

# **Object-Oriented Storage User Manual**

V6

China Telecom Cloud Technology Co.,Ltd





#### **Table of Contents**

1 Introduce	1
2 Basic Concept	2
2.1 OOS Basic Concept	2
2.1.1 Account	2
2.1.2 Service	2
2.1.3 Bucket	3
2.1.4 Object	3
2.1.5 Storage Classes	3
2.1.6 Compliance Retention (Object Lock Function)	4
2.2 Statistics	5
2.2.1 Basic Concept	5
2.3 CloudTrail	5
2.3.1 Basic Concpet	6
2.4 IAM	6
2.4.1 Features	6
2.4.2 Application Scenario	6
2.4.3 Basic Concept	6
2.4.4 Constraints	7
3 Account Management	8
3.1 Activate OOS Service	8
3.2 Enter Object-Oriented Storage Console	8
3.3 Retrieve Password	8
3.4 Logout	8
3.5 Region Switch	8
4 Statistics Overview	10
4.1 Overview	10
4.2 Statistics	11
4.2.1 Storage	11
4.2.2 Deleted Storage	13
4.2.3 Traffic	14
4.2.4 Requests	16
4.2.5 Concurrent Connections	18
4.2.6 Restore	19
5 Buckets	21
5.1 Bucket Management	21
5.1.1 Creating a Bucket	21
5.1.2 Bucket List	24
5.1.3 Deleting a Bucket	24
5.1.4 Bucket Properties	25
5.1.5 Region Properties	26
5.1.6 Security Policy	26
5.1.7 Website	29
5.1.8 Logging	33



	5.1.9 Lifecycle	33
	5.1.10 Cross-Origin Resource Sharing (CORS)	36
	5.1.11 Compliance Retention (Object Lock Function)	37
	5.1.12 Inventory Configuration	41
	5.2 Object Management	48
	5.2.1 Viewing Object Details	49
	5.2.2 Uploading Objects	50
	5.2.3 Downloading Objects	54
	5.2.4 Managing Object Metadata	55
	5.2.5 Previewing an Object	59
	5.2.6 Sharing Objects	60
	5.2.7 Creating a Folder	63
	5.2.8 Deleting Objects or Folders	64
	5.2.9 Copying Objects	65
	5.2.10 Moving Objects	66
	5.2.11 Modifying Storage Classes	67
	5.2.12 Searching for a File or Folder	68
	5.2.13 Copy the Object Name	69
6 C	loudtrail	70
	6.1 Management Events Record	70
	6.1.1 View Event Details	71
	6.1.2 Event List	73
	6.2 Trails List	76
	6.2.1 Create Trail	76
	6.2.2 Modify the Trail	78
7 IA	.M	79
	7.1 Getting Started	80
	7.2 IAM Users	84
	7.2.1 Create an IAM User	84
	7.2.2 View and Modify the IAM User	88
	7.2.3 Delete the IAM User	95
	7.2.4 IAM User Login	95
	7.3 IAM User Groups	95
	7.3.1 Create an IAM User Group	95
	7.3.2 View and Modify the IAM User Group	98
	7.3.3 Delete the User Group	101
	7.4 Policy Management	102
	7.4.1 System Policy	102
	7.4.2 Custom Policy	103
	7.4.3 View the Policy Basic Information	116
	7.4.4 Attach Policy	117
	7.5 Security Setting	118
	7.5.1 Password Policy	118
	7.5.2 Login Security Policy	120



7.6 Security Credential	121
7.6.1 Accesskeys	121
7.6.2 Password	122
7.6.3 MFA	122
7.7 Best Practices	124
7.7.1 Recommendations for Using IAM	124
7.7.2 Assigning Permissions to IAM users	125
8 Resource Package	129
9 Appendix	130
9.1 Endpoints	130
9.1.1 Object Storage Network Endpoint	130
9.1.2 Object Storage Network 2 Endpoint	130
9.1.3 Hongkong Endpoint	131
9.2 Action List and Corresponding API	132
9.3 Statement	135
9.3.1 Version	135
9.3.2 Statement	135
9.3.3 Sid	
9.3.4 Effect	136
9.3.5 Action	137
9.3.6 NotAction	137
9.3.7 Resource	138
9.3.8 NotResource	139
9.3.9 Condition	139
9.3.10 IAM Policy Variables	



