can identify scenes, objects, people, and other information in images. It contains thousands of tags in over 60 subcategories in 8 categories, such as natural scenery (mountain, sea, sky, sunset, etc.), man-made environment (building, playground, meeting room, etc.), people (male, female, selfie, group photo, etc.), object (food, clothing, daily necessities, etc.), and pet/wild animal (cat, dog, bird, mammal, marine animal, etc.).

Directions

1. Log in to the [COS console](#) and click **Smart Toolbox** on the left sidebar.
2. On the **Smart Toolbox** page, select **AI Processing** > **Image Tagging**.
3. Add an image to the tool.
4. After the image is added, the tool will automatically start analyzing the image and display image tag information on the right.

2. Vehicle and license plate detection

The vehicle and license plate detection tool can accurately identify the coordinates, brands, models, model years, and colors of almost all passenger cars on the market.

Directions

1. Add an image to the tool as instructed in steps 1–3 in the [Image tagging](#) section.
2. After the image is added, the tool will automatically start analyzing the image and display the vehicle and license plate information on the right.

File processing

Online file preview

The file preview tool can convert any Office documents into a webpage format that can be previewed online. After conversion, you can copy the file link to view the file in a browser.

Directions

1. Log in to the [COS console](#) and click **Smart Toolbox** on the left sidebar.
2. On the **Smart Toolbox** page, select **File Preview > Online File Preview**.
3. Add a file (e.g., a PPT file) to the tool.
4. After the PPT file is added, the tool will automatically start processing it to generate the HTML webpage for online preview. You can preview it directly or copy the link to preview it in a browser.

Data Processing Workflow

Custom Function Processing

Last updated : 2024-06-24 16:14:43

Overview

If the existing services or features of COS media processing cannot meet your needs, you can use the custom function processing feature of SCF to write core code logic in order to flexibly implement your business needs while reducing your development costs. For more information on SCF, see [Overview](#).

Note:

Currently, the custom function processing feature can only be initiated in a [workflow](#).

Using SCF for custom processing will incur fees, which will be charged by SCF. For billing details, see [Billing Overview](#).

Directions

1. Log in to the [COS console](#).
2. Select **Bucket List** on the left sidebar.
3. Click the name of the desired bucket.
4. On the left sidebar, click **Data Processing Workflow > Workflow** to enter the workflow management page.
5. Click **Create Workflow**.
6. Click **+** to the right of "Configure Workflow" to add a **custom function** node.

Workflow Name *

Enter workflow name

Only a combination of letters, numbers, Chinese characters, underscores (_) and hyphens (-) with a length of 3 to 64 characters.

Input Bucket Name

examplebucket-125

Input Path ⓘ

If not filled in, it is valid for all paths under the bucket

Select

Format ⓘ

☒ Mainstream video/audio files ⓘ ☐ Image ⓘ ☐ Custom rule ⓘ ☐ All files ⓘ

Queue ⓘ *

Media processing queue (queue-1) ↻

Callback

☒ Use queue callback ☐ Custom

Queue Callback URL ⓘ

Empty [Edit](#)

Configure Workflow

Input

+

Audio/Video Transcoding
Video Frame Capturing
Converting Video to Animated Images
Intelligent Thumbnail
Audio/Video Splicing
Voice Separation
Highlights Generation
Adaptive Bitrate Streaming
SDRtoHDR
Video Enhancement
Audio/Video Segmentation
Custom Function
Image Processing

to open the workflow

End

7. In the pop-up window, configure the following information.

Input Parameters: The input parameters specified with a custom function in a workflow don't need to be added manually. Instead, they can be obtained according to the node before the custom function.

Namespace: The created function is in the COS namespace by default.

Type: Select **Common feature** to quickly perform common operations on COS objects or **Custom** to configure other feature parameters.

Feature: The preset feature is supported when select the common feature.

Function: Currently, only functions that are executed asynchronously and have status tracking enabled are supported in a workflow.

To create a function, click **Create Function** and configure the function as prompted.

8. After confirming that the configuration is correct, click **OK**.

Configuring a Workflow

Last updated : 2024-06-24 16:14:43

Overview

With a data processing workflow, you can quickly and flexibly create video processing processes as needed. A workflow is bound to a path of an input bucket. When a video file is **uploaded** to the path, the media workflow will be **automatically triggered** to perform the specified processing operation, with the processing result automatically saved to the specified path of the destination bucket.

You can use a data processing workflow to implement the following features: **audio/video transcoding (including top speed codec transcoding and broadcast media format transcoding)**, **video frame capturing**, **video-to-animated image conversion**, **intelligent thumbnail**, **audio/video splicing**, **voice separation (also known as voice/sound separation)**, **highlights generation (also known as video montage)**, **adaptive multi-bitrate**, **SDR to HDR**, **video enhancement**, **super resolution**, **audio/video segmentation**, **custom function**, and **image processing**.

Note:

Currently, workflows can process 3GP, ASF, AVI, DV, FLV, F4V, M3U8, M4V, MKV, MOV, MP4, MPG, MPEG, MTS, OGG, RM, RMVB, SWF, VOB, WMV, WEBM, MP3, AAC, FLAC, AMR, M4A, WMA, and WAV files. When initiating a media processing request, you must enter the complete file name and extension; otherwise, the format cannot be recognized and processed.

Currently, the workflow feature can only manipulate video files being uploaded. To perform media operations on cloud data, use the [job](#) feature.

Directions

Creating workflow

1. Log in to the [COS console](#).
2. Click **Bucket List** on the left sidebar.
3. Click the name of the bucket for media processing.
4. On the left sidebar, select **Data Processing Workflow > Workflow** to go to the workflow management page.
5. Click **Create Workflow**.
6. On the **Create Workflow** page, configure the following items:

←

Create Workflow

Workflow Name *

test1

✓

Only a combination of letters, numbers, Chinese characters, underscores (_) and hyphens (-) with a length n

Input Bucket Name *

peach-ns-1258535724 (na-silici)

↻

Input Path ⓘ

If not filled in, it is valid for all paths under the bucket

Select

Format ⓘ

☒ Mainstream video/audio files ⓘ
 ☐ Image ⓘ
 ☐ Custom rule ⓘ
 ☐ All files ⓘ

Queue ⓘ *

Select a queue

↻

Callback

☒ Use queue callback
 ☐ Custom

Queue Callback URL ⓘ

Empty

Edit

Configure Workflow

Input

+

→

↻

→

End

Add a node by clicking "+" to open the workflow

Workflow Name: It is required and can contain up to 128 letters, digits, underscores (_), and hyphens (-).

Input Bucket Name: It is the current bucket by default.

Input Path: It is optional and must start and end with /. If it is not specified, the workflow will be triggered for all paths in the input bucket. After the media workflow is enabled, when a video file is uploaded to this path, the workflow will be automatically triggered.

Format: Select the default audio, video, or image file filter rule or a custom rule. You can also select all files to process all objects in the bucket.

Queue: It is required. When you activate the service, the system will automatically create a user queue for you. When you submit a job, the job will be arranged in the queue first and executed in sequence according to the priority and order of submission. You can view the queue information in **Common Configuration**.

Callback: You can use the queue callback, i.e., callback URL bound to the queue. To modify it, please go to the corresponding queue list.

Configure Workflow: Click + on the right to add any of the following nodes: **audio/video transcoding (including top speed codec transcoding and broadcast media format transcoding), video frame capturing, video to animated image conversion, intelligent thumbnail, audio/video splicing, voice separation, highlights generation, HLS adaptive multi-bitrate, SDR to HDR, video enhancement, super-resolution, audio/video segmentation, custom function, and image processing.** You need to configure at least one job node in a workflow and set the destination bucket, filename (see [Workflow Variable Description](#)), path, and job template for each job node. For more information on templates and how to set them, see [Template](#).

Audio/Video transcoding

Video frame capturing

Video-to-animated image conversion

Intelligent thumbnail

Audio/Video splicing

Audio/Video Transcoding

Destination Bucket *

Select destination bucket ▼

Supports only media processing-enabled buckets in the same region.

Destination File Name *

`${InputName}_${RunId}.${ext}`

Default variables such as `${InputName}` can be used in the destination filenames. For more information about default variables, please see [Workflow Variable Description](#)

Destination Path ⓘ *

`${InputPath}`[Select](#)

`${InputPath}` is the input path (e.g., for the input file `test/path/demo.mp4`, the value of `${InputPath}` should be `test/path/`). A custom path must end with a slash (/).

Transcoding Type

☒ Regular ☐ Top Speed Codec Transcoding ☐ Broadcast Media Format Transcoding

Template Type

☒ System Template ☐ Custom Template

Template *

Please select a task template ▼

Digital Watermark ⓘ



Watermark



Remove Watermark ⓘ



Note: 1. After creating a task, you will be charged for related fees. For more information, see [Billing Guide](#)

2. To use the media processing service, you need to make sure that the resource is available, and the access restriction features such as original image protection and hotlink protection are not enabled.

3. Audio/Video transcoding applies only to files uploaded to the bucket after the workflow is enabled.

OK

Cancel

Video Frame Capturing

Destination Bucket *

Select destination bucket ▼ ↻

Supports only media processing-enabled buckets in the same region.

Destination File Name *

`${InputName}_${RunId}_${Number}.jpg`

Default variables such as `${InputName}` can be used in the destination filenames. For more information about default variables, please see [Workflow Variable Description](#)

Destination Path ⓘ *

`${InputPath}`

Select

`${InputPath}` is the input path (e.g., for the input file `test/path/demo.mp4`, the value of `${InputPath}` should be `test/path/`). A custom path must end with a slash (/).

Template Type

☒ System Template ☐ Custom Template

Template *

Please select a task template ▼ ↻

Note:1. After creating a task, you will be charged for related fees. For more information, see [Billing Guide](#)

2. To use the media processing service, you need to make sure that the resource is available, and the access restriction features such as original image protection and hotlink protection are not enabled.

3. Frame capturing of videos is only valid to video files uploaded to bucket after the workflow is started

OK

Cancel

Converting Video to Animated Images

Destination Bucket *

Select destination bucket ▼ ↻

Supports only media processing-enabled buckets in the same region.

Destination File Name *

`${InputName}_${RunId}.${ext}`

Default variables such as `${InputName}` can be used in the destination filenames. For more information about default variables, please see [Workflow Variable Description](#)

Destination Path ⓘ *

`${InputPath}`[Select](#)

`${InputPath}` is the input path (e.g., for the input file `test/path/demo.mp4`, the value of `${InputPath}` should be `test/path/`). A custom path must end with a slash (/).

Template Type

☒ System Template ☐ Custom Template

Template *

Please select a task template ▼ ↻

Note: 1. After creating a task, you will be charged for related fees. For more information, see [Billing Guide](#)

2. To use the media processing service, you need to make sure that the resource is available, and the access restriction features such as original image protection and hotlink protection are not enabled.


3. Video to animated image converting is only valid to video files uploaded to the bucket after workflow is started

OK

Cancel

Intelligent Thumbnail ✕

Destination Bucket *

Select destination bucket ▾ 

Supports only media processing-enabled buckets in the same region.

Destination File Name *


`${InputName}_${RunId}_${Number}.jpg`

Default variables such as `${InputName}` can be used in the destination filenames. For more information about default variables, please see [Workflow Variable Description](#)

Destination Path ⓘ *

`${InputPath}` Select

`${InputPath}` is the input path (e.g., for the input file test/path/demo.mp4, the value of `${InputPath}` should be test/path/). A custom path must end with a slash (/).

Note:1. After creating a task, you will be charged for related fees. For more information, see [Billing Guide](#) 

2. To use the media processing service, you need to make sure that the resource is available, and the access restriction features such as original image protection and hotlink protection are not enabled.

3. Intelligent cover is only effective to video files uploaded to the bucket after the workflow is started

OK

Cancel

Description: The intelligent thumbnail feature understands the video content with the aid of Tencent Cloud's advanced AI technologies to intelligently extract three optimal keyframes.

Audio/Video Splicing

Destination Bucket *

Select destination bucket

Supports only media processing-enabled buckets in the same region.

Destination File Name *

`${InputName}_${RunId}.${ext}`

Default variables such as `${InputName}` can be used in the destination filenames. For more information about default variables, please see [Workflow Variable Description](#)

Destination Path ⓘ *

`${InputPath}`

Select

`${InputPath}` is the input path (e.g., for the input file test/path/demo.mp4, the value of `${InputPath}` should be test/path/). A custom path must end with a slash (/).

Template *

Please select a task template

Supports only templates with opening or closing credits. For more templates, go to [Create Template](#)

Note:1. After creating a task, you will be charged for related fees. For more information, see [Billing Guide](#)

2. To use the media processing service, you need to make sure that the resource is available, and the access restriction features such as original image protection and hotlink protection are not enabled.

3. Audio/video splicing is only effective to video files uploaded to the bucket after the workflow is started

OK

Cancel

Voice separation

Highlights generation

Adaptive bitrate streaming

SDRtoHDR

Video enhancement

Voice Separation

Destination Bucket *

Select destination bucket ▾



Supports only media processing-enabled buckets in the same region.

Voice Filename *

`${InputName}_${RunId}_vocal.${ext}`

Default variables such as `${InputName}` can be used in the destination filenames. For more information about default variables, please see [Workflow Variable Description](#)

Background Sound Filename *

`${InputName}_${RunId}_background.${ext}`

Default variables such as `${InputName}` can be used in the destination filenames. For more information about default variables, please see [Workflow Variable Description](#)

Destination Path ⓘ *

`${InputPath}`[Select](#)

`${InputPath}` is the input path (e.g., for the input file `test/path/demo.mp4`, the value of `${InputPath}` should be `test/path/`). A custom path must end with a slash (/).

Template *

Please select a task template ▾



For more templates, go to [Create Template](#)

Note:1. After creating a task, you will be charged for related fees. For more information, see [Billing Guide](#)

2. To use the media processing service, you need to make sure that the resource is available, and the access restriction features such as original image protection and hotlink protection are not enabled.

3. Voice Separation takes effect only for files uploaded to the bucket after the workflow is enabled.

OK

Cancel

Highlights Generation

Destination Bucket *

Select destination bucket ▾ ↻

Supports only media processing-enabled buckets in the same region.

Destination File Name *

`${InputName}_${RunId}.${ext}`

Default variables such as `${InputName}` can be used in the destination filenames. For more information about default variables, please see [Workflow Variable Description](#)

Destination Path ⓘ *

`${InputPath}`

Select

`${InputPath}` is the input path (e.g., for the input file `test/path/demo.mp4`, the value of `${InputPath}` should be `test/path/`). A custom path must end with a slash (/).

Template *

Please select a task template ▾ ↻

For more templates, go to [Create Template](#)

Note:1. After creating a task, you will be charged for related fees. For more information, see [Billing Guide](#)

2. To use the media processing service, you need to make sure that the resource is available, and the access restriction features such as original image protection and hotlink protection are not enabled.
3. Highlights Generation take effect only for videos uploaded to the bucket after the workflow is enabled.

OK

Cancel

Packaging Configuration

Package Format

HLS

Destination Bucket *

Select destination bucket

Supports only media processing-enabled buckets in the same region.

Destination File Name *

`${InputName}_${RunId}.${ext}`

Default variables such as `${InputName}` can be used in the destination filenames. For more information about default variables, please see [Workflow Variable Description](#)

Destination Path ⓘ *

`${InputPath}`

Select

`${InputPath}` is the input path (e.g., for the input file `test/path/demo.mp4`, the value of `${InputPath}` should be `test/path/`). A custom path must end with a slash (/).

Note:1. After creating a task, you will be charged for related fees. For more information, see [Billing Guide](#)

2. To use the media processing service, you need to make sure that the resource is available, and the access restriction features such as original image protection and hotlink protection are not enabled.

OK

Cancel

Description: The HLS adaptive multi-bitrate feature encapsulates multiple files with multiple bitrates and audio tracks into one multi-bitrate adaptive HLS or DASH video file.

SDRtoHDR✕

Destination Bucket *

Select destination bucket ▾ ↻

Supports only media processing-enabled buckets in the same region.

Destination File Name *

`${InputName}_${RunId}.${ext}`

Default variables such as `${InputName}` can be used in the destination filenames. For more information about default variables, please see [Workflow Variable Description](#)

Destination Path ⓘ *

`${InputPath}` Select

`${InputPath}` is the input path (e.g., for the input file test/path/demo.mp4, the value of `${InputPath}` should be test/path/). A custom path must end with a slash (/).