## 1 Introduce

Object-Oriented Storage (OOS) is a cloud storage service, it provides a massive, flexible, cheap, and highly available storage. You can get an almost unlimited storage space at a low cost. You can adjust the occupation of resources at any time according to your needs, and only pay for the resources that are actually used.

OOS provides two access methods based on Web portal and HTTP REST interface. You can manage and access data through the Internet anywhere. The REST interface provided by OOS is compatible with Amazon S3, so OOS-based businesses can easily interface with Amazon S3.

You can choose to use the **Object Storage Network** in the mainland or **Hongkong** nodes according to your needs.



## 2 Basic Concept

### 2.1 OOS Basic Concept

The main concepts of OOS system are

- Account: The account used by OOS when the user logs in.
- Service: OOS provides services for registered users successfully.
- Object: Each file that the user stores on OOS is an Object.
- Bucket: Container for storing objects.

The relationship between them is shown below.



Before using OOS, you first need to register an Account on the website www.ctyun.cn. After successful registration, OOS will provide a service for the account. Under this service, users can create 1 to 10 Buckets (object containers), and each object container can store an unlimited number of Objects.

#### 2.1.1 Account

Before using OOS, you need to register an Account on the website **www.ctyun.cn**. Email, password and mobile phone number are required when registering. After correctly filling in the required information and conducting real name authentication, contact CTYUN customer service (customer service hotline: 400-810-9889) to apply for OOS service activation. After the activation is successful, you can log in with the account and use the OOS service.

#### 2.1.2 Service

Service is a service provided by OOS for successfully registered users. This service provides users with flexible and expandable storage space. Users can create 1 to 10 object containers (buckets) according to



their business needs.

## 2.1.3 Bucket

Bucket is a container for storing objects. Each Object must be contained in a Bucket. OOS provides is a flat storage method based on buckets and objects. All objects in the bucket are at the same logical level, eliminating the multi-level tree directory structure in the file system.

You can set the properties of the Bucket to control the data storage location, access permissions, lifecycle, etc. These property settings directly affect all objects in the container. You can create different buckets to complete different management functions. Each account can create up to 10 buckets. Users can operate on Buckets only if they have corresponding permissions. This ensures data security and prevents unauthorized users from illegally accessing them.

## 2.1.4 Object

Each file that a user stores in OOS is an Object. The file can be text, image, audio, video or web page. The size of a single object supported by OOS ranges from 1 byte to 5T bytes.

Users can upload, download, delete and share objects. At the same time, users can also manage the organization of objects, move or copy objects to the target directory.

## 2.1.5 Storage Classes

OOS provides two storage classes: **Standard Storage** and **Infrequent Access Storage**. You can choose different storage classes according to different business scenarios.

- The Standard storage has low access latency and high throughput, it can effectively support frequent access to various types of hot data. It is suitable for data storage of various audio and video services, image services, large-scale websites, big data analysis and other applications. If the storage class is not specified when uploading the object, OOS uses Standard storage by default.
- The Infrequent Access storage is suitable for long-term storage of infrequently accessed data. For data that is not frequently accessed but still needs real-time access, Infrequent Access storage can be used, such as long-term backup of various mobile applications, smart devices, and corporate data.
  - Objects stored in Infrequent Access storage have the shortest storage time. When objects with storage time shorter than 30 days are deleted or changed in advance, a certain fee will be incurred.
  - Infrequent access storage objects have a minimum chargeable size, that is, if the size of the object is less than 64KiB, it will be charged according to 64KiB, and the object is greater than or equal to 64KiB according to the actual storage charge.
  - Data restoration fees will be incurred when Infrequent Access storage data is acquired.

#### Comparison of Storage Classes

Compared Item	Standard Storage	Infrequent Access Storage
---------------	------------------	---------------------------



Data Durability         99.999999999999%		99.99999999999%	
Service Availability	99.99%	99.9%	
Minimum chargeable Calculated according to the actual			
size of the object	size of the object	04NIB	
Minimum otorogo timo	No minimum storage time	20 days	
minimum storage time	requirement	30 days	
Data restaration	No data restoration for	Charged according to the actual amount	
Data restoration	no data restoration ree	of data restoration, in GiB	
Data access         Real-time access		Real-time access	
Image processing Supported		Supported	
HTTPS encrypted Supported		Supported	
transmission			
Modify storage classes Supported		Supported	

#### Changing Object Storage Classes

The storage class of object can be changed.

- Change object storage class from Standard storage to Infrequent Access storage: Standard storage can be converted to Infrequent Access storage by setting lifecycle rules or modifying object storage types.
- Change object storage class from Infrequent Access storage to Standard storage: The Infrequent Access storage can be converted to Standard storage by modifying the object storage type, but the Infrequent Access storage cannot be converted to Standard storage through the life cycle.

### 2.1.6 Compliance Retention (Object Lock Function)

OOS provides compliance retention (object lock function) for buckets, that is, after the compliance retention is enabled, no user (including the root user) can modify or delete objects in this bucket that are in the compliance retention (object lock) period.

You can enable the compliance retention for the bucket level according to your needs, and set the compliance retention time in days (Days) or years (years), 1year=365 days. **Note:** 

• Once the compliance retention is enabled, it cannot be disabled, and the compliance retention period cannot be shortened, but the compliance retention period can be extended.



- The compliance retention time is accurate to the second. For example, set the compliance retention time for Bucket A to 10 days. Object A1 belongs to Bucket A. The last update time of A1 is 2019-03-01 12:00:00, and A1 will be pass the ompliance retention period in 2019-03-11 12:00:01.
- No user (including the root user) can modify or delete objects in the compliance retention period.
- Objects in the compliance retention period cannot modify the storage class of the object by calling the API or console, but can only modify the storage classes by modifying the lifecycle.
- The object is in the compliance retention period: If the lifecycle rule is to modify the object storage class, the lifecycle rule can take effect. If the lifecycle rule is to delete the object after expiration, the object must pass the compliance retention period, the lifecycle rule can take effect.

## 2.2 Statistics

Statistics indicates that users can query the usage of buckets and the usage of specified data region. Users can take corresponding measures based on statistical analysis data.

## 2.2.1 Basic Concept

- Internet Direct traffic: Upload and download object through the Internet without internal scheduling of OOS.
- **Non-Internet Direct traffic**: Upload and download object through the Non-Internet (for example Intranet) without internal scheduling of OOS.
- Internet Roaming traffic: Upload and download object through the Internet, and with internal scheduling of OOS.
- **Non-Internet Roaming traffic**: Upload and download object through the Non-Internet (for example intranet), and with internal scheduling of OOS.
- **Deleted capacity**: The size of the deleted objects.

## 2.3 CloudTrail

CloudTrail is an OOS service that helps you record the management events of OOS account, and save the generated trail logs to the specified OOS bucket. The record information includes the identity of the user, the time of request, the source IP address, the request parameters, and the response elements returned by the service.

CloudTrail functions include:

- Management event record: You can view the management events of the last 6 months through CloudTrail, including: log in, log out, view, create, modify, and delete resources.
- Trail logs: When a management event occurs in the OOS account, OOS will match the management event with the configured trail parameters. When the trail parameters match, the management event will be saved in the specified bucket in the form of a log, that is trail logs.



## 2.3.1 Basic Concpet

#### • Management events

Performing bucket operations, management API operations, IAM operations, CloudTrail operations in the OOS account are all management events.