HDR Standard

☒ HLG ☐ HDR10

Transcoding Template ⓘ *

Select H.265Transcoding Template ▾ ↻

Supports only H.265 transcoding templates.[Create Template](#)

Watermark

☐

Note:1. After creating a task, you will be charged for related fees. For more information, see [Billing Guide](#) 🔗

2. To use the media processing service, you need to make sure that the resource is available, and the access restriction features such as original image protection and hotlink protection are not enabled.

3. SDRtoHDR takes effect only for objects uploaded to the bucket after the workflow is enabled.

OK

Cancel

Super resolution

Audio/Video segmentation

Custom function

Image processing

Audio/Video information (determining node)

Audio/Video Segmentation ✕

Destination Bucket *

Select destination bucket ▼ ↻

Supports only media processing-enabled buckets in the same region.

Destination File Name *

`${InputName}_${Number}.${ext}`

`${Number}` must be included as the sequence number of each output audio/video segment. For example, if Destination Filename is set to test-`${Number}`.mp4 and the file is segmented into two parts, the actual destination filenames will be test-0.mp4 and test-1.mp4.

Destination Path ⓘ *

`${InputPath}` Select

`${InputPath}` is the input path (e.g., for the input file test/path/demo.mp4, the value of `${InputPath}` should be test/path/). A custom path must end with a slash (/).

Encapsulation Format

MP4 ▼

Segment Duration *

5 seconds

Note:1. After creating a task, you will be charged for related fees. For more information, see [Billing Guide](#) 🔗

2. To use the media processing service, you need to make sure that the resource is available, and the access restriction features such as original image protection and hotlink protection are not enabled.

3. Audio/Video Segmentation takes effect only for objects uploaded to the bucket after the workflow is enabled.

OK Cancel

Note: The audio/video information node can determine the aspect ratio, duration, and other information of the input file as the execution precondition of the next node.

7. After confirming that the configuration is correct, click **Save**.

Workflows are disabled by default. To enable a workflow, click the toggle in the **Enable** column. Once enabled, the workflow will take effect in five minutes. Then, it will automatically perform media processing operations on video files uploaded subsequently. After processing files, it will output the new generated files to the specified file path.

Managing workflow

You can view the list of created workflows on the workflow management page.

The workflow list displays the names, IDs, input paths, creation times, and statuses of workflows. You can search for workflows by name and ID to view, edit, or delete specified workflows.

Enable: Once a workflow is enabled, video files uploaded to the specified path in the input bucket will be automatically processed according to the workflow configuration. You can click the toggle again to pause the workflow.

Note:

Workflows are disabled by default. To enable a workflow, click the toggle in the **Enable** column. Once enabled, the workflow will take effect in 5 minutes.

Details: You can view the configuration details of the current workflow.

View Execution Instance: You can view the workflow execution status and time by time.

More:

Click **More > Edit** in the **Operation** column to enter the **Edit Workflow** page, where you can modify the workflow configuration.

Click **More > Delete** in the **Operation** column to delete the workflow.

Note:

You cannot edit or delete an enabled workflow.

Viewing execution instance

An execution instance will be generated after a workflow is executed for each video file. The execution instance page displays the source file address, workflow execution status, and execution time.

1. Go to the workflow management page and click **View Execution Instance** in the **Operation** column of the target workflow to enter the execution instance list page.
2. On the list page, click **Details** in the **Operation** column of the target instance to enter the instance details page.
3. On the instance details page, you can view the job ID, execution status, start time, and end time of each workflow node.

Triggering workflow

After a workflow is created, it can be automatically triggered for files uploaded to the specified bucket or manually triggered for existing files in the bucket.

1. On the workflow management page, click **More > Create Execution Instance** of the target workflow.
2. On the **Create Execution Instance** page, select the file for which to trigger the workflow and click **Save** to immediately trigger and execute the workflow.

You can view the workflow execution status on the execution instance page.

Workflow Name *

Enter workflow name

Only a combination of letters, numbers, Chinese characters, underscores (_) and hyphens (-) with a length no greater than 128 characters is supported

Input Bucket Name

jaime-1258535724

Input Path ⓘ

If not filled in, it is valid for all paths under the bucket

Select

Format ⓘ

☒ Mainstream video/audio files ⓘ ☐ Image ⓘ ☐ Custom rule ⓘ ☐ All files ⓘ

Queue ⓘ *

Media processing queue (queue-1) ↻

Callback

☒ Use queue callback ☐ Custom

Queue Callback URL ⓘ

Empty [Edit](#)

Configure Workflow

Input

Audio/Video Transcoding

Video Frame Capturing

Converting Video to Animated Images

Intelligent Thumbnail

Audio/Video Splicing

Voice Separation

Highlights Generation

HLS Adaptive Multi-bitrate

SDRtoHDR

Video Enhancement

Audio/Video Segmentation

Custom Function

Image Processing

End

" to open the workflow

Save

Workflow Variable Description

Workflows support rendering destination file names and URLs with the following variables:

Variable Name	Description
InputName	Filename of the input file (without file extension)

InputNameAndExt	Filename of the input file (with file extension)
InputPath	File input path
RunId	Execution instance ID
Ext	Destination file format
Number	Destination file number

Sample

If the names of your input files are `test1.mp4` and `test2.mp4`, and you want to convert them to the FLV format (the final filenames will be `test1.flv` and `test2.flv`), then set the parameter format of the destination filename to `${InputName}.${Ext}`.

If the parameter format of the destination filename is set to `${InputNameAndExt}_${RunId}.${Ext}`:

When the workflow generates two instances (`000001` and `000002`) during execution, the final filenames will be `test1.mp4_000001.flv` and `test2.mp4_000002.flv`.

Configuring Job

Last updated : 2024-06-24 16:14:43

Overview

For files already in a bucket, you can create a job for media processing, speech recognition, file processing, and other operations. Currently, the following jobs are supported: **audio/video transcoding**, **top speed codec transcoding**, **broadcast media format transcoding**, **highlights generation (also known as video montage)**, **voice separation (also known as voice/sound separation)**, **audio/video splicing**, **video enhancement**, **audio/video segmentation**, **super resolution**, **SDR to HDR**, **video frame capturing**, **video-to-animated image conversion**, **intelligent thumbnail**, **digital watermark extraction**, **image processing**, **text to speech**, **speech recognition**, and **file preview**, some of which can be created by template. You can use the preset templates or customize templates. For more information, see [Template](#).

Note:

Currently, jobs can process 3GP, ASF, AVI, DV, FLV, F4V, M3U8, M4V, MKV, MOV, MP4, MPG, MPEG, MTS, OGG, RM, RMVB, SWF, VOB, WMV, WEBM, MP3, AAC, FLAC, AMR, M4A, WMA, and WAV files. When initiating a media processing request, you must enter the complete file name and extension; otherwise, the format cannot be recognized and processed.

Currently, the job feature can only manipulate **existing files**. To manipulate files during **upload**, use the workflow feature as described in [Configuring Workflow](#).

After a job is created, feature fees will be charged by CI. For billing details, see Media Processing Fees.

Viewing Job

On the job page, you can view all jobs in different types for the **specified time period**, click **Job Status** to filter and view jobs in different statuses, and search for jobs by job ID in the **search box**.

1. Log in to the [COS console](#).
2. Click **Bucket List** on the left sidebar.
3. Click the name of the bucket that you want to manipulate.
4. On the left sidebar, select **Data Processing Workflow** and click **Job** to enter the job management page.
5. Click **View** on the right of a job to view its information:

Job information: Job ID, job status, queue ID, template ID, job creation time, and job end time.

Input information: Source file bucket, region, and storage path.

Output information: Output file address, bucket, region, and storage path.

Note:

A job has six statuses: succeeded, failed, executing, pending, paused, and canceled.
You can query the records of jobs for the past month only.

Creating Audio/Video Transcoding Job

The audio/video transcoding feature converts an audio/video file bitstream. It changes parameters of the source bitstream, such as codec, resolution, and bitrate, to adapt to different devices and network conditions.

Directions

1. Log in to the [COS console](#).
2. Click **Bucket List** on the left sidebar.
3. Click the name of the bucket that you want to manipulate.
4. On the left sidebar, select **Data Processing Workflow** and click **Job** to enter the job management page.
5. Select the **Media Processing** tab, select **Transcoding > Audio/Video Transcoding** as the job type, click **Create Job**, and configure as follows:

Create Job

Please upload the file to preview in File Management in advance.[Upload in File Management](#)

Task Type

Media Processing

Audio/Video Transcoding

Source File URL ⓘ *

Select

Transcoding Type

☒ Regular

☐ Top Speed Codec Transcoding

☐ Broadcast Media Format Transcoding

Template Type

☒ System Template

☐ Custom Template

Template *

Please select a task template

Digital Watermark ⓘ

☐

Watermark

☐

Remove Watermark ⓘ

☐

Destination Bucket *

Select destination bucket

Supports only media processing-enabled buckets in the same region.

Destination Path ⓘ

If not specified, the output path remains the same

Select

Destination File Name *

example.mp4

m3u8 file names need no suffix

Queue ⓘ

Media Processing Queue (pfdc76470b5494022b29e1e1c4e1143bd)

Queue Callback URL ⓘ

Empty [Edit](#)

Note:1. After creating a task, you will be charged for related fees. For more information, see [Pricing](#)

2. Resources need to be available for task execution. Therefore, do not enable original image protection, hotlink protection, or other features that restrict access.

OK

Cancel

Source File URL: Enter the path of the source file, which cannot begin or end with `/` .

Transcoding Type: Select **Standard**.

Template Type: Select preset or custom template.

Template: Select the specified template.

Digital Watermark: Add a blind watermark as needed for copyright protection.

Watermark: Add a visible image or text watermark as needed.

Remove Watermark: Remove the watermark.

Destination Bucket: Select a bucket for which the media processing feature has been enabled in the current region.

Destination Path: Path of the output file.

Destination Filename: Name of the output file.

Queue: Currently, only the default queue `queue-1` is supported. For more information, see [Queues and Callbacks](#).

Queue Callback URL: Callback URL bound to the queue. You can configure it in the queue in [Common Configuration](#).

Creating Top Speed Codec Transcoding Job

The top speed codec technology improves the subjective image quality of a video at the minimum bitrate. Compared with standard transcoding, it makes videos smaller and clearer and delivers a better visual experience with low network resource usage.

Directions

1. Log in to the [COS console](#).
2. Click **Bucket List** on the left sidebar.
3. Click the name of the bucket that you want to manipulate.
4. On the left sidebar, select **Data Processing Workflow** and click **Job** to enter the job management page.
5. Select the **Media Processing** tab, select **Transcoding > Audio/Video Transcoding** as the job type, click **Create Job**, and configure as follows:

Source File URL: Enter the path of the source file, which cannot begin or end with `/` .

Transcoding Type: Select **Top Speed Codec Transcoding**.

Template: Select the specified template.

Digital Watermark: Add a blind watermark as needed for copyright protection.

Watermark: Add a visible image or text watermark as needed.

Destination Bucket: Select a bucket for which the media processing feature has been enabled in the current region.

Destination Path: Path of the output file.

Destination Filename: Name of the output file.

Queue: Currently, only the default queue `queue-1` is supported. For more information, see [Queues and Callbacks](#).

Queue Callback URL: Callback URL bound to the queue. You can configure it in the queue in [Common Configuration](#).

Creating Broadcast Media Format Transcoding

This feature produces videos in broadcast media formats such as Apple ProRes and Sony XAVC.

Directions

1. Log in to the [COS console](#).
2. Click **Bucket List** on the left sidebar.
3. Click the name of the bucket that you want to manipulate.
4. On the left sidebar, select **Data Processing Workflow** and click **Job** to enter the job management page.
5. Select the **Media Processing** tab, select **Transcoding > Audio/Video Transcoding** as the job type, click **Create Job**, and configure as follows:

Source File URL: Enter the path of the source file, which cannot begin or end with `/`.

Transcoding Type: Select **Broadcast Media Format**.

Template: Select the specified template.

Digital Watermark: Add a blind watermark as needed for copyright protection.

Watermark: Add a visible image or text watermark as needed.

Destination Bucket: Select a bucket for which the media processing feature has been enabled in the current region.

Destination Path: Path of the output file.

Destination Filename: Name of the output file.

Queue: Currently, only the default queue `queue-1` is supported. For more information, see [Queues and Callbacks](#).

Queue Callback URL: Callback URL bound to the queue. You can configure it in the queue in [Common Configuration](#).

Creating Highlights Generation Job

The highlights generation feature accurately extracts highlight segments from a video and outputs them as a new file for use in different scenarios subsequently, such as replay and preview.

Directions

1. Log in to the [COS console](#).
2. Click **Bucket List** on the left sidebar.
3. Click the name of the bucket that you want to manipulate.
4. On the left sidebar, select **Data Processing Workflow** and click **Job** to enter the job management page.

5. Select the **Media Processing** tab, select **Smart Editing > Highlights Generation** as the job type, click **Create Job**, and configure as follows:

Create Job ✕

Please upload the file to preview in File Management in advance.[Upload in File Management](#)

Task Type

Media Processing ▼

Highlights Generation ▼

Source File URL ⓘ *

Select

Template *

Please select a task template ▼

↻

For more templates, go to [Create Template](#)

Destination Bucket *

Select destination bucket ▼

↻

Supports only media processing-enabled buckets in the same region.

Destination Path ⓘ

If not specified, the output path remains the same

Select

Destination File Name *

Queue ⓘ

Media Processing Queue (pfdc76470b5494022b29e1e1c4e1143bd)

Queue Callback URL ⓘ

Empty [Edit](#)

Note:1. After creating a task, you will be charged for related fees. For more information, see [Pricing](#) [🔗](#)

2. Resources need to be available for task execution. Therefore, do not enable original image protection, hotlink protection, or other features that restrict access.

OK

Cancel

Source File URL: Enter the path of the source file, which cannot begin or end with `/` or `.`

Template: Select the specified template.

Destination Bucket: Select a bucket for which the media processing feature has been enabled in the current region.

Destination Path: Path of the output file.

Destination Filename: Name of the output file.

Queue: Currently, only the default queue `queue-1` is supported. For more information, see [Queues and Callbacks](#).

Queue Callback URL: Callback URL bound to the queue. You can configure it in the queue in [Common Configuration](#).

Creating Voice Separation Job

The voice separation feature separates the voice from the background sound in a video material to generate a new independent audio file. Then, you can apply artistic processing of other styles to the material without accompaniment and noise.

Directions

1. Log in to the [COS console](#).
2. Click **Bucket List** on the left sidebar.
3. Click the name of the bucket that you want to manipulate.
4. On the left sidebar, select **Data Processing Workflow** and click **Job** to enter the job management page.
5. Select the **Media Processing** tab, select **Smart Editing > Voice Separation** as the job type, click **Create Job**, and configure as follows:

Create Job ✕

Please upload the file to preview in File Management in advance.[Upload in File Management](#)

Task Type

Media Processing ▼ Voice Separation ▼

Source File URL ⓘ *

Select

Template *

Please select a task template ▼ ↺

For more templates, go to [Create Template](#)

Destination Bucket *

Select destination bucket ▼ ↺

Supports only media processing-enabled buckets in the same region.

Destination Path ⓘ

If not specified, the output path remains the same

Select

Voice Filename *

Background Sound Filename *

Queue ⓘ

Media Processing Queue (pfdc76470b5494022b29e1e1c4e1143bd)

Queue Callback URL ⓘ

Empty [Edit](#)

Note:1. After creating a task, you will be charged for related fees. For more information, see [Pricing](#) 🔗

2. Resources need to be available for task execution. Therefore, do not enable original image protection, hotlink protection, or other features that restrict access.

OK

Cancel

Source File URL: Enter the path of the source file, which cannot begin or end with `/` .

Template: Select the specified template.

Destination Bucket: Select a bucket for which the media processing feature has been enabled in the current region.

Destination Path: Path of the output file.

Voice Filename: Name of the output voice file.

Background Sound Filename: Name of the output background sound file.

Queue: Currently, only the default queue `queue-1` is supported. For more information, see [Queues and Callbacks](#).

Queue Callback URL: Callback URL bound to the queue. You can configure it in the queue in [Common Configuration](#).

Creating Text-to-Speech Job

The text to speech feature can convert text into natural-sounding and smooth speeches for use in smart customer service and audiobook scenarios.

Directions

1. Log in to the [COS console](#).
2. Click **Bucket List** on the left sidebar.
3. Click the name of the bucket that you want to manipulate.
4. On the left sidebar, select **Data Processing Workflow** and click **Job** to enter the job management page.
5. Select the **Media Processing** tab, select **Smart Editing > Text to Speech** as the job type, click **Create Job**, and configure as follows:

Source File URL: Enter the path of the source file, which cannot begin or end with `/`.

Template: Select the specified template.