• Read Events

Read events are operations that can view and read resources, but do not modify the resources.

Write Events

Write events are operations that can modify the resources, including creating, modifying and deleting operations.

### 2.4 IAM

Identity and Access Management (IAM) provides identity management and access control service to your OOS services. You can use IAM to create and manage user accounts, and assign permissions to resource. IAM can be used free of charge. You pay only for the resources in your China Telecom Cloud account.

## 2.4.1 Features

As long as you have a China Telecom Cloud account, you can have IAM functions. China Telecom Cloud account administrators can:

- Create and manage sub-user accounts.
- Control the operation permissions of the resources in the sub-user account.
- Assign different permissions to users as needed, so as to avoid sharing resource usage and access key usage with other users, and reduce the information security risk of the account.
- Multi-identity authentication: Through Multi-Factor Authentication (MFA), MFA can be used when performing IAM-related operations, which adds a security guarantee to the operation.

### 2.4.2 Application Scenario

#### **User Management and Decentralization**

There are different staffs in an enterprise with different responsibilities and different authorities. Some staffs need to upload and download objects, some staffs only need to view statistical information, and some staffs only need to view log information. Through IAM, you can assign different operation permissions to different staffs.

### 2.4.3 Basic Concept

#### Root User

When you create a China Telecom Cloud account which you use to sign in to China Telecom Cloud,



you create a China Telecom Cloud account root user identity. When you use your root user credentials, you have complete, unrestricted access to all resources in your China Telecom Cloud account.

#### IAM User

An IAM user which is created by China Telecom Cloud account in OOS is an entity, and it represents the application or person who uses it to interact with OOS. By default, new IAM users have no permission to perform any operation, or access any OOS resource.

#### • User Group

User group is a collection of users. You can add an IAM user to corresponding user groups. By authorizing IAM user group, the permissions of the user group will affect IAM users within user group. It is recommended that IAM users with the same permissions can be added to the same user group. The same IAM user can join multiple user groups at the same time.

#### • MFA

Multi-Factor Authentication (MFA) is a simple and secure secondary authentication method, which adds security protection for users. Only IAM users support MFA.

#### Authorization

Authorization is the process of granting required permissions for a user to perform a task. After a policy is assigned to a user group or user, the user will have permissions to manage resources defined by the policy.

#### • Policy

A policy describes a collection of permission information in a JSON format. And policies can accurately describe the set of resource covered, the set of operations, and authorization conditions. OOS IAM supports the custom policy and system policy:

- **Custom Policy**: The policy is created by the user, and the user can modify and delete the policy.
- **System policy**: The policy is created by the OOS, users can directly use according to their own needs. But the user can only use it and cannot modify the policy.

### 2.4.4 Constraints

There are limited quotas for users and user groups in IAM.

Item	Limit
Number of IAM users	500
Number of custom policy	150
Number of user groups	30
Number of policies attached to an IAM user	10
Number of AK/SK pairs that the root user can create	2
Number of AK/SK pairs that an IAM user can create	2
Number of groups to which an IAM user can be added	10
Number of tags attached to an IAM user	10
Number of policies attached to the IAM group	10



## **3 Account Management**

## 3.1 Activate OOS Service

Contact CTYUN customer service to apply for OOS service activation. Customer service hotline: 400-810-9889.

## 3.2 Enter Object-Oriented Storage Console

You can enter object-oriented storage console through the following methods:

- Click 控制中心 on China Telecom Cloud website, switch language to English, click Object-oriented Storage (Classic Edition) Type I, enter Object-Oriented Storage console.
- Log in to the <u>OOS Document</u> on China Telecom Cloud website, click on 管理控制台 to enter Object-Oriented Storage console.

#### 3.3 Retrieve Password

When a registered user forgets the password, he can click 忘记密码 on the login web to retrieve the password. When retrieving the password, the user needs to follow the prompts and enter the relevant information step by step to retrieve the password.

### 3.4 Logout

For the logged-in account, click the Log Out button to log out of the currently logged-in account.

### 3.5 Region Switch

You can switch the OOS region and jump to a different region according to the selection.

Console	Object Storage Network 2 🔺	Q Search Billing Service Tickets ICP License Supp	ort Cooperation English 🛋 🛑 💬 🕜
III Object-Oriented Storage	China Mainland Object Storage Network Object Storage Network 2 Regions Jiangsu Hangzhou		
Statistics Overview +	Beijing2		Name V Q C
Buckets	Each user can create up to 10 Buckets.		
Cloudtrail -	Bucket Name	Region Creation Date	Operation
~ MAI	uma.	2024-03-13 14:11:14 UTC+0800	Properties Delete
Resource Package	Charles .	2024-03-07 15:11:34 UTC+0800	Properties Delete
	agente.	C 2024-03-08 11:16:07 UTC+0800	Properties Delete
			total 3 10 ~ < 1 >



You can select the **Object Storage Network**, **Object Storage Network 2**, **Hongkong** nodes.

- **Object Storage Network** : Contains multiple regions. The Bucket, Object, and AccessKeyId/SecretAccessKey of these regions can communicate with each other, which can realize the reading and writing of national data nearby.
- **Object Storage Network 2** : Contains multiple regions. The Bucket, Object, and AccessKeyId/SecretAccessKey of these regions can communicate with each other, which can realize the reading and writing of national data nearby.
- Hongkong node: Hongkong nodes include Highquality network and Normal network.



## **4 Statistics Overview**

On the **Statistics Overview**, you can query related information such as capacity, traffic, number of requests, and number of concurrent connections.

**Note**: For IAM users, they can view statistics-related information only if they have the corresponding permissions. The permission required is as follows.

Operation	Permission required
Statistics	statistics:GetAccountStatistcsSummary

#### 4.1 Overview

Click Statistics Overview > Overview to view Statistics Today, including Storage Usage (Standard Storage and Infrequent Access Storage), Traffic Today (Standard Storage and Infrequent Access Storage), Request Today (Standard Storage and Infrequent Access Storage).

- For Traffic Today, you can select Outbound Traffic Over Internet or Inbound Traffic Over Internet. If it is a Hongkong node, you can also select the network type: ALL (the sum of highquality network traffic and normal network traffic), Highquality Network, or Normal Network.
- For **Request Today**, you can select **ALL** (the sum of PUT/POST requests and GET/HEAD requests), **PUT/POST** or **GET/HEAD**.

Object-Oriented Storage	Overview				Collect	on Time:2023-07-11 09:30:00 UTC+0800
Statistics Overview   Overview Statistics Buckets	Statistics Too Occupared with y	ay Standard Storage () 807.81 MB Intrequent Access Storage () 82.29 MB esterday 🕈 0.0%	Traffic Today Standard Storage 1.69 KiB	Outbound Traffic Over Internet $\checkmark$ Intercuent Access Storage <b>OByte</b>	Request Today Standard Storage 11 times	All vitequent Access Storage 0 times
Cloudtrail •	Historical Ke Yesterday	/ Data This Month				
	Data Location	Standard Storage(Peak)	Infrequent Access Storage(Peak)	Outbound Traffic Over Internet	t Number of Reques	ts Restore
	WuHu	OByte	OByte	OByte	Otimes	0Byte
	QingDao	250.01 MiB	80.94 MiB	0Byte	Otimes	OByte
	WuLuMuQi	OByte	OByte	OByte	Otimes	OByte
	ShenYang	OByte	OByte	OByte	Otimes	OByte
	LaSa	0Byte	OByte	OByte	Otimes	0Byte
	SuZhou	OByte	0Byte	0Byte	Otimes	0Byte
	ZhengZhou	557.80 MiB	1.35 MiB	3.19 KiB	37times	0Byte
	ShenZhen	OByte	OByte	OByte	Otimes	OByte
	GuiYang	OByte	OByte	OByte	Otimes	OByte
	LanZhou	OByte	OByte	OByte	Otimes	OByte
	ChengDu	OByte	0Byte	OByte	Otimes	0Byte

Click **Yesterday** or **This month**, you can view yesterday's statistics or this month's statistics. For yesterday, the statistical time range is the data from 00:00-24:00 the day before the current time in Beijing time. For this month, the statistical time range is from 00:00 on the 1st of the current month Beijing time to the last available data at the current time.