Destination Bucket: Select a bucket for which the media processing feature has been enabled in the current region.

Destination Path: Path of the output file.

Destination Filename: Name of the output audio file.

Queue: Currently, only the default queue `queue-1` is supported. For more information, see [Queues and Callbacks](#).

Queue Callback URL: Callback URL bound to the queue. You can configure it in the queue in [Common Configuration](#).

Creating Audio/Video Splicing Job

The video/audio splicing feature adds the specified video/audio segment at the beginning or end of a video/audio file to generate a new one.

Directions

1. Log in to the [COS console](#).
2. Click **Bucket List** on the left sidebar.
3. Click the name of the bucket that you want to manipulate.
4. On the left sidebar, select **Data Processing Workflow** and click **Job** to enter the job management page.

5. Select the **Media Processing** tab, select **Transcoding > Audio/Video Splicing** as the job type, click **Create Job**, and configure as follows:

Create Job

×

Please upload the file to preview in File Management in advance.[Upload in File Management](#)

Task Type

Media Processing

Audio/Video Splicing

Splicing File Path 1 *

Select

+

Template *

Please select a task template

↻

For more templates, go to [Create Template](#)

Destination Bucket *

Select destination bucket

↻

Supports only media processing-enabled buckets in the same region.

Destination Path ⓘ

If not specified, the output path remains the same

Select

Destination File Name *

example.mp4

Queue ⓘ

Media Processing Queue (pfdc76470b5494022b29e1e1c4e1143bd)

Queue Callback URL ⓘ

Empty

Edit

Note:1. After creating a task, you will be charged for related fees. For more information, see [Pricing](#)

2. Resources need to be available for task execution. Therefore, do not enable original image protection, hotlink protection, or other features that restrict access.

OK

Cancel

Source File URL: Enter the path of the source file, which cannot begin or end with `/`.

Template: Select a created audio/video splicing template.

Destination Bucket: Select a bucket for which the media processing feature has been enabled in the current region.

Destination Path: Storage path of the output file.

Destination Filename: Name of the output file.

Queue: Currently, only the default queue `queue-1` is supported. For more information, see [Queues and Callbacks](#).

Queue Callback URL: Callback URL bound to the queue. You can configure it in the queue in [Common Configuration](#).

Creating Audio/Video Segmentation Job

The audio/video segmentation feature splits the specified audio/video file into several segments and outputs them in the specified container format.

Directions

1. Log in to the [COS console](#).
2. Click **Bucket List** on the left sidebar.
3. Click the name of the bucket that you want to manipulate.
4. On the left sidebar, select **Data Processing Workflow** and click **Job** to enter the job management page.
5. Select the **Media Processing** tab, select **Transcoding > Audio/Video Segmentation** as the job type, click **Create Job**, and configure as follows:

Source File URL: Enter the path of the source file, which cannot begin or end with `/` .

Container Format: Select the container format for the output segment.

Segment Duration: Specify the duration of the output segment.

Destination Bucket: Select a bucket for which the media processing feature has been enabled in the current region.

Destination Path: Storage path of the output file.

Destination Filename: Name of the output file.

Queue: Currently, only the default queue `queue-1` is supported. For more information, see [Queues and Callbacks](#).

Queue Callback URL: Callback URL bound to the queue. You can configure it in the queue in [Common Configuration](#).

Creating Video Frame Capturing Job

Video frame capturing is a screenshot feature provided by CI to capture the frames of a video at specified time points. After the job is enabled in the console, the output screenshots are in JPG format by default. If you enable captured frame compression, screenshots can be output in HEIF or TPG format.

Note:

A video frame capturing job can be created by template. You can customize the frame capturing start time, frame capturing interval, captured frames, output image size, and output format (captured frame compression needs to be enabled for this option) in a custom video frame capturing template.

Directions

1. Log in to the [COS console](#).
2. Click **Bucket List** on the left sidebar.
3. Click the name of the bucket that you want to manipulate.
4. On the left sidebar, select **Data Processing Workflow** and click **Job** to enter the job management page.
5. Select the **Media Processing** tab, select **Transcoding > Video Frame Capturing** as the job type, click **Create Job**, and configure as follows:

Create Job

Please upload the file to preview in File Management in advance.[Upload in File Management](#)

Task Type

Media Processing

Video Frame Capturing

Source File URL ⓘ *

Select

Template Type

☒ System Template

☐ Custom Template

Template *

Please select a task template

Output

JPG

Destination Bucket *

Select destination bucket

Supports only media processing-enabled buckets in the same region.

Destination Path ⓘ

If not specified, the output path remains the same.

Select

Destination File Name *

example\${Number}.jpg

The destination file name must include \${Number} as screenshot number. Take "test-\${Number}.jpg" as an example. If two screenshots are taken, their actual destination file names will be "test-0.jpg" and "test-1.jpg".

Queue ⓘ

Loading...

Note:1. After creating a task, you will be charged for related fees. For more information, see [Pricing](#).

2. Resources need to be available for task execution. Therefore, do not enable original image protection, hotlink protection, or other features that restrict access.

OK

Cancel

Source File URL: Enter the path of the source file, which cannot begin or end with `/`.

Template Type: You can select preset or custom template. For more information, see [Template](#).

Template: Select the specified template.

Output: If the video frame capturing job is enabled in the console, screenshots in JPG format will be output by default. If captured frame compression is enabled in the template, screenshots in HEIF or TPG format can be output. If you

use the video frame capturing API, you can choose to output JPG or PNG screenshots. For more information, see [Getting Media File Screenshot](#).

Destination Bucket: Select a bucket for which the media processing feature has been enabled in the current region.

Destination Path: Storage path of the video screenshots.

Destination Filename: Name of the output file. Note that as more than one files are output by **smart video frame capturing**, the output filename must contain the `${Number}` parameter as the sequence number of the screenshot.

For example, if the destination file path is set to `test-${Number}.jpg` and the job captures two screenshots, the actual names of the output files will be `test-0.jpg` and `test-1.jpg`.

Queue: Currently, only the default queue `queue-1` is supported. For more information, see [Queues and Callbacks](#).

Queue Callback URL: Callback URL bound to the queue. You can configure it in the queue in [Common Configuration](#).

Creating Video Enhancement Job

Video enhancement is a video image quality improvement feature provided by CI. You can use it to enhance and beautify image colors and improve the image details.

Note:

A video enhancement job can be created by template. You can customize the color and detail enhancement settings in a custom video enhancement template.

Directions

1. Log in to the [COS console](#).
2. Click **Bucket List** on the left sidebar.
3. Click the name of the bucket that you want to manipulate.
4. On the left sidebar, select **Data Processing Workflow** and click **Job** to enter the job management page.
5. Select the **Media Processing** tab, select **Image Quality Optimization > Video Enhancement** as the job type, click **Create Job**, and configure as follows:

Create Job

×

Please upload the file to preview in File Management in advance.[Upload in File Management](#)

Task Type

Media Processing Video Enhancement

Source File URL ⓘ *

Select

Enhancement Template ⓘ *

Please selectEnhancement Template ↕

For more templates, go to [Create Template](#)

Transcoding Template type

☒ System Template
 ☐ Custom Template

Transcoding Template ⓘ *

Please selectTranscoding Template ↕

Digital Watermark ⓘ

☐

Watermark

☐

Destination Bucket *

Select destination bucket ↕

Supports only media processing-enabled buckets in the same region.

Destination Path ⓘ

If not specified, the output path remains the same

Select

Destination File Name *

example.mp4

m3u8 file names need no suffix

Queue ⓘ

Media Processing Queue (pfdc76470b5494022b29e1e1c4e1143bd)

Queue Callback URL ⓘ

Empty [Edit](#)

Note:1. After creating a task, you will be charged for related fees. For more information, see [Pricing](#) [🔗](#)

2. Resources need to be available for task execution. Therefore, do not enable original image protection, hotlink protection, or other features that restrict access.

OK

Cancel

Note:

The input video must be shorter than 30 minutes.

Source File URL: Enter the path of the source file, which cannot begin or end with `/`.

Enhancement Template: Select a video enhancement template as needed.

Transcoding Template Type: You can select preset or custom template. For more information, see [Template](#).

Transcoding Template: You can select a transcoding template and specify parameters such as resolution, bitrate, and format of the output file.

Digital Watermark: Add a blind watermark as needed for copyright protection.

Watermark: Add a visible image or text watermark as needed.

Destination Bucket: Select a bucket for which the media processing feature has been enabled in the current region.

Destination Path: Path of the output video.

Destination Filename: Name of the output file.

Queue: Currently, only the default queue `queue-1` is supported. For more information, see [Queues and Callbacks](#).

Queue Callback URL: Callback URL bound to the queue. You can configure it in the queue in [Common Configuration](#).

Creating Super Resolution Job

The super resolution feature reconstructs the details and local features of a video by recognizing its content and contour so as to generate a high-resolution video image through a series of low-resolution video images. It can be used in combination with video enhancement to remaster old videos.

Directions

1. Log in to the [COS console](#).
2. Click **Bucket List** on the left sidebar.
3. Click the name of the bucket that you want to manipulate.
4. On the left sidebar, select **Data Processing Workflow** and click **Job** to enter the job management page.
5. Select the **Media Processing** tab, select **Image Quality Optimization > Super Resolution** as the job type, click **Create Job**, and configure as follows:

Source File URL: Enter the path of the source file, which cannot begin or end with `/`.

Super Resolution Template: Select the destination resolution template as needed.

Transcoding Template Type: You can select preset or custom template. For more information, see [Template](#).

Transcoding Template: You can select a transcoding template and specify parameters such as bitrate and format of the output file.

Digital Watermark: Add a blind watermark as needed for copyright protection.

Watermark: Add a visible image or text watermark as needed.

Destination Bucket: Select a bucket for which the media processing feature has been enabled in the current region.

Destination Path: Path of the output video.

Destination Filename: Name of the output file.

Queue: Currently, only the default queue `queue-1` is supported. For more information, see [Queues and Callbacks](#).

Queue Callback URL: Callback URL bound to the queue. You can configure it in the queue in [Common Configuration](#).

Creating SDR-to-HDR Job

SDR to HDR is a video dynamic range conversion feature provided by CI. You can use it to convert a standard dynamic range (SDR) video to a high dynamic range (HDR) video.

Directions

1. Log in to the [COS console](#).
2. Click **Bucket List** on the left sidebar.
3. Click the name of the bucket that you want to manipulate.
4. On the left sidebar, select **Data Processing Workflow** and click **Job** to enter the job management page.
5. Select the **Media Processing** tab, select **Image Quality Optimization > SDR to HDR** as the job type, click **Create Job**, and configure as follows:

Create Job

×

Please upload the file to preview in File Management in advance.[Upload in File Management](#)

Task Type

Media Processing

SDRtoHDR

Source File URL ⓘ *

Select

HDR Standard

☒ HLG ☐ HDR10

Transcoding Template ⓘ *

Select H.265Transcoding Template

↻

Supports only H.265 transcoding templates.[Create Template](#)

Watermark

☐

Destination Bucket *

Select destination bucket

↻

Supports only media processing-enabled buckets in the same region.

Destination Path ⓘ

If not specified, the output path remains the same

Select

Destination File Name *

example.mp4

m3u8 file names need no suffix

Queue ⓘ

Media Processing Queue (pfdc76470b5494022b29e1e1c4e1143bd)

Queue Callback URL ⓘ

Empty [Edit](#)

Note:1. After creating a task, you will be charged for related fees. For more information, see [Pricing](#)

2. Resources need to be available for task execution. Therefore, do not enable original image protection, hotlink protection, or other features that restrict access.

OK

Cancel

Note:

The input video must be shorter than 30 minutes.

Source File URL: Enter the path of the source file, which cannot begin or end with `/`.

HDR Standard: Select HLG or HDR10.

Transcoding Template: Select an H.265 transcoding template. If there are no templates, create an audio/video transcoding template and select H.265 as the encoding format. For more information on how to create a template and configure parameters, see [Custom Template](#).

Watermark: Add a visible image or text watermark as needed.

Destination Bucket: Select a bucket for which the media processing feature has been enabled in the current region.

Destination Path: Storage path of the destination file after the SDR-to-HDR conversion is completed.

Destination Filename: Name of the output file.

Queue: Currently, only the default queue `queue-1` is supported. For more information, see [Queues and Callbacks](#).

Queue Callback URL: Callback URL bound to the queue. You can configure it in the queue in [Common Configuration](#).

Creating Video-to-Animated Image Conversion Job

You can use the video-to-animated image conversion feature to convert a video to animated images.

Note:

A video-to-animated image conversion job can be created by template. You can customize the transcoding start time, transcoding duration, frame extraction method, output animated image frame rate, and output animated image size in a custom video to animated image conversion template.

Directions

1. Log in to the [COS console](#).
2. Click **Bucket List** on the left sidebar.
3. Click the name of the bucket that you want to manipulate.
4. On the left sidebar, select **Data Processing Workflow** and click **Job** to enter the job management page.
5. Select the **Media Processing** tab, select **Transcoding > Video-to-Animated Image Conversion** as the job type, click **Create Job**, and configure as follows:

Create Job

×

Please upload the file to preview in File Management in advance.[Upload in File Management](#)

Task Type

Media Processing

Converting Video to Animated Images

Source File URL ⓘ *

Select

Template Type

☒ System Template ☐ Custom Template

Template *

Please select a task template

↻

Destination Bucket *

Select destination bucket

↻

Supports only media processing-enabled buckets in the same region.

Destination Path ⓘ

If not specified, the output path remains the same

Select

Destination File Name *

example.gif

Queue ⓘ

Media Processing Queue (pfdc76470b5494022b29e1e1c4e1143bd)

Queue Callback URL ⓘ

Empty [Edit](#)

Note:1. After creating a task, you will be charged for related fees. For more information, see [Pricing](#) ↗

2. Resources need to be available for task execution. Therefore, do not enable original image protection, hotlink protection, or other features that restrict access.

OK

Cancel

Source File URL: Enter the path of the source file, which cannot begin or end with `/` .

Template Type: You can select preset or custom template. For more information, see [Template](#).

Template: Select the specified template.

Destination Bucket: Select a bucket for which the media processing feature has been enabled in the current region.

Destination Path: Storage path of the animated images.

Destination Filename: Name of the output file.

Queue: Currently, only the default queue `queue-1` is supported. For more information, see [Queues and Callbacks](#).

Queue Callback URL: Callback URL bound to the queue. You can configure it in the queue in [Common Configuration](#).

Creating Intelligent Thumbnail Job

The intelligent thumbnail feature intelligently analyzes the quality, brilliance, and content relevance of video frames by understanding the video content with Tencent Media Lab's advanced AI technologies. Then, it extracts optimal frames to generate thumbnails to make the content more engaging.

Note:

The intelligent thumbnail feature is a paid service and billed by the original video duration. For billing details, see [Media Processing Fees](#).

Three optimal keyframes will be output through smart analysis of each video file.

Directions

1. Log in to the [COS console](#).
2. Click **Bucket List** on the left sidebar.
3. Click the name of the bucket that you want to manipulate.
4. On the left sidebar, select **Data Processing Workflow** and click **Job** to enter the job management page.
5. Select the **Media Processing** tab, select **Smart Editing > Intelligent Thumbnail** as the job type, click **Create Job**, and configure as follows:

Create Job

×

Please upload the file to preview in File Management in advance.[Upload in File Management](#)

Task Type

Media Processing

Intelligent Thumbnail

Source File URL ⓘ *

Select

Destination Bucket *

Select destination bucket

↻

Supports only media processing-enabled buckets in the same region.

Destination Path ⓘ

If not specified, the output path remains the same

Select

Destination File Name *

example\${Number}.jpg

The destination file name must include \${Number} as cover number. Take "test-\${Number}.jpg" as an example, and the actual destination file names will be "test-0.jpg" and "test-1.jpg".

Queue ⓘ

Media Processing Queue (pfdc76470b5494022b29e1e1c4e1143bd)

Queue Callback URL ⓘ

Empty

Edit

Note:1. After creating a task, you will be charged for related fees. For more information, see [Pricing](#).

2. Resources need to be available for task execution. Therefore, do not enable original image protection, hotlink protection, or other features that restrict access.

OK

Cancel

Source File URL: Enter the path of the source file, which cannot begin or end with `/`.

Destination Bucket: Select a bucket for which the media processing feature has been enabled in the current region.

Destination Path: Storage path of the smart thumbnails.

Destination Filename: Name of the output file.

Note:

As more than one files are output by **intelligent thumbnail**, the output filename must contain the parameter `${Number}` as the thumbnail serial number. For example, if the output file path is set to `test-${Number}.jpg`, the actual names of the output files will be `test-0.jpg` and `test-1.jpg`.