Statistical information includes Data Location, Standard Storage (Peak), Infrequent Access Storage (Peak), Outbound Traffic Over Internet, Number of Requests, Restore.



## 4.2 Statistics

## 4.2.1 Storage

Enter the **Statistics**, click **Storage**, you can view the statistical information of the storage capacity usage, including **Billed Storage Usage** and **Actual Storage Usage**.

Statistics	Collection Time:2023-12-07 08:45:00 UTC+0800 C
Storage Deleted Storage Traffic Requests Concurrent Connections Restore	
Time Today Yesterday Last 7 Days Last 30 Days 📄 2023-12-06 — 2023-12-06	By hour V
All Data Locations        All Buckets        Real-time        All Storage Ct	lass V
Billed Storage Usage	Actual Storage Usage
4GiB	600MiB
3GiB	500MiB
2GiB	300Mi8
16iB	200MiB
0088 - 2022-12-06 01:00 2022-12-06 05:00 2023-12-06 09:00 2022-12-06 13:00 2022-12-06 17:00 2023-12-06 21:00	0Mi8 2023-12-66 01:00 2023-12-66 05:00 2023-12-66 05:00 2023-12-66 13:00 2023-12-66 17:00 2023-12-06 21:00 

#### Statistics description of storage

ltem	Description		
Time	he time period for storage capacity query:		
	• Today		
	• Yesterday		
	• Last 7 Days		
	• Last 30 Days		
	• According to the calendar button, select and query the storage in any 90 days		
Query	The time granularity for the storage capacity query:		
	• <b>By 5 minutes</b> : Statistical information is displayed every 5 minutes, you can		
	choose to query Today, Yesterday, or select any day's data according to the		
	calendar.		
	• By hour: Statistical information is displayed every hour, you can choose to		
	query <b>Today</b> , <b>Yesterday</b> , Last 7 Days or select any 7 days of data		
	according to the calendar.		
	• By day: The statistical information is displayed on a daily basis, you can		
	query Today, Yesterday, Last 7 Days, Last		
	<b>30</b> Days or select any 90 days of data according to the calendar.		
Data Location	Data location:		



	• All Data Locations: Show the sum of the storage capacity for all data	
	locations.	
	• Specific data location: Choose according to the displayed data location and	
	view the storage for the selected data location.	
Bucket	Bucket for storage capacity query:	
	• All Buckets: Show the total storage for all buckets.	
	• Specific bucket: Choose according to the displayed bucket and view the	
	storage for the selected bucket.	
Value Type	Value type for storage capacity query:	
	• Average: The average storage of the selected time period can only be	
	queried by hour or by day.	
	• <b>Real-time</b> : Select the real-time value of the sotrage for the time period, and	
	you can choose to query by 5 minutes, query by hour, or query by day.	
	• <b>Peak</b> : The peak storage of the selected time period can only be queried by	
	hour or by day.	
Storage Class	Storage class:	
	• All Storage Class: Show the storage capacity for Standard Storage and	
	Infrequent Access Storage respectively.	
	• Standard Storage.	
	• Infrequent Access Storage.	

You can click the Download button to download the statistical information.

Item	Description		
Date	Time of statistics		
StorageClass	Storage class:		
	• STANDARD: Standard Storage.		
	<ul> <li>STANDARD_IA: Infrequent Access Storage.</li> </ul>		
BilledStorageUsage	Billed storage, the unit is Byte.		
SampleCapacity	Real-time value, the unit is Byte.		
MaxCapacity	Peak value, the unit is Byte.		
AverageCapacity	The average value, the unit is Byte.		
RemainderChargeStorageUsage	The Infrequent Access storage data complement capacity (the		
	sum of the duration complement and the size complement		
	capacity), the unit is Byte.		
RemainderChargeOfDuration	The Infrequent Access storage data storage duration		
	complements the capacity, the unit is Byte.		
RemainderChargeOfSize	The Infrequent Access storage data size complements the		
	capacity, the unit is Byte.		



## 4.2.2 Deleted Storage

Enter the **Statistics**, click **Deleted Storage**, you can view the statistical information of the deleted storage capacity.

tatistics	Collection Time 2023-12-07 08:50:00 UTC+0800
Storage Deleted Storage Traffic Requests Concurrent Connections	Restore
Time Today Yesterday Last 7 Days Last 30 Days 🗎 2023-12-01 All Data Locations V All Buckets V All Storage	—     2023-12-06     By hour     ✓       Class     ✓
Deleted Storage	±
210MiB -	
180MiB-	
150MiB-	
123.38	
90MiB -	2023-12-06 16:00
60Мів -	Standard Storage(Byte): 0     Information Access (Margar(MiP): 114-39
30MiB -	• Thirduett Access Storage (Wild), Theod
0MHB + 2023-12-66 01:00 2023-12-66 03:00 2023-12-66 05:00 2023-12-66 07:00	2023-12-06 (560) 2023-12-06 11:00 2023-12-06 13:00 2023-12-06 16:00 06 17:00 2023-12-06 19:00 2023-12-06 21:00 2023-12-06 23:00

#### Statistics description of deleted storage

Item	Description			
Time	The time period for deleted storage capacity query:			
	<ul><li>Today</li><li>Yesterday</li></ul>			
	• Last 7 Days			
	• Last 30 Days			
	• According to the calendar button, select and query the deleted storage in any			
	90 days			
Query	The time granularity for the deleted storage capacity query:			
	• <b>By 5 minutes</b> : Statistical information is displayed every 5 minutes, you can			
	choose to query Today, Yesterday, or select any day's data according to the			
	calendar.			
	• By hour: Statistical information is displayed every hour, you can choose to			
	query <b>Today</b> , <b>Yesterday</b> , Last 7 Days or select any 7 days of data			
	according to the calendar.			
	• By day: The statistical information is displayed on a daily basis, you can			
	query Today, Yesterday, Last 7 Days, Last 30 Days or select any 90			
	days of data according to the calendar.			
Data Location	Data location:			
	• All Data Locations: Show the sum of the deleted storage capacity for all			
	data locations.			



	• Specific data location: Choose according to the displayed data location and		
	view the deleted storage for the selected data location.		
Bucket	Bucket for deleted storage capacity query:		
	• All Buckets: Show the total storage for all buckets.		
	• Specific bucket: Choose according to the displayed bucket and view the		
	storage for the selected bucket.		
Storage Class	Storage class:		
	• All Storage Class: Show the deleted storage capacity for Standard		
	Storage and Infrequent Access Storage respectively.		
	• Standard Storage.		
	• Infrequent Access Storage.		

You can click the **Download** button to download the statistical information.

Item	Description	
Date	Time of statistics	
StorageClass	Storage class:	
	• STANDARD: Standard storage.	
	<ul> <li>STANDARD_IA: Infrequent Access storage.</li> </ul>	
DeleteStorageUsage(Bytes)	Deleted storage capacity, the unit is Byte.	

## 4.2.3 Traffic

Enter the **Statistics**, click **Traffic**, you can view the statistical information of the traffic, including **Inbound Traffic** and **Outbound Traffic**.