Queue: Currently, only the default queue `queue-1` is supported. For more information, see [Queues and Callbacks](#).

Queue Callback URL: Callback URL bound to the queue. You can configure it in the queue in [Common Configuration](#).

Creating Digital Watermark Extraction Job

You can use the media processing service to extract the digital watermark from a watermarked video.

Directions

1. Log in to the [COS console](#).
2. Click **Bucket List** on the left sidebar.
3. Click the name of the bucket that you want to manipulate.
4. On the left sidebar, select **Data Processing Workflow** and click **Job** to enter the job management page.
5. Select the **Media Processing** tab, select **Copyright Protection > Digital Watermark Extraction** as the job type, click **Create Job**, and configure as follows:

Create Job ✕

Please upload the file to preview in File Management in advance.[Upload in File Management](#)

Task Type

Media Processing

Extract Digital Watermark

Submitting File ⓘ *

Select


Queue ⓘ

Media Processing Queue (pfdc76470b5494022b29e1e1c4e1143bd)

Queue Callback URL ⓘ

Empty

Edit

Note:1. After creating a task, you will be charged for related fees. For more information, see [Pricing](#) 

2. Resources need to be available for task execution. Therefore, do not enable original image protection, hotlink protection, or other features that restrict access.

OK

Cancel

Source File: Enter the path of the source file, which must begin with but cannot end with `/`. Different folders are separated with `/`.

Queue: Currently, only the default queue `queue-1` is supported. For more information, see [Queue](#).

Creating Speech Recognition Job

The speech recognition feature recognizes a recording file and asynchronously returns the recognized text. It can be used for call center speech quality inspection, video subtitles generation, and meeting recording transcription.

Directions

1. Log in to the [COS console](#).
2. Click **Bucket List** on the left sidebar.
3. Click the name of the bucket that you want to manipulate.
4. On the left sidebar, select **Data Processing Workflow** and click **Job** to enter the job management page.
5. Select the **Speech Recognition** tab, click **Create Job**, and configure as follows:

Source File URL: Enter the path of the source file, which cannot begin or end with `/` .

Recognition Engine: Select a speech recognition engine. Different engines are as described below:

8k_zh: Applies to telephone recording, 8 kHz audio sample rate, Mandarin.

8k_zh_s: Applies to telephone recording, 8 kHz audio sample rate, Mandarin; supports audio separation by speaker.

16k_zh: Applies to audio/video live streaming and video conferences, 16 kHz audio sample rate, Mandarin.

16k_zh_video: Applies to audio/video live streaming, 16 kHz audio sample rate, Mandarin.

16k_en: Applies to English audio, 16 kHz audio sample rate.

16k_ca: Applies to Cantonese audio, 16 kHz audio sample rate.

Sound Channels: Select mono-channel or dual-channel.

Recognition Result: Speech recognition result text output by sentence or word (only supported for the Chinese speech recognition engines at 16 kHz audio sample rate).

Destination Bucket: Select a bucket for which the media processing feature has been enabled in the current region.

Destination Path: Storage path of the recognized text.

Destination Filename: Name of the output file.

Filter Restricted Words: Select whether to filter restricted words or replace them with `*` .

Filter Modal: Select whether to filter modal.

Smart Speech Conversion: After it is enabled, recognized Chinese numbers will be converted to Arabic numbers.

Queue: Currently, only the default speech recognition queue `queue-speech-1` is supported. For more information, see [Queues and Callbacks](#).

Queue Callback URL: Callback URL bound to the queue. You can configure it in the queue in [Common Configuration](#).

Creating File Preview Job

The file preview feature allows you to preview files of nearly 30 types online through image or HTML, with the source file style preserved as much as possible. This addresses the lack of support for certain file formats on different devices

and enables easy online file preview on PC, app, and other terminals.

Directions

1. Log in to the [COS console](#).
2. Click **Bucket List** on the left sidebar.
3. Click the name of the bucket that you want to manipulate.
4. On the left sidebar, select **Data Processing Workflow** and click **Job** to enter the job management page.
5. Select the **File Preview** tab, click **Create Job**, and configure as follows:

Source File URL: It cannot begin or end with `/` ; for example, `doc/example.doc` .

Preview Setting: Select to preview whole document or specified page. A job supports up to 5,000 pages. If more pages are input, only the first 5,000 pages can be converted.

Output Format: Currently, JPG and PNG formats are supported for output images. The PDF format is supported only for whole document preview.

Destination Bucket: Select a bucket for which the file preview feature has been enabled in the current region.

Destination Path: It is optional. If it is not set, it will be the same as the input file path.

Destination Filename: The file preview service converts each page of the original file into an image. Therefore, you need to add a placeholder (`${Number}` or `${Page}`) to the output filename to number the output images. The output numbers are the same as the file page numbers. For example, if you want to preview a file with three pages and set the output filename to `output${Number}.jpg` , then three images `output1.jpg` , `output2.jpg` , `output3.jpg` will be output.

Queue: Currently, only the default file preview queue `queue-doc-process-1` is supported. For more information, see [Queues and Callbacks](#).

Queue Callback URL: Callback URL bound to the queue. You can configure it in the queue in [Common Configuration](#).

Creating Image Processing Job

The image processing feature supports flexible image editing, such as rotation, cropping, transcoding, and scaling. It provides multiple image downsizing solutions like Guetzli compression, TPG transcoding, and HEIF transcoding, as well as diversified copyright protection solutions like image/text/blind watermarking. This meets your image processing needs in different business scenarios.

Directions

1. Log in to the [COS console](#).
2. Click **Bucket List** on the left sidebar.
3. Click the name of the bucket that you want to manipulate.
4. On the left sidebar, select **Data Processing Workflow** and click **Job** to enter the job management page.

5. Select the **Image Processing** tab, click **Create Job**, and configure as follows:

Input Bucket Name: It is the current bucket by default.

File Path: Enter the path of the source file, which must begin with but cannot end with `/`. Different folders are separated with `/`.

Template: Select the specified template.

Destination Bucket: Select a bucket for which the media processing feature has been enabled in the current region.

Destination Path: Storage path of the image processing result.

Destination Filename: Name of the output file.

Queue: Currently, only the default queue `queue-1` is supported. For more information, see [Queues and Callbacks](#).

Queue Callback URL: Callback URL bound to the queue. You can configure it in the queue in [Common Configuration](#).

Template

Last updated : 2024-06-24 16:14:43

Overview

When using the data processing workflow feature, you usually need to set a series of parameters, which can be combined through a template. This **simplifies your operations** and allows you to reuse the configured parameters with no need to enter them repeatedly.

For media processing features such as audio/video transcoding, audio/video splicing, video frame capturing, and video to animated image conversion, you need to specify a template when creating a job or workflow. The template page provides **system templates**, and you can also **customize templates** based on your business needs.

System Templates

The system combines common parameters in advance into system templates, so that you can use them directly. When creating a job or workflow, you can select such a template by the template name.

1. Log in to the [COS console](#).
2. Click **Bucket List** on the left sidebar.
3. Click the name of the bucket that you want to operate.
4. On the left sidebar, select **Data Processing Workflow > Template Configuration** to view templates of different processing types.

jaime-1258535724

Template

Queues and Callbacks

To use a workflow or task, you need to set the processing parameters. A template simplifies operations. You can use the preset template provided by CI or customize one.[Learn More](#)

Media Processing

Audio/Video Transcoding

Top Speed Codec Transcoding

Super-Resolution

Highlights Generation

Video Enhancement

Video Frame Capturing

Converting Video to Animated Images

Video Watermark

Audio/Video Splicing

Voice Separation

Broadcast Media Format Transcoding

Create Transcoding Template

System Preset Template

Template Name

Please enter search content

Template ID/Name	Encapsulation Format	Video Encoding Format	Resolution	Video Bitrate	Operation
t03e862f296fba4152a1dd186b4ad5f64b HLS-265-2K	HLS	H.265	2048 * Proportional height	4800 Kbps	Detail
t09f9da59ed3c44ecd8ea1778e5ce5669c HLS-265-FHD	HLS	H.265	1920 * Proportional height	3500 Kbps	Detail
t02ef37d96448848c7bc3c3baeb983ccb7 HLS-265-HD	HLS	H.265	1280 * Proportional height	2000 Kbps	Detail
t09e77dcad7b2a4ae18e886b937983f8f8 HLS-265-SD	HLS	H.265	720 * Proportional height	1024 Kbps	Detail
t0a28e166c1e6f43c4b61a55603f38390c HLS-265-FLU	HLS	H.265	640 * Proportional height	512 Kbps	Detail
t02ef141e964d74988a8c16191efc26c44 MP4-265-2K	MP4	H.265	2048 * Proportional height	4800 Kbps	Detail

Click **View** in the **Operation** column to view template details.

Note:

Currently, the system provides 15 **audio/video transcoding**, 3 **video frame capturing**, and 18 **video to animated image conversion** templates.

You can view the information of system templates but cannot edit or delete them.

System templates for audio/video transcoding

Template ID	Template Name	Container Format	Video Encoding Format	Resolution	Video Bitrate
t0e2b9f4cd25184c6ab73d0c85a6ee9cb5	H264-MP4-LD-360P	MP4	H.264	640 * proportionally scaled	512 Kbps
t0876739cd865042d1957d73c78f0484fb	H264-MP4-SD-480P	MP4	H.264	720 * proportionally scaled	1024 Kbps
t0852e7ff4acd4484e99ba104f3840d3cb	H264-MP4-HD-720P	MP4	H.264	1280 * proportionally scaled	2000 Kbps
t04df9eb0c373c4a8780ec894ce05469a7	H264-MP4-FHD-1080P	MP4	H.264	1920 * proportionally scaled	3500 Kbps
t09d027135634d47048e5a30dc1e19ee90	H264-MP4-2K	MP4	H.264	2048 * proportionally scaled	4800 Kbps
t0e634622e8dfb49339ba478d60ddc7188	H264-HLS-LD-360P	M3U8	H.264	640 * proportionally scaled	512 Kbps
t0fa5bdfb58bb348e88bf73fae5d674fdf	H264-HLS-SD-480P	M3U8	H.264	720 * proportionally scaled	1024 Kbps
t09d0f419921e44ed98190f355ec9fd629	H264-HLS-HD-720P	M3U8	H.264	1280 * proportionally scaled	2000 Kbps

t080ae8a06f9074f3daa46201078f8d4b1	H264-HLS-FHD-1080P	M3U8	H.264	1920 * proportionally scaled	3500 Kbps
t0ab68939cef0f40d19c4a135df540239f	H264-HLS-2K	M3U8	H.264	2048 * proportionally scaled	4800 Kbps
t0e165bef65ed24d568eeecc8661248af6	H264-FLV-LD-360P	M3U8	H.264	640 * proportionally scaled	512 Kbps
t057d0410c32444e48b9220f9571e6097a	H264-FLV-SD-480P	M3U8	H.264	720 * proportionally scaled	1024 Kbps
t00daf332ba39049f8bfb899c1ed0134b0	H264-FLV-HD-720P	M3U8	H.264	1280 * proportionally scaled	2000 Kbps
t0d41905a814434c8a81897ecb54d53a32	H264-FLV-FHD-1080P	M3U8	H.264	1920 * proportionally scaled	3500 Kbps
t0e287e59454b94a8983ba78a6a30ee864	H264-FLV-2K	M3U8	H.264	2048 * proportionally scaled	4800 Kbps

System templates for video frame capturing

Template ID	Template Name	Frame Capturing Start Time	Frame Capturing Interval	Max Frame Count Per Video	Output Image Size
t01d40e440761448fc8c538fb8d5a5b81e	snapshot_320 * 180_1	0s	2s	5	320 * 180 px
t0a60a2bc71a4b40c7b3d7f7e8a2779a81	snapshot_640 * 360_2	0s	10s	5	640 * 360 px
t07740e32081b44ad7a0aea03adcfd54a	snapshot_1280 * 720_3	0s	10s	5	1280 * 720 px

System templates for video to animated image conversion

Template ID	Template Name	Transcoding Start Time	Transcoding Duration	Frame Extraction Method	On Ar Ir Fr R
t04373959a69c04d47b62fd214dd13d8e9	gif_320 * 180_1	0s	600s	Only keyframes are extracted	Ac
t0341b0ab2b8a340ff826e9cb4f3a7baea	gif_320 * 180_2	0s	600s	One frame is extracted every 10s	Ac (0
t046b1d8e5bdf842c6a58d8028b48eafee	gif_320 * 180_3	0s	600s	Ten frames are extracted per second	Ac (1
t0ef2077f215864c018a2fca73614ceca6	gif_640 * 360_4	0s	600s	Only keyframes are extracted	Ac
t0d21406ca737a40869973a37a5daa349a	gif_640 * 360_5	0s	600s	One frame is extracted every 10s	Ac (0
t0878a9c9c1f054cb5bca68b8b06e556c2	gif_640 * 360_6	0s	600s	Ten frames are extracted per second	Ac (1
t0dae821708cea4ba5b3e271810ac80a21	gif_1280 * 720_7	0s	600s	Only keyframes are extracted	Ac

t03fef67ad94d2466b9c0c89252ed72e87	gif_1280 * 720_8	0s	600s	One frame is extracted every 10s	Ac (0
t030a64e9f9f5a4f53a9ef64bb7ce490b5	gif_1280 * 720_9	0s	600s	Ten frames are extracted per second	Ac (1
t03b0e9eca4fc34e2cba9da89d9c7c13a2	webp_320 * 180_1	0s	60s	Only keyframes are extracted	Ac
t016fcddf6bc3c44b793e9b7b07119b4ee	webp_320 * 180_2	0s	600s	One frame is extracted every 10s	Ac (0
t0bf1f1ce6d2404b258c0f81fbb9aaece1	webp_320 * 180_3	0s	600s	One frame is extracted every 10s	Ac (1
t098d6d3fcd2c45309a408594a42559f6	webp_640 * 360_4	0s	60s	Only keyframes are extracted	Ac
t0169a6a9c2eec4b51972eb63bafcbf08d	webp_640 * 360_5	0s	600s	One frame is extracted every 10s	Ac (0
t0ef9ba537011e4876b8777aebc19d10a5	webp_640 * 360_6	0s	600s	One frame is extracted every 10s	Ac (1
t02743d344b5e74c579e50e9e135b432b8	webp_1280 * 720_7	0s	60s	Only keyframes are extracted	Ac

t0dd27c136ff2741538bec96981e058868	webp_1280 * 720_8	0s	600s	One frame is extracted every 10s	Ac (0
t00ad05235d67a45a9a697b553052b7346	webp_1280 * 720_9	0s	600s	One frame is extracted every 10s	Ac (1

Custom Template

If system templates cannot meet your needs, use custom templates. Currently, you can create custom templates for **audio/video transcoding**, **top speed codec transcoding**, **highlights generation**, **video frame capturing**, **video to animated image conversion**, **video watermark**, **audio/video splicing**, **voice/sound separation**, **video enhancement**, **super-resolution**, **image processing**, and **broadcast media format transcoding**.

Audio/Video transcoding

The audio/video transcoding feature converts an audio/video file bitstream. It changes parameters of the source bitstream, such as codec, resolution, and bitrate, to adapt to different devices and network conditions. You can customize the template parameters in a custom audio/video transcoding template.

Directions

1. Log in to the [COS console](#).
2. Click **Bucket List** on the left sidebar.
3. Click the name of the bucket where you want to store the video.
4. On the left sidebar, select **Data Processing Workflow > Template Configuration** to enter the template configuration page.
5. Select **Media Processing > Audio/Video Transcoding** and click **Create Transcoding Template**.

Create Transcoding Template ✕

Template Name *

Up to 64 chars. Only supports Chinese characters, English letters, numbers, underscores (_), hyphens (-) and *

Transcoding Type

Video

Encapsulation Format *

MP4

Transcoding Duration

☒ Input file duration

☐ Custom configuration

Video Parameters

Delete Video Stream

☐

Encoding Format *

H.264

Bitrate *

☒ Custom bitrate

☐ CRF

Kbps

Please enter an integer between 100 and 50000

Resolution

☒ Source Video Resolution

☐ Custom

Video Frame Rate

☒ Source Video Frame Rate

☐ Custom

Encoding Level

High resolution device

More Settings

☐

Audio Parameters ▾

Delete Audio Stream

☐

Advanced Settings ▾

OK

Cancel

6. In the **Create Transcoding Template** window, configure the following items:

Template Name: It can contain up to 64 letters, digits, underscores (_), hyphens (-), and asterisks (*).

Transcoding Type: You can select video or audio transcoding.

Container Format: Video transcoding supports the MP4, FLV, HLS, TS, MKV, and WebM formats. Audio transcoding supports the MP3, AAC, AMR, FLAC, and WebM formats.

Encoding Format: H264, H265, AV1, VP8, and VP9 are supported.

Bitrate: Adaptive bitrate is supported, which can automatically analyze the video content to set the optimal bitrate.

Transcoding Duration: You can select the input file duration or customize the duration.

Audio/Video Parameters: You can customize audio/video parameters as needed.

7. Click **OK**.

After successfully creating the template, you can **view**, **edit**, or **delete** it in the custom template list.

Note:

You can use the template when creating an audio/video transcoding job as instructed in [Configuring Job](#) or creating a workflow as instructed in [Configuring Workflow](#).

TSC transcoding

The top speed codec transcoding feature improves the subjective image quality of a video at a low bitrate. Compared with regular audio/video transcoding, it outputs smaller files and clearer video images and delivers a better visual experience with guaranteed low network resource usage. You can customize parameters such as codec, resolution, and bitrate in a custom top speed codec transcoding template.

Directions

1. Log in to the [COS console](#).
2. Click **Bucket List** on the left sidebar.
3. Click the name of the bucket where you want to store the video.
4. On the left sidebar, select **Data Processing Workflow > Template Configuration** to enter the template configuration page.
5. Select **Top Speed Codec Transcoding** and click **Create Top Speed Codec Transcoding Template**.

6. In the **Create Broadcast Media Format Transcoding Template** window, configure the following items:

Template Name: It can contain up to 64 letters, digits, underscores (_), hyphens (-), and asterisks (*).

Transcoding Type: It is video transcoding by default.

Container Format: Supported formats include MP4 and HLS.

Transcoding Duration: You can select the input file duration or customize the duration.

Audio/Video Parameters: You can customize audio/video parameters as needed.

7. Click **OK**.

After successfully creating the template, you can **view**, **edit**, or **delete** it in the custom template list.

Note:

You can use the template when creating a broadcast media format transcoding job as instructed in [Configuring Job](#) or creating a workflow as instructed in [Configuring Workflow](#).

Broadcast media format transcoding

This feature processes special formats such as XAVC and ProRes.

Directions

1. Log in to the [COS console](#).
2. Click **Bucket List** on the left sidebar.
3. Click the name of the bucket where you want to store the video.
4. On the left sidebar, select **Data Processing Workflow > Template Configuration** to enter the template configuration page.
5. Select **Broadcast Media Format Transcoding** and click **Create Broadcast Media Format Transcoding Template**.
6. In the **Create Broadcast Media Format Transcoding Template** window, configure the following items:
Template Name: It can contain up to 64 letters, digits, underscores (_), hyphens (-), and asterisks (*).
Preset Encoder Configuration: Select the default values of encoder parameters such as sample rate.
Container Format: Supported formats include MXF.
Transcoding Duration: You can select the input file duration or customize the duration.
Audio/Video Parameters: You can customize audio/video parameters as needed.
7. Click **OK**.

After successfully creating the template, you can **view**, **edit**, or **delete** it in the custom template list.

Note:

You can use the template when creating a broadcast media format transcoding job as instructed in [Configuring Job](#) or creating a workflow as instructed in [Configuring Workflow](#).

Highlights generation

The highlights generation feature automatically extracts highlights from a video. You can use a custom template to set the highlights generation template name and specify the maximum duration, resolution, and format of the output highlight video.

Directions

1. Log in to the [COS console](#).
2. Click **Bucket List** on the left sidebar.
3. Click the name of the bucket where you want to store the video.
4. On the left sidebar, select **Data Processing Workflow > Template Configuration** to enter the template configuration page.
5. Select **Highlights Generation** and click **Create Highlights Generation Template**.
6. In the **Create Voice Separation Template** window, configure the following items:

Note:

Currently, highlights generation can be used only for landscape, food, street, and vlog scenarios and will support more scenarios in the future. If you want to customize this feature, [contact us](#) for assistance.

Template Name: It can contain up to 64 letters, digits, underscores (_), hyphens (-), and asterisks (*).

Container Format: Supported formats include MP4, FLV, HLS, TS, and MKV.

Highlight Video Duration: You can select the duration of the complete output highlight video after automatic analysis or customize the duration.

Audio/Video Parameters: You can customize audio/video parameters as needed.

7. Click **OK**.

After successfully creating the template, you can **view**, **edit**, or **delete** it in the custom template list.

Note:

You can use the template when creating a highlights generation job as instructed in [Configuring Job](#) or creating a workflow as instructed in [Configuring Workflow](#).

Video frame capturing

The video frame capturing feature captures the frames of a video at specified time points. The output screenshots are in JPG format by default. If you enable captured frame compression, screenshots can be output in HEIF or TPG format. You can customize the template name, frame capturing start time, frame capturing interval, captured frames, and output image size and format in a custom video frame capturing template.

Directions

1. Log in to the [COS console](#).
2. Click **Bucket List** on the left sidebar.
3. Click the name of the bucket where you want to store the video.
4. On the left sidebar, select **Data Processing Workflow > Template Configuration** to enter the template configuration page.
5. Select **Video Frame Capturing** and click **Create Video Frame Capturing Template**.

Create Frame Capturing Template

Template Name *

Enter a template name

Up to 64 chars. Only supports Chinese characters, English letters, numbers, underscores (_), hyphens (-) and *

Frame Capturing Start Time *

seconds

Frame Capturing Method *

☒ All frames will be captured

☐ Custom Frame Capture Interval

☐ Average Frame Capturing

☐ Capture Keyframes

Maximum Number of Frames *

Output Image Size

☒ Input Image Size

☐ Custom Image Size

Video Frame Compression

☐

Detect Starting Frames ⓘ

☐

OK

Cancel

6. In the **Create Video Frame Capturing Template** window, configure the following items:

Template Name: It can contain up to 64 letters, digits, underscores (_), hyphens (-), and asterisks (*).

Frame Capturing Start Time: You can select any time point within the full video length.

Frame Capturing Method:

All frames will be captured by default: Every video frame will be captured.

Custom Frame Capturing Interval: Frames will be captured at specified time intervals from the frame capturing start time to the end of the video.

Even Frame Capturing: Frames will be captured at even intervals calculated based on the specified **number of captured frames** from the frame capturing start time to the end of the video.

Capture Keyframes: Capture only keyframes.

Max Frame Count Per Video: This parameter is required if you select **All frames will be captured by default**, **Custom Frame Capturing Interval**, or **Capture Keyframes** as the frame capturing method.

Captured Frames: This parameter is required if you select **Even Frame Capturing** as the frame capturing method.

Frames will be captured at even intervals calculated based on the specified number of frames captured from the frame capturing start time to the end of the video.

Output Image Size: The default output screenshot size is the same as that of the original video image. If you select custom image size, you must enter an integer between 128 and 4096 for the width and height respectively.

Video Frame Compression: If it is enabled, captured images can be compressed.

7. Click **OK**.

After successfully creating the template, you can **view**, **edit**, or **delete** it in the custom template list.

Note:

You can use the template when creating a video frame capturing job as instructed in [Configuring Job](#) or creating a workflow as instructed in [Configuring Workflow](#).

Video-to-animated image conversion

The video to animated image conversion feature converts a video to animated images. You can customize the template name, transcoding start time, transcoding duration, frame extraction method, output animated image frame rate, and output animated image size in a custom video to animated image conversion template.

Directions

1. Log in to the [COS console](#).
2. Click **Bucket List** on the left sidebar.
3. Click the name of the bucket where you want to store the video.
4. On the left sidebar, select **Data Processing Workflow > Common Configuration**. Then, select the **Template** tab to go to the template configuration page.
5. Select **Video to Animated Image Conversion** and click **Create Video to Animated Image Conversion Template**.

Create Animated Image Template ✕

Template Name *

Enter a template name

Up to 64 chars. Only supports Chinese characters, English letters, numbers, underscores (_), hyphens (-) and *

Transcoding Start Time *

seconds

Transcoding Duration

☒ Original Video Duration ☐ Custom Duration

Frame Extraction Method *

☒ Extract all frames

☐ Frame Extraction Frequency

☐ Frame Extraction Interval

☐ Extract key frames only

Output Animated Image Frame Rate

☒ Adaptive Source video frame rate ☐ Custom Playback Frame Rate

Output Animated Image Format

☒ GIF ☐ WEBP

Output Animated Image Size

☒ Source Video Width and Height ☐ Custom

OK

Cancel

6. In the **Create Video to Animated Image Conversion Template** window, configure the following items:

Template Name: It can contain up to 64 letters, digits, underscores (_), hyphens (-), and asterisks (*).

Transcoding Start Time: You can select any time point within the full video length.

Transcoding Duration: It specifies the duration of video transcoding after the **transcoding start time**. You can select **Original Video Duration** or **Custom Duration**.

Frame Extraction Method:

Extract all frames: Every video frame will be extracted.

Frame Extraction Frequency: You can set the number of frames to be extracted per second (an integer between 1 and 50).

Frame Extraction Interval: Frame will be extracted at the specified intervals in seconds.

Extract key frames only: The system will intelligently identify and extract the optimal set of frames based on AI understanding of the video content and output them as an animated image.

Output Animated Image Frame Rate: If **Adaptive** is selected, the system will automatically select an appropriate frame rate based on the settings of the above parameters. You can also select **Custom Playback Frame Rate** to restrict the frame rate to 1–60 FPS.

Output Animated Image Format: The output animated image is in GIF format by default. If you select the WEBP format, you need to select the animated image quality, which ranges from 1 to 99 and is 75 by default.

Output Animated Image Size: The default output animated image size is the same as that of the original video. If you select custom width and height, you must enter an integer between 128 and 4096 for the width and height respectively.

7. Click **OK**.

After successfully creating the template, you can **view**, **edit**, or **delete** it in the custom template list.

Note:

You can use the template when creating a video-to-animated image conversion job as instructed in [Configuring Job](#) or creating a workflow as instructed in [Configuring Workflow](#).

Video watermark

The video watermark feature adds a text or image watermark to a video during transcoding.

Note:

Currently, you can add up to three watermarks in the console or five via API at a time. To add more watermarks, [contact us](#) for assistance.

Directions

1. Log in to the [COS console](#).
2. Click **Bucket List** on the left sidebar.
3. Click the name of the bucket where you want to store the video.
4. On the left sidebar, select **Data Processing Workflow > Template Configuration** to enter the template configuration page.
5. Select **Video Watermark** and click **Create Video Watermark Template**.

Opacity: Select a value between 1% and 100%.

Offset Method: The watermark offset is based on the origin point. You can select offset by ratio or fixed position.

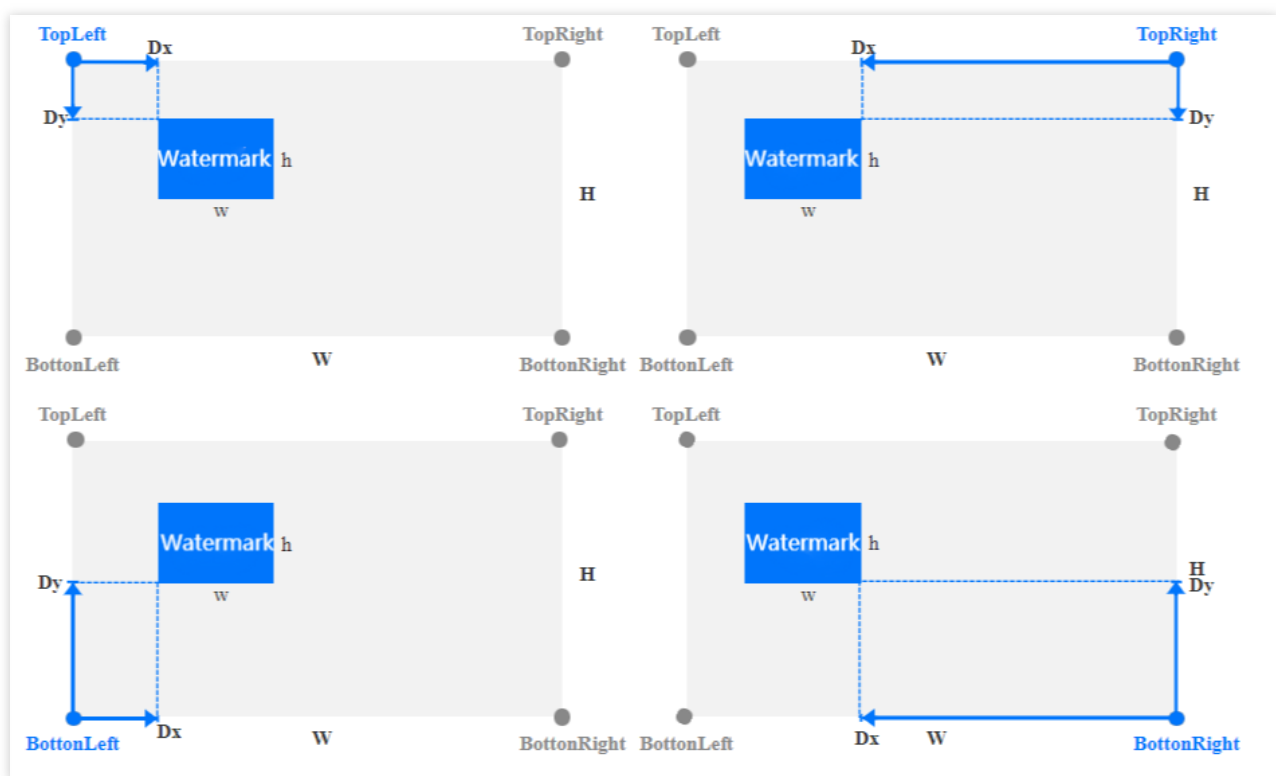
Watermark Duration: Select **Same as video duration** or **Specified period**. If you select the latter, you can set the watermark start time and end time. If you set the start time only, the watermark will be displayed until the video ends by default.

Image watermark parameters

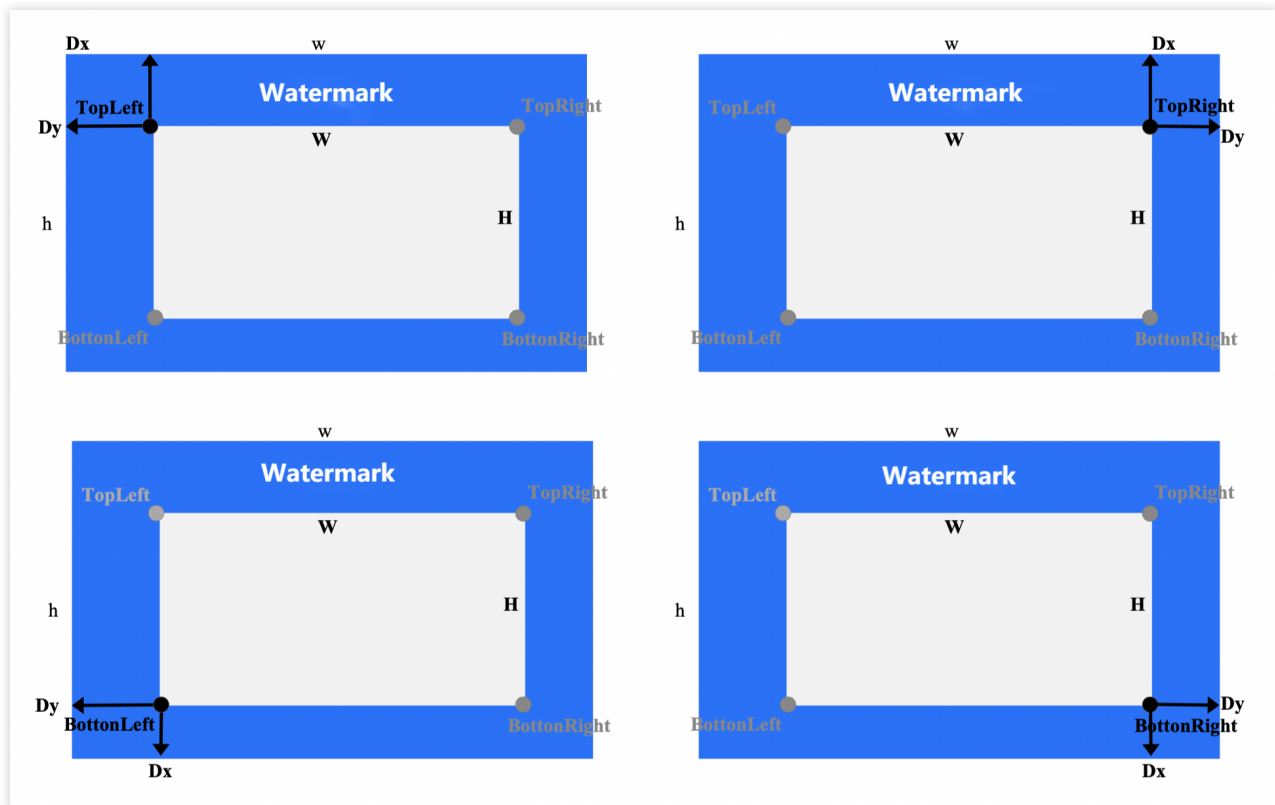
Select Image: If you select image watermark, you need to select its source. Currently, only a watermark image in the same bucket can be selected. If the bucket doesn't have desired images, you need to upload a new one.

Image Layer: Select whether to place the image on top of or underneath the video.

If the image is placed on top of the video, the effect is as shown below:



If the image is placed underneath the video (as the background), the effect is as shown below:



Watermark Dimensions:

Input image size: The original watermark image size will be retained without any processing. Note that if the watermark image is larger than the video image, the watermark cannot be completely displayed.

By ratio: You can set the percentage (1–100) of only the width or height or both of them. If the width or height is not set, it will be scaled proportionally. Suppose the width ratio is a and height ratio is b , then the watermark width will be $w = W * a$, and the watermark height will be $h = H * b$ (here, W and H are the video width and height respectively).

Fixed size: You can specify the watermark width and height between 8 and 4096 px.

Offset Method (On top of video):

By ratio: You can set the percentage (0–100) of the width or height. As shown below, suppose the horizontal offset ratio is a and the vertical ratio is b , then the horizontal offset will be $Dx = W * a$, and the vertical offset will be $Dy = H * b$ (here, W and H are the video width and height respectively).

Fixed position: Select a value between 0 and 4096 px. The horizontal offset is Dx , and the vertical offset is Dy .

Watermark Dimensions:

Input image size: The original watermark image size will be retained without any processing. Note that if the watermark image is smaller than the video image, the watermark cannot be completely displayed.

By ratio: You can set the percentage (100–300) of only the width or height or both of them. If the width or height is not set, it will be scaled proportionally. Suppose the width ratio is a and height ratio is b , then the watermark width

will be $w = W * a$, and the watermark height will be $h = H * b$ (here, W and H are the video width and height respectively).

Fixed size: You can specify the watermark width and height between 8 and 4096 px.

Offset Method (Underneath video):

By ratio: You can set the percentage (-300~0) of the width or height. As shown below, suppose the horizontal offset ratio is a and the vertical ratio is b , then the horizontal offset will be $Dx = W * a$, and the vertical offset will be $Dy = H * b$ (here, W and H are the video width and height respectively).

Fixed position: Select a value between -4096 and 0 px. The horizontal offset is Dx , and the vertical offset is Dy .

Text watermark parameters

Watermark Text: It can contain up to 64 letters, digits, underscores (_), hyphens (-), and asterisks (*).

Font Size: Select a value between 5 and 100 px.

Font: Select Ariblk, Arial, Ahronbd, Helvetica, or HelveticaNeue.

Font Color: It is in the format of $0xRRGGBB$.

7. Click **OK**.

After successfully creating the template, you can **view**, **edit**, or **delete** it in the custom template list.

You can click **Preview** to view the position and dimensions of the watermark in videos of three common resolutions and quickly adjust the template.

Note:

You can use the template when [creating an audio/video transcoding, SDR-to-HDR, video enhancement, or super resolution job as instructed in [Configuring Job](#) or creating a workflow as instructed in [Configuring Workflow](#).

Audio/Video splicing

The video/audio splicing feature adds the specified video/audio segment at the beginning or end of a video/audio file to generate a new one.

Directions

1. Log in to the [COS console](#).
2. Click **Bucket List** on the left sidebar.
3. Click the name of the bucket where you want to store the video.
4. On the left sidebar, select **Data Processing Workflow > Common Configuration**. Then, select the **Template** tab to go to the template configuration page.
5. Select **Audio/Video Splicing** and click **Create Audio/Video Splicing Template**.
6. In the **Create Audio/Video Splicing Template** window, configure the following items:
 Template Name: It can contain up to 64 letters, digits, underscores (_), hyphens (-), and asterisks (*).
 Container Format: Supported formats include AAC, MP3, MP4, FLV, HLS, and TS.
 Splicing Position: Select whether to add the file at the beginning or end of the source file.
 Other parameters: You can customize the audio/video parameters as needed.

7. Click **OK**.

After successfully creating the template, you can **view**, **edit**, or **delete** it in the custom template list.

Note:

You can use the template when creating an audio/video splicing job as instructed in [Configuring Job](#) or creating a workflow as instructed in [Configuring Workflow](#).

Voice separation

You can separate the same audio file into a voice file and a background sound file for subsequent video editing and playback.

Directions

1. Log in to the [COS console](#).
2. Click **Bucket List** on the left sidebar.
3. Click the name of the bucket where you want to store the video.
4. On the left sidebar, select **Data Processing Workflow > Template Configuration** to enter the template configuration page.
5. Select **Smart Audio > Voice Separation** and click **Create Voice Separation Template**.

Create Voice Separation Template ✕

Template Name *

Enter a template name

Up to 64 chars. Only supports Chinese characters, English letters, numbers, underscores (_), hyphens (-) and *

Output Audio Format

AAC

Output Audio *

☒ Voice ☐ Background sound

Sample Rate

44100

Audio Bitrate

128

Kbps

Value range: 8–1000. If this field is not set, the encoder's default bitrate is used.

Channels

Source File Channel Num

OK

Cancel

6. In the **Create Voice Separation Template** window, configure the following items:

Template Name: It can contain up to 64 letters, digits, underscores (_), hyphens (-), and asterisks (*).

Output Audio Format: Supported formats include MP3, AAC, AMR, and FLAC.

Output Audio: Specify to output voice or background sound.

Sample Rate: Select an option as needed.

Audio Bitrate: Enter a value as needed.

Channels: Select an option as needed.

7. Click **OK**.

After successfully creating the template, you can **view**, **edit**, or **delete** it in the custom template list.

Note:

You can use the template when creating a voice separation job as instructed in [Configuring Job](#) or creating a workflow as instructed in [Configuring Workflow](#).

Text to speech

You can convert text to speeches in different voices for use in audiobook, navigation, and other scenarios.

Directions

1. Log in to the [COS console](#).
2. Click **Bucket List** on the left sidebar.
3. Click the name of the bucket where you want to store the video.
4. On the left sidebar, select **Data Processing Workflow > Template Configuration** to enter the template configuration page.
5. Select **Smart Audio > Text to Speech** and click **Create Text-to-Speech Template**.
6. In the **Create Text-to-Speech Template** window, configure the following items:
Template Name: It can contain up to 64 letters, digits, underscores (_), hyphens (-), and asterisks (*).
Output Audio Format: Supported formats include MP3, AAC, AMR, and FLAC.
Voice: Specify the output voice.
Processing Mode: Select async or sync processing.
Volume: Adjust the output volume.
Speech Speed: Adjust the output speech speed.
7. Click **OK**.

After successfully creating the template, you can **view**, **edit**, or **delete** it in the custom template list.

Note:

You can use the template when creating a text-to-speech job as instructed in [Configuring Job](#) or creating a workflow as instructed in [Configuring Workflow](#).

Image quality enhancement

Video enhancement uses AI to improve the video quality and enhance the video colors and details visually. It includes super resolution, detail enhancement, SDR-to-HDR, and frame interpolation features.

Directions

1. Log in to the [COS console](#).
2. Click **Bucket List** on the left sidebar.
3. Click the name of the bucket where you want to store the video.
4. On the left sidebar, select **Data Processing Workflow > Template Configuration** to enter the template configuration page.
5. Select **Image Quality Enhancement** and click **Create Image Quality Enhancement Template**.
6. In the **Create Image Quality Enhancement Template** window, configure the following items:

Note:

Currently, video enhancement supports color enhancement, detail enhancement, super resolution, and SDR-to-HDR. Other features will be provided in the future.

The input video for enhancement must be shorter than 30 minutes.

Template Name: It can contain up to 64 letters, digits, underscores (_), hyphens (-), and asterisks (*).

Color Enhancement: Select automatic system analysis for color enhancement or customize the color enhancement parameters.

Detail Enhancement: Select automatic system analysis for detail enhancement or customize the detail enhancement parameters.

7. Click **OK**.

After successfully creating the template, you can **view**, **edit**, or **delete** it in the custom template list.

Note:

You can use the template when creating a video enhancement job as instructed in [Configuring Job](#) or creating a workflow as instructed in [Configuring Workflow](#).

Image processing

Image processing is a rich-featured, cost-effective, and high-reliability image processing service provided by CI. It supports flexible image editing, such as rotation, cropping, transcoding, and scaling. It provides multiple image downsizing solutions like Guetzli compression, TPG transcoding, and HEIF transcoding, as well as diversified copyright protection solutions like image/text/blind watermarking. This meets your image processing needs in different business scenarios.

Directions

1. Log in to the [COS console](#).
2. Click **Bucket List** on the left sidebar.
3. Click the name of the bucket where you want to store the video.
4. On the left sidebar, select **Data Processing Workflow > Common Configuration**. Then, select the **Template** tab to go to the template configuration page.
5. Select **Video Processing** and click **Create Video Processing Template**.

6. In the **Create Video Processing Template** window, configure the following items:

Template Name: It can contain up to 64 letters, digits, underscores (_), hyphens (-), and asterisks (*).

Editing Mode: Select Basic or Enhanced. The latter delivers greater image reconstruction and restoration effects.

Basic Processing: Select the output target resolution.

Text Watermark: After it is enabled, you can add a single or tiled watermark to the image.

Image Watermark: After it is enabled, you can add an animated or static watermark at the specified position on the image.

Preview: You can preview the processing effect.

7. Click **OK**.

After successfully creating the template, you can **view**, **edit**, or **delete** it in the custom template list.

Note:

You can use the template when creating an image processing job as instructed in [Configuring Job](#) or creating a workflow as instructed in [Configuring Workflow](#).

Queues and Callbacks

Last updated : 2024-06-24 16:14:43

Overview

When you activate the data processing workflow service, the system will **automatically create** a user queue for you. When you submit a job, the job will be arranged in the queue first and executed in sequence according to the priority and order of submission. You can also set a **callback rule** to stay up to date with the job or workflow progress, and the system will send the processing result and status information to the specified address. The queues for different services are as follows:

Feature Name	Queue Name
Media processing	queue-1
Speech recognition	queue-speech-1
File preview	queue-doc-process-1

Note:

Currently, one feature supports only one queue. If you want more concurrent queues, [contact us](#).

Directions

Enabling or pausing queue

You can enable or pause a queue in its **Operation** column.

1. Log in to the [COS console](#).
2. Select **Bucket List** on the left sidebar.
3. Click the name of the bucket for video storage.
4. On the left sidebar, select **Data Processing Workflow > Common Configuration**. Then, click **Queues and Callbacks** to enter the queue configuration page to enable or pause a queue.

Note:

After a queue is paused, its jobs will stop, and you cannot use the [job](#) and [workflow](#) features in the console.

Setting callback rule

COS supports user-defined callback URLs. After an event is completed, the system sends an HTTP POST request whose body contains notification content to a user-defined callback URL. You can use the configured callback URL to

learn about the processing progress and status so that you can perform other operations as needed.

1. Log in to the [COS console](#).
2. Select **Bucket List** on the left sidebar.
3. Click the name of the bucket for video storage.
4. On the left sidebar, select **Data Processing Workflow > Common Configuration**. Then, click **Queues and Callbacks** to enter the queue configuration page.
5. Click **Configure Callback Rule** in the **Operation** column of the target queue.
6. In the pop-up window, set the status to enable or disable callback.

Configure Callback Rule

Status

☒

Callback Mode

General callback

Callback URL ⓘ

After the callback URL takes effect, tasks that match the callback events v and send it a standard HTTP POST message. The HTTP status code 200 in is successful, 4xx callback content format not expected, and 5xx a service

Callback Fomat

☐ JSON ☒ XML

Callback Event

☒ Task completion ☐ Workflow completion

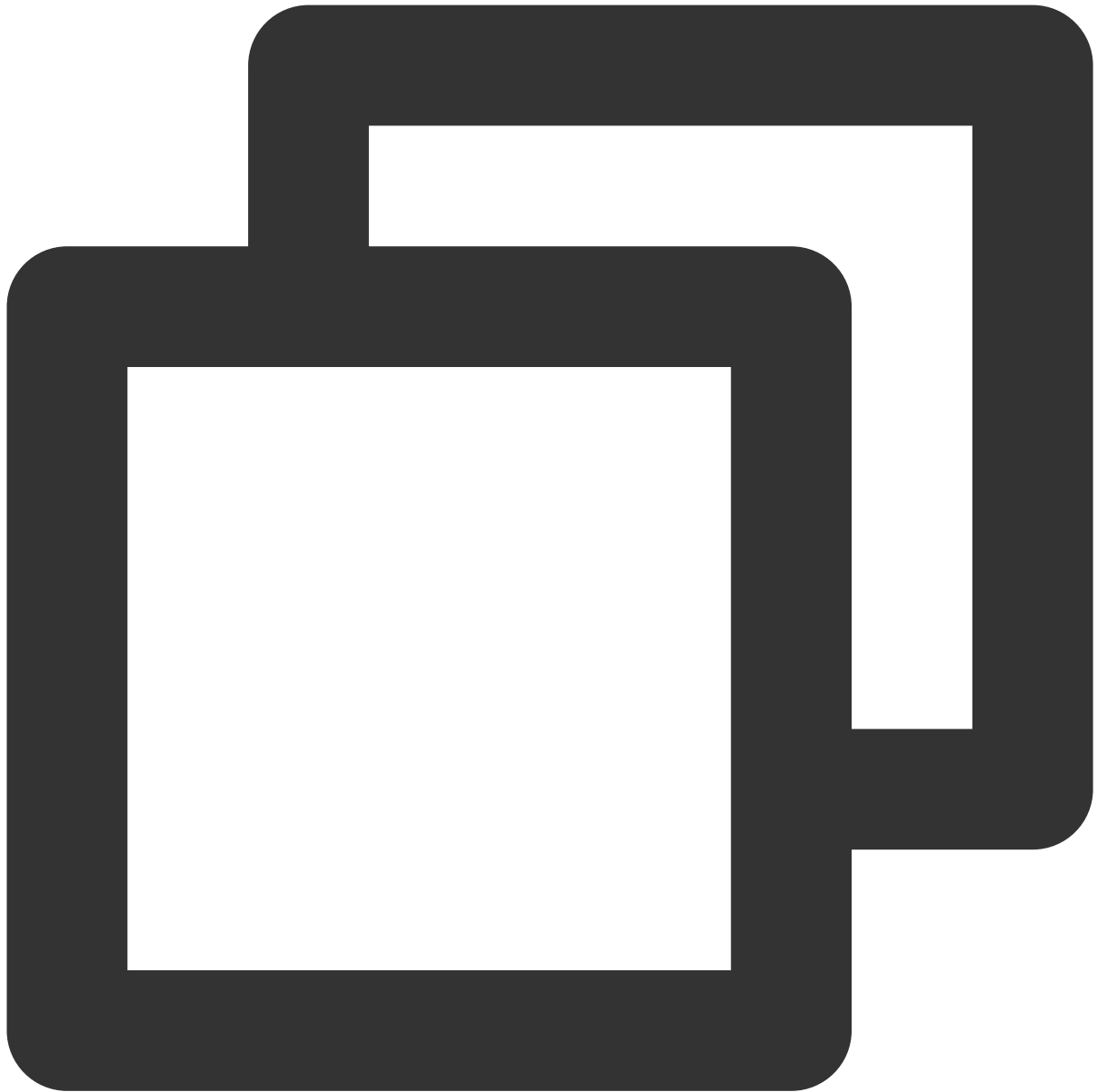
OK

Cancel

When enabling callback, you need to specify a URL for the system to send HTTP requests. For more information on callback, see [Callback content](#).

Callback content

After a job is completed, the system will send the following callback content to the configured callback URL:



```
<Response>
  <JobsDetail></JobsDetail>
  <NonExistJobIds></NonExistJobIds>
</Response>
```

The parameters are described as follows:

Parameter	Description	Type
JobsDetail	Job details. Same as <code>Response.JobsDetail</code> in <code>CreateMediaJobs</code> .	Container

NonExistJobIds	List of non-existing job IDs queried. If all jobs exist, this parameter is not returned.	String
----------------	--	--------

Application Integration

MySQL Backup

Last updated : 2024-06-24 16:14:43

Overview

MySQL Backup is a [SCF](#)-based feature provided by COS. It allows you to store data in TencentDB for MySQL to COS so that data can be stored persistently and protected from data loss or corruption. After you set a backup function rule for a bucket, SCF will scan your MySQL backup files periodically and store them in the bucket.

Notes

MySQL Backup functions only back up the backup files of TencentDB for MySQL. Therefore, if MySQL backup has not been enabled, the functions cannot be executed. For more information about TencentDB for MySQL backups, see [Backing up Databases](#).

If you have added a MySQL backup rule to your bucket in the COS console, the backup function will appear in the [SCF console](#). **DO NOT** delete the function. Otherwise, your rule may not take effect.

MySQL Backup is supported in SCF-enabled regions, including Guangzhou, Shanghai, Beijing, Chengdu, Hong Kong (China), Singapore, Mumbai, Toronto, and Silicon Valley. For more supported regions, see [SCF Documentation](#).

Directions

Setting backup via Application Integration

1. Log in to the [COS console](#).
2. On the left sidebar, click **Application Integration > Data Backup** and find **MySQL Backup**.
3. Click **Configure Backup Rule** to go to the rule configuration page.
4. Click **Add Function**.

Note:

If you haven't activated SCF, go to the [SCF console](#) to activate it and authorize the service as instructed.

5. In the pop-up window, configure the following items:

Function Name: Uniquely identifies a function and cannot be modified after being set. You can view the function in the [SCF console](#).

Associated Bucket: A bucket to store the MySQL backup files

Note:

The MySQL data to be backed up must be in the same region as the associated bucket.

Trigger Period: Triggers the backup operation for the MySQL Backup function. Every day, every week, and custom periods are supported.

Cron Expression: If you use a custom period, you can use Cron to specify the trigger period rule. Cron follows the local Standard Time. For detailed configuration policies, see [Timer Trigger Description](#).

Database Instance: MySQL instance in the region where the current bucket resides

Delivery Path: Delivery path prefix of the backups. If not specified, backups will be stored in the root directory of the bucket.

SCF Authorization: SCF needs to be authorized so that it can read the MySQL instances as well as their backup files, and store the backup files to the specified bucket.

6. Click **Confirm**.

You can perform the following operations on the created function:

Click **Log** to view the historical running status of MySQL backup. If an error is reported, you can click **Log** to quickly redirect to the SCF console for viewing the error log details.

Click **More > Edit** to modify the MySQL data backup rule.

Click **More > Delete** to delete the unwanted MySQL backup rule.

Setting backup via bucket configuration

1. Log in to the [COS console](#).

2. Click **Bucket List** on the left sidebar and then click the desired bucket for the backup.

3. Click **Function Service > MySQL Backup Function**.

Note:

If you haven't activated SCF, go to the [SCF console](#) to activate it and authorize the service as instructed.

4. Click **Add Function**.

5. In the pop-up window, configure the following items:

Function Name: Uniquely identifies a function and cannot be modified after being set. You can view the function in the [SCF console](#).

Trigger Period: Triggers the backup operation for the MySQL Backup function. Every day, every week, and custom periods are supported.

Cron Expression: If you use a custom period, you can use Cron to specify the trigger period rule. Cron follows China Standard Time (UTC+8:00). For detailed configuration policies, see [Cron Documentation](#).

Database Instance: MySQL instance in the region where the current bucket resides

Delivery Path: Delivery path prefix of the backups. If not specified, backups will be stored in the root directory of the bucket.

SCF Authorization: SCF needs to be authorized so that it can read the MySQL instances as well as their backup files, and store the backup files to the specified bucket.

6. Click **Confirm**.

You can perform the following operations on the created function:

Click **Log** to view the historical running status of MySQL backup. If an error is reported, you can click **Log** to quickly redirect to the SCF console for viewing the error log details.

Click **More > Edit** to modify the MySQL data backup rule.

Click **More > Delete** to delete the unwanted MySQL backup rule.

MongoDB Backup

Last updated : 2024-06-24 16:14:43

Overview

MongoDB Backup is a [SCF](#)-based feature provided by COS. It allows you to back up data in TencentDB for MongoDB to COS so that data can be stored persistently and protected from data loss or corruption. After you set a backup function rule for a bucket, SCF will scan your MongoDB backup files periodically and store them in the bucket.

Notes

MongoDB Backup functions only back up the backup files of TencentDB for MongoDB. Therefore, if MongoDB backup has not been enabled, the functions cannot be executed. For more information about TencentDB for MongoDB backups, see [Data Backup](#).

If you have added a MongoDB backup rule to your bucket in the COS console, the backup function will appear in the [SCF console](#). **DO NOT** delete this function. Otherwise, your rule may not take effect.

MongoDB Backup is supported in SCF-enabled regions, including Guangzhou, Shanghai, Beijing, Chengdu, Hong Kong (China), Singapore, Mumbai, Toronto, and Silicon Valley. For more supported regions, see [SCF Documentation](#).

Directions

1. Log in to the [COS console](#).
2. On the left sidebar, click **Application Integration > Data Backup** and find **MongoDB Backup**.
3. Click **Configure Backup Rule** to go to the rule configuration page.
4. Click **Add Function**.

Note:

If you haven't activated SCF, go to the [SCF console](#) to activate it and authorize the service as instructed.

5. In the pop-up window, configure the following items:

Function Name: Uniquely identifies a function and cannot be modified after being set. You can view the function in the [SCF console](#).

Associated Bucket: A bucket to store the MongoDB backup files.

Trigger Period: Triggers the backup operation for the MongoDB Backup function. Every day, every week, and custom periods are supported.

Cron Expression: If you use a custom period, you can use Cron to specify the trigger period rule. Cron follows the local Standard Time. For detailed configuration policies, see [Timer Trigger Description](#).

Database Instance: MongoDB instance in the region where the current bucket resides

Delivery Path: Delivery path prefix of the backups. If not specified, backups will be stored in the root directory of the bucket.

SCF Authorization: SCF needs to be authorized so that it can read the MongoDB instances as well as their backup files, and store the backup files to the specified bucket.

6. Click **Confirm**.

You can perform the following operations on the created function:

Click **Log** to view the historical running status of MongoDB backup. If an error is reported, you can click **Log** to quickly redirect to the SCF console for viewing the error log details.

Click **More > Edit** to modify the MongoDB data backup rule.

Click **More > Delete** to delete the unwanted MongoDB backup rule.

SQL Server Data Backup

Last updated : 2024-06-24 16:14:43

Overview

SQL Server data backup is a [SCF](#)-based database backup feature provided by COS. It allows you to dump SQL Server data to COS so that data can be stored persistently and protected from data loss or corruption. After you set a backup function rule for a specified bucket, SCF will scan your server backup files periodically and dump them in the bucket.

Notes

SQL Server data backup functions back up only the backup files of SQL Server. If SQL Server backup is not enabled, the backup functions cannot be executed.

If you have added a SQL Server data backup rule to your bucket in the COS console, you can view it in the [SCF console](#). **DO NOT** delete the function. Otherwise, your rule may not take effect.

SQL Server data backup is supported in SCF-enabled regions, including Guangzhou, Shanghai, Beijing, Chengdu, Hong Kong (China), Singapore, Mumbai, Toronto, and Silicon Valley. For more supported regions, see [SCF Documentation](#).

Directions

1. Log in to the [COS console](#).
2. On the left sidebar, click **Application Integration > Data Backup**.
3. Find **SQL Server Backup** and click **Configure Backup Rule** to go to the rule configuration page.
4. Click **Add Function**.

Note:

If you haven't activated SCF, go to the [SCF console](#) to activate it and authorize the service as instructed.

5. In the pop-up window, configure the following items:

Function Name	Uniquely identifies a function and cannot be modified after being set. You can view the function in the SCF console .
Associated Bucket	A bucket to store SQL Server backup files.
Trigger Period	Triggers the backup operation for the SQL Server backup function. Every day, every week, and custom periods are supported.

Cron Expression	If you use a custom period, you can use Cron to specify the trigger period rule. Cron follows the local Standard Time. For detailed configuration policies, see Timer Trigger Description .
Database Instance	SQL Server instance list of the region where the current bucket resides
Delivery Path	Delivery path prefix of the backups. If not specified, backups will be stored in the root directory of the bucket.
SCF Authorization	SCF needs to be authorized so that it can read the SQL Server instances as well as their backup files, and save the backup files to the specified bucket.

6. Click **Confirm**.

You can perform the following operations on the created function:

Click **Log** to view the historical running status of the SQL Server data backup. If an error is reported, you can click **Log** to quickly redirect to the SCF console for viewing the error log details.

Click **More > Edit** to modify the SQL Server data backup rule.

Click **More > Delete** to delete the unwanted SQL Server data backup rule.

CKafka Message Backup

Last updated : 2024-06-24 16:14:43

Overview

CKafka message backup is provided by COS based on [SCF](#) to dump CKafka messages to COS, which facilitates data analysis and download.

Based on the open-source Apache Kafka message queuing engine, Tencent Cloud Kafka (CKafka) provides high-throughput and highly scalable message queuing services. For more information, see [Overview](#).

If a backup rule has been configured for a bucket, messages generated in a CKafka instance will be dumped to the COS bucket according to the specified time granularity.

Notes

If you have added a CKafka message backup rule to your bucket via the COS console, the function will appear in the [SCF console](#). **DO NOT** delete the function. Otherwise, your rule may not take effect.

CKafka message backup is supported in SCF-enabled regions, including Guangzhou, Hong Kong (China), Shanghai, Beijing, Chengdu, Singapore, Mumbai, Toronto, and Silicon Valley. For more supported regions, see the [SCF documentation](#).

Directions

1. Log in to the [COS console](#).
2. On the left sidebar, click **Application Integration > Data Backup** and find **CKafka Message Backup**.
3. Click **Configure Backup Rule** to go to the rule configuration page.
4. Click **Add Function**.

Note:

If you haven't activated SCF, go to the [SCF console](#) to activate it and authorize the service as instructed.

5. In the pop-up window, configure the following items:

Function Name: Uniquely identifies a function and cannot be modified after being set. You can view the function in the [SCF console](#).

Associated Bucket: A COS bucket that stores CKafka messages

Time Granularity: You can set an interval (5–15 minutes) to aggregate messages according to the message volume. The dumping performance is affected by the number of files aggregated, the number of partitions, and the value of

`partition_max` . For more information, see **Partition** in [Glossary](#).

SCF Authorization: (required) SCF needs to be authorized to read messages of CKafka instances and dump the messages to the specified bucket.

6. Click **Next** to configure CKafka as follows:

Instance: A CKafka instance that is used as the message source. Only instances in the same region are supported.

Topic: A topic used as the message source

Start Point: The topic offset for dumping the backup messages

Address: A VPC address is required. CKafka instances that use a classic network require a routing policy. For more information, see [Adding Routing Policy](#).

Note:

An IP address in the corresponding VPC subnet must be available and support DHCP.

7. Click **Next** to configure delivery. The configuration item is as follows:

Destination Path: A path to deliver the backup messages. If this field is not specified, the files will be stored in the root directory of the bucket. To use a prefix, end it with a slash (/).

8. Click **Confirm**.

You can perform the following operations on the created function:

Click **Log** to view the historical running status of CKafka message backup. If an error is reported, you can click **Log** to quickly redirect to the SCF console for viewing the error log details.

Click **More > Edit** to modify the CKafka message backup rule.

Click **More > Delete** to delete the unwanted CKafka message backup rule.

TDMQ Message Backup

Last updated : 2024-06-24 16:14:43

Overview

TDMQ message backup is provided by COS based on [SCF](#) to dump TDMQ messages to COS, which facilitates data analysis and download.

TDMQ is a proprietary finance-grade distributed message middleware developed based on [Pulsar](#), an open-source project of Apache. It features high cross-region consistency, reliability, and concurrency. For more information, see [Overview](#).

If a backup rule has been configured for a bucket, SCF will dump messages generated in TDMQ to a COS bucket according to the specified time granularity.

Notes

If you have added a TDMQ message backup rule to your bucket via the COS console, the function will appear in the [SCF console](#). **DO NOT** delete the function. Otherwise, your rule may not take effect.

Currently, regions that support backing up TDMQ messages to COS include Guangzhou, Shanghai, Hong Kong (China), Beijing, Chengdu, Singapore, and Silicon Valley.

Directions

1. Log in to the [COS console](#).
2. On the left sidebar, click **App Integration** > **Data Backup** and find **TDMQ Message Backup**.
3. Click **Configure Backup Rule** to go to the rule configuration page.
4. Click **Add Function**.

Note:

If you haven't activated SCF, go to the [SCF console](#) to activate it and authorize the service as instructed.

5. In the pop-up window, configure the following items:

Function Name: Uniquely identifies a function and cannot be modified after being set. You can view the function in the [SCF console](#).

Associated Bucket: A COS bucket that stores TDMQ messages

Time Granularity: An interval (5–15 minutes) to aggregate messages according to the message volume. Each message file can be up to 500 MB and contain up to 5,000 pieces of messages.

SCF Authorization: (required) SCF needs to be authorized to read TDMQ messages and dump the messages to the specified bucket.

6. Click **Next** to configure TDMQ as follows:

Cluster: A TDMQ cluster as the message source. Only TDMQ clusters in the same region are supported.

Namespace: A namespace in the cluster

Topic: A topic used as the message source

Subscription: Select a subscription. If existing subscriptions cannot meet your needs, you can create a new one in the [TDMQ console](#).

Start Point: Start point of historical messages

Role: Select the TDMQ role (a TDMQ-specific concept, which is different from that mentioned in Tencent Cloud), which is the minimum unit for permission division within TDMQ. You can create multiple roles and grant them different message production/consumption permissions in different namespaces.

Role Key: Select the TDMQ role key, which is an authentication tool. You can add a key in the client to access TDMQ to produce/consume messages. Each role has a unique key corresponding to itself.

Address: It must be a VPC access address. The TDMQ cluster should be connected to the VPC. For more information, see [VPC Access](#).

Note:

An IP address in the corresponding VPC subnet must be available and support DHCP.

7. Click **Next** to configure delivery. The configuration item is as follows:

Destination Path: A path to deliver the backup messages. If this field is not specified, the files will be stored in the root directory of the bucket. To use a prefix, end it with a slash (/).

8. Click **Confirm**.

You can perform the following operations on the created function:

Click **Log** to view the historical running status of TDMQ message backup. If an error is reported, you can click **Log** to quickly redirect to the SCF console for viewing the error log details.

Click **More > Edit** to modify a TDMQ message backup rule.

Click **More > Delete** to delete an unwanted TDMQ message backup rule.

Redis Backup

Last updated : 2024-06-24 16:14:43

Overview

Redis Backup is a [SCF](#)-based feature provided by COS. It allows you to store data in TencentDB for Redis to COS so that data can be stored persistently and protected from data loss or corruption. After you set a backup function rule for a bucket, SCF will scan your Redis backup files periodically and store them in the bucket.

Notes

Redis Backup functions back up only the backups of TencentDB for Redis. Therefore, if Redis Backup has not been enabled, the functions cannot be executed. For more information on TencentDB for Redis backup, see [Backing up Data](#).

If you have added a Redis Backup function rule to your bucket via the COS console, the function will appear in the [SCF console](#). **DO NOT** delete the function. Otherwise, your rule may not take effect.

Redis Backup is supported in SCF-enabled regions, including Guangzhou, Shanghai, Beijing, Chengdu, Hong Kong (China), Singapore, Mumbai, Toronto, and Silicon Valley. For more supported regions, see the [SCF documentation](#).

Directions

1. Log in to the [COS console](#).
2. On the left sidebar, click **Application Integration > Data Backup**.
3. Find **Redis Backup** and click **Configure Backup Rule** to go to the rule configuration page.
4. Click **Add Function**.

Note:

If you haven't activated SCF, go to the [SCF console](#) to activate it and authorize the service as instructed.

5. In the pop-up window, configure the following items:

Function Name: Uniquely identifies a function and cannot be modified after being set. You can view the function in the [SCF console](#).

Associated Bucket: A bucket to store Redis backups

Trigger Period: Triggers the backup operation for the Redis Backup function. Every day, every week, and custom periods are supported.

Cron Expression: If you use a custom period, you can use Cron to specify the trigger period rule. Cron follows the Local Standard Time. For detailed configuration policies, see [Timer Trigger Description](#).

Database Instance: TencentDB for Redis instance in the same region where the current bucket resides

Delivery Path: Delivery path prefix of the backups. If not specified, backups will be stored in the root directory of the bucket.

SCF Authorization: SCF needs to be authorized so that it can read the Redis instances as well as their backups, and store the backups to the specified bucket.

6. Click **Confirm**.

You can perform the following operations on the created function:

Click **Log** to view the historical running status of Redis backup. If an error is reported, you can click **Log** to quickly redirect to the SCF console for viewing the error log details.

Click **More > Edit** to modify the Redis backup rule.

Click **More > Delete** to delete the unwanted Redis backup rule.

CDN Log Backup

Last updated : 2024-06-24 16:14:43

Overview

After a domain name is connected to [Content Delivery Network \(CDN\)](#), users' resource requests will be scheduled to CDN nodes. If a CDN node has the resource cached, it returns the resource directly. Otherwise, the request will be passed through to the origin server to pull the requested resource.

CDN nodes respond to most of the user requests. To facilitate access analysis, CDN packages access logs of the entire network at an hourly granularity.

The CDN log backup feature is provided by COS based on [SCF](#) to dump CDN logs to COS, which facilitates access behavior analysis and service quality monitoring.

After you configure a log backup rule for a bucket, SCF will dump the CDN logs to the bucket according to the time granularity configured.

Notes

Once you added a CDN log backup rule to your bucket via the COS console, the backup function can be viewed in the [SCF console](#). **DO NOT** delete the function. Otherwise, your rule may not take effect.

CDN log backup is supported in SCF-enabled regions, including Guangzhou, Shanghai, Hong Kong (China), Beijing, Chengdu, Singapore, Mumbai, Toronto, and Silicon Valley. For more supported regions, see the [SCF documentation](#).

Directions

1. Log in to the [COS console](#).
2. On the left sidebar, click **Application Integration > Data Backup** and find **CDN Log Backup**.
3. Click **Configure Backup Rule** to go to the rule configuration page.
4. Click **Add Function**.

Note:

If you haven't activated SCF, go to the [SCF console](#) to activate it and authorize the service as instructed.

5. In the pop-up window, configure the following items:

CreatedCDN Log Backup Function

Function Name

Enter the prefix of function name -cdnlog-6e3e8dd67e26def6809d64bd103814c3

Beginning with a letter, support a-z, A-Z, 0-9, -, _, up to 10 characters, and at least 1 character

Associated Bucket

examplebucket-125-125-125-125

Trigger Period

Every day

Every day00:00

Cron Expression

0 0 0 * * *

Cron follows China Standard Time (UTC+08:00). For detailed configuration policies, please see [Cron Documentation](#).

CDN Acceleration Domain

Please select

Delivery Path ⓘ

☒ Root-directory ☐ Specified prefix

SCF Authorization

☐ Authorize SCF Service

To use SCF, you need to authorize a third-party role to SCF so that it can access cloud resources for you.
Please click above to authorize.

Confirm

Cancel

Function Name: Uniquely identifies a function and cannot be modified after being set. You can view the function in the [SCF console](#).

Associated Bucket: A COS bucket that stores the CDN logs

Trigger Period: A period to trigger the CDN log backup (a timer is used). Every day and custom periods are supported.

Cron Expression: If you use a custom period, you can use Cron to specify the trigger period rule. Cron follows the Local Standard Time. For detailed configuration policies, see [Timer Trigger Description](#).

CDN Acceleration Domain: One or multiple domains whose logs are to dump

Destination Path: A path to deliver the logs. You can deliver logs to the root directory or specify a path prefix.

SCF Authorization: (required) SCF needs to be authorized to read CDN logs and dump them to the specified bucket.

6. Click **Confirm**. After the CDN backup rule is created, you can view it in the list.

You can perform the following operations on the created CDN log backup rule:

Click **Log** to view the historical running status of CDN log backup. If an error is reported, you can click **Log** to quickly redirect to the SCF console for viewing the error log details.

Click **More > Edit** to modify the CDN log backup rule.

Click **More > Delete** to delete the unwanted CDN log backup rule.

CLS Log Backup

Last updated : 2024-06-24 16:14:43

Overview

The CLS log backup feature is provided by COS based on [SCF](#) to dump CLS logs to COS.

After you configure a log backup rule for a bucket, SCF will dump the CLS logs to the bucket according to the time granularity configured.

CLS log backup can ship log data to COS to further meet the needs of log backup scenarios and harness the value of log data. Log backup is an asynchronous process. When log data is generated, SCF automatically backs up the log data to COS for storage via trigger.

Notes

If you have previously added a CLS log backup rule to your bucket via the COS console, you can view the CLS log backup function you created in the [SCF console](#). **DO NOT** delete the function. Otherwise, your rule may not take effect.

CLS log backup is supported in SCF-enabled regions, including Guangzhou, Shanghai, Beijing, Hong Kong (China), Chengdu, Singapore, Mumbai, Toronto, and Silicon Valley. For more supported regions, see the [SCF documentation](#).

Directions

1. Log in to the [COS console](#).
2. On the left sidebar, click **Application Integration > Data Backup** and find **CLS Log Backup**.
3. Click **Configure Backup Rule** to go to the rule configuration page.
4. Click **Add Function**.

Note:

If you haven't activated SCF, go to the [SCF console](#) to activate it and authorize the service as instructed.

5. In the pop-up window, configure the following items:

Function Name: Uniquely identifies a function and cannot be modified after being set. You can view the function in the [SCF console](#).

Associated Bucket: A COS bucket that stores the CLS logs.

Logset: A [logset](#) is a project management unit of CLS, used to distinguish logs of different projects. You can select the logset of the message source, which must be in the function region.

Log Topic: A log topic is the basic management unit of CLS and also the smallest unit for managing and configuring CLS triggers. A logset can contain multiple log topics. You can select a log topic of the message source.

Max Wait Time: You can set this parameter to control the log obtaining frequency. The parameter value can range from 3 to 300 seconds. If you set the parameter to 300 seconds, the SCF will collect the log data generated within 300 seconds and package it centrally as log files for backup.

SCF Authorization: SCF needs to be authorized to read CLS logs and dump them to the specified bucket.

6. Click **Next** to configure the following information:

Compression Format: You can determine whether to compress log files before backup. A compressed log file can be up to 128 KB. Currently, log files can be compressed using gzip, lzop or snappy.

Partition Format: A directory is automatically generated based on the strftime syntax. For example, if the partition format is `%Y/%m/%d/%Y%m%d%H%M`, the generated directory is `2021/06/25/202106252232`.

Delivery Path: Log backup path. You can select the root directory or specify a path prefix.

Delivery Sample: The final backup filename is in the format of `{COS bucket}{Directory prefix}{Partition format}_{random}.{type}`.

7. Click **Confirm**. After the CLS backup rule is created, you can view it in the list.

You can perform the following operations on the created CLS log backup rule:

Click **Log** to view the historical running status of CLS log backup. If an error is reported, you can click **Log** to quickly redirect to the SCF console for viewing the error log details.

Click **More > Edit** to modify the CLS log backup rule.

Click **More > Delete** to delete the unwanted CLS log backup rule.

Adding Log Analysis Function

Last updated : 2024-06-24 16:14:43

Overview

The COS log analysis feature applies to various scenarios to help you efficiently extract key information from log files. This document describes how to add a COS log analysis function. After adding a function, see [Setting Log Analysis](#) to use this feature.

Notes

If you have added a COS log analysis rule to your bucket via the COS console, you can view the COS log analysis function you created in the [SCF console](#). **Do not** delete the COS log analysis function. Otherwise, your rule may not take effect.

COS log analysis is supported in SCF-enabled regions, including Guangzhou, Shanghai, Beijing, Chengdu, Hong Kong (China), Singapore, Mumbai, Toronto, and Silicon Valley. For more supported regions, see the [SCF documentation](#).

The log analysis feature depends on the SCF service, which provides users with a [free tier](#). You will be billed for the part exceeding the free tier according to [SCF pricing](#).

Directions

1. Log in to the [COS console](#).
2. On the left sidebar, click **App Integration > Extended Features** and find **COS Log Analysis**.
3. Click **Configure Analysis Feature** to enter the function rule configuration page.
4. Select a region to add the function and click **Add Function**. Configure the following information in the pop-up window:

Function Name: Uniquely identifies a function and cannot be modified after it is created. You can view the function in the [SCF console](#).

Associated Bucket: Select a COS bucket with the log analysis feature enabled.

Execution Method: Only async execution is supported. After the function is called, tasks will be executed asynchronously without returning the execution result. A longer running time is supported.

Authentication Method: Only SCF is supported.

SCF Authorization: SCF need to be authorized to read files from your bucket and save the result file to the specified folder.

5. Click **Confirm**.

You can perform the following operations on the created function:

Click **Log** to view the historical running status.

Click **Details** to view detailed configuration rules.

Click **More > Edit** to modify a COS log analysis rule.

Click **More > Delete** to delete an unwanted COS log analysis rule.

Data Export to CKafka

Last updated : 2024-06-24 16:14:43

Overview

Data export to CKafka is a data export solution provided by COS based on [SCF](#). It can help you export data in CSV, JSON, and other formats to the CKafka service in the same region for aggregation and analysis of massive amount of message and log data.

Notes

Data export to CKafka involves COS' data extraction APIs. For more information on the restrictions, see [SELECT Overview](#).

If you have added a rule of data export to CKafka to your bucket in the COS console, the export function will appear in the [SCF console](#). **Do not** delete or modify the function; otherwise, your rule may not take effect.

Currently, the data export to CKafka feature is only supported in Guangzhou, Shanghai, Beijing, and Chengdu regions.

The data export to CKafka feature depends on the SCF service, which provides a [free tier](#). Excessive usage will be billed at SCF prices. For more information, see [Pricing](#).

Directions

1. Log in to the [COS console](#).
2. On the left sidebar, click **App Integration** > **Data Export** and find **Data Export to CKafka**.
3. Click **Configure Rule** to enter the rule configuration page.
4. Click **Add Function**.

Note:

If you haven't activated SCF, go to the [SCF console](#) to activate it and authorize the service as instructed.

5. In the pop-up window, configure the following information:

Create data export function - Configurations

Function name prefix

Beginning with a letter, support a-z, A-Z, 0-9, -, _ up to 10 characters, and at least 1 character

Scenario

☒ COS log file export ☐ Custom export

Source Bucket

Log storage status

Enabled

Destination Bucket

Log delivery prefix

SCF Authorization

☐ Authorize SCF Service

SCF needs to be granted a third-party role to access cloud resources.

Enter preset parameter

Cancel

Function name prefix: It uniquely identifies a function and cannot be modified after being set. You can view the function in the [SCF console](#).

Scenario: Select the log source from which you want to export data. We recommend you select **COS log file export**.

Source bucket: It is the name of the bucket where the logs are stored. If you select **COS log file export**, you need to enable the COS log storage feature first.

Log storage status: Make sure that the status is **Enabled**.

Destination Bucket: The bucket to store the logs.

Log delivery prefix: Enter a path prefix that makes it easy for you to find logs.

SCF authorization: This authorization is required, because data export to CKafka requires you to authorize SCF to read logs from your bucket.

6. Click **Enter preset parameter** to set the data export to CKafka configuration items as follows:

Create Data export function

×

✓ Basic Function Configuration

>

✓ Data extraction

>

3 Data export

Access method

☒ Public network
 ☐ VPC

Address

The access URL does not need to contain a protocol

Topic

Authentication Configuration

☒ No
 ☐ Authentication required

Max rate

100

data entries per second

Previous

Confirm

Access method: Select the CKafka access method. If you select **VPC**, you need to enter the VPC information.

Address: Enter your CKafka access address.

Topic: Enter the name of your CKafka topic.

Authentication configuration: Select your CKafka authentication method. If you select **Authentication required**, you need to enter the corresponding username and password.

Max rate: Set the rate cap for exporting data to CKafka.

7. If you want to personalize log data extraction, click **Previous** to configure options. Generally, we recommend you directly click **Confirm** to add the function.

Function Name	Associate...	Event Type	Trigger Sc...	Data extraction	Data export	Authorize...	Operation
test-lokafka-6def149cef...	examplebu...	File upload	Prefix: cos-...	Decompression method: Decompressi... Extraction method: CSV Row delimiter: \n Column delimiter: space Column header: None SQL expression: Select _1 as eventVe...	Access method: Public network Access URL: example.com Topic: 11 Max rate: 100 data entries per second	COS_SCF...	Log Details More ▾

You can perform the following operations on the created function:

Click **Log** to view the historical running status of data export to CKafka. If an error is reported, you can click **Log** to quickly redirect to the SCF console to view its details.

Click **Details** to view the detailed configuration of the function.

Click **Edit** to modify a rule of data export to CKafka.

Click **Trigger** and select an existing log in the bucket to directly trigger the export to CKafka.

Click **Delete** to delete an unwanted rule of data export to CKafka.

Data Export to ES

Last updated : 2024-06-24 16:14:43

Overview

Data export to ES is a data export solution provided by COS based on [SCF](#). It can help you export data in CSV, JSON, and other formats to the ES service in the same region for quick setup of log analysis and exception monitoring use cases.

Notes

Data export to ES involves COS' data extraction APIs. For more information on the restrictions, see [SELECT Overview](#).

If you have added a rule of data export to ES to your bucket in the COS console, the export function will appear in the [SCF console](#). **Do not** delete or modify the function; otherwise, your rule may not take effect.

Currently, the data export to ES feature is only supported in Guangzhou, Shanghai, Beijing, and Chengdu regions.

The data export to ES feature depends on the SCF service, which provides a [free tier](#). Excessive usage will be billed at SCF prices. For more information, see [Pricing](#).

Directions

1. Log in to the [COS console](#).
2. On the left sidebar, click **App Integration > Data Export** and find **Data Export to ES**.
3. Click **Configure Rule** to enter the rule configuration page.
4. Click **Add Function**.

Note:

If you haven't activated SCF, go to the [SCF console](#) to activate it and authorize the service as instructed.

5. In the pop-up window, configure the following information:

Create data export function - Configurations

Function name prefix

Beginning with a letter, support a-z, A-Z, 0-9, -, _ up to 10 characters, and at least 1 character

Scenario

☒ COS log file export ☐ Custom export

Source Bucket

Log storage status

Enabled

Destination Bucket

Log delivery prefix

cos-access-log/

SCF Authorization

☐ Authorize SCF Service

SCF needs to be granted a third-party role to access cloud resources.

Enter preset parameter

Cancel

Function name prefix: It uniquely identifies a function and cannot be modified after being set. You can view the function in the [SCF console](#).

Scenario: Select the log source from which you want to export data. We recommend you select **COS log file export**.

Source bucket: It is the name of the bucket where the logs are stored. If you select **COS log file export**, you need to enable the COS log storage feature first.

SCF authorization: This authorization is required, because data export to ES requires you to authorize SCF to read logs from your bucket.

6. Click **Enter preset parameter** to set the data export to ES configuration items as follows:

Create Data export function

×

✓ Basic Function Configuration

>

✓ Data extraction

>

3 Data export

Service version

☒ 7.x
 ☐ 6.x

Access method

☒ Public network
 ☐ VPC

Address

The access URL must contain a protocol and start with http:// or https://

Index name

Authentication Configuration

☒ No
 ☐ Authentication required

Max rate

100

data entries per second

Previous

Confirm

Service version: Select the ES version, which can be 7.x or 6.x.

Access method: Select the ES access method. If you select **VPC**, you need to enter the VPC information.

Address: Enter the ES access address, which must start with `http://` or `https://`.

Index name: Enter the name of the ES search index you created.

Authentication configuration: Select your ES authentication method. Currently, you can only select **Authentication required** for ES, and you need to enter the corresponding username and password.

Max rate: Set the rate cap for exporting data to ES.

7. If you want to personalize log data extraction, click **Previous** to configure options. Generally, we recommend you directly click **Confirm** to add the function.

Function Name	Associate...	Event Type	Trigger Sc...	Data extraction	Data export	Authorize...	Operation
test-toes-6def149cefd5...	examplebu...	File upload	Prefix: cos-...	Decompression method: Decompressi... Extraction method: CSV Row delimiter: \n Column delimiter: space Column header: None SQL expression: Select _1 as eventVe...	Service version: 7.x Access method: Public network Access URL: https:// Index name: doc Max rate: 100 data entries per second	COS_SCF...	Log Details More ▾

You can perform the following operations on the created function:

Click **Log** to view the historical running status of data export to ES. If an error is reported, you can click **Log** to quickly redirect to the SCF console to view its details.

Click **Details** to view the detailed configuration of the function.

Click **Edit** to modify a rule of data export to ES.

Click **Trigger** and select an existing log in the bucket to directly trigger the export to ES.

Click **Delete** to delete an unwanted rule of data export to ES.