Statistics	Collection Time 2023-12-07 08:55:00 UTC+0800			
Storage Deleted Storage Traffic Requests Concurrent Connections Restore				
Time     Today     Yesterday     Last 7 Days     Last 30 Days     Image: 2023-12-06     By hour     Image: 2023-12-06       All Data Locations     V     All Buckets     V     All Traffic Type     V     Image: 2023-12-06				
Inbound Traffic	Outbound Traffic			
600Mi8	100MiB			
500MiB -	вомів			
400MiB- 35250	60MiB			
2023-12-06 16:00 200468 - Standard Storage (MB): 10.56	40Mi8 -			
100MiB-	20MiB			
OMEB         2023-12-06 0100         2023-12-06 0500         2022-12-06 1100         0         2023-12-06 1100         0         0         0         2023-12-06 1100         0         0         0         0         0         0         0         0	OMB         2022-12-06 01:00         2022-12-06 01:00         2022-12-06 12:00         2022-12-06 12:00           -O-         Standard Storage         -O-         Infrequent Access Storage			

#### Statistics description of traffic

ltem	Description
Time	The time period for traffic query:



	• Today.		
	• Yesterday.		
	• Last 7 Days.		
	• Last 30 Days.		
	• According to the calendar button, select and query the traffic in any 90 days.		
Query	The time granularity for the traffic query:		
	• <b>By 5 minutes</b> : Statistical information is displayed every 5 minutes, you can		
	choose to query <b>Today</b> , <b>Yesterday</b> , or select any day's data according to the		
	calendar.		
	• By hour: Statistical information is displayed every hour, you can choose to		
	query Today, Yesterday, Last 7 Days or select any 7 days of data		
	according to the calendar.		
	• By day: The statistical information is displayed on a daily basis, you can		
	query Today, Yesterday, Last 7 Days, Last 30 Days or select any 90		
	days of data according to the calendar.		
Data Location	Data location for traffic query:		
	• All Data Locations: Show the sum of the traffic of all data locations.		
	• Specific data location: Choose according to the displayed data location and		
	view the traffic of the selected data location.		
Bucket	Bucket for traffic query:		
	• All Buckets: Show the total traffic of all buckets.		
	• Specific bucket: Choose according to the displayed bucket and view the		
	traffic of the selected bucket.		
Traffic Type	The type of traffic statistics (all traffic is a cumulative value)		
	• All Traffic Type: The sum of all traffic, including Internet direct traffic,		
	Internet roaming traffic, Non-Internet direct traffic, and Non-Internet roaming		
	traffic.		
	• Internet Direct: The traffic generated by uploading and downloading		
	object through the Internet without internal scheduling of OOS		
	• Internet Roaming: The traffic generated by uploading and downloading		
	object through the Internet and with internal scheduling of OOS.		
	• Non-Internet Direct: The traffic generated by uploading and downloading		
	object through the Non-Internet (for example Intranet) without internal		
	scheduling of OOS.		
	• Non-Internet Roaming: The traffic generated by uploading and		
	downloading object through the Non-Internet (for example Intranet) and with		
1			
	internal scheduling of OOS.		



•	All Network Quality Type: The sum of the traffic of the High Quality	
	network and the normal network.	
•	High Quality: The traffic of the High Qualit network.	
•	Normal: The traffic of the normal network.	

You can click the **Download** button to download the statistical information.

Item	Description	
Date	Time of statistics	
Region	Data location.	
Bucket	Bucket for traffic query.	
StorageClass	Storage class:	
	• STANDARD: Standard storage.	
	<ul> <li>STANDARD_IA: Infrequent Access storage.</li> </ul>	
NetType	Network type for traffic (only supported byHongkong node):	
	<ul> <li>highqualitynet: The traffic of the High Qualit network.;</li> </ul>	
	<ul> <li>normalqualitynet: The traffic of the normal network.</li> </ul>	
InternetDirectInbound	The Internet direct inbound traffic, the unit is Byte.	
InternetRoamInbound	The Internet roaming inbound traffic, the unit is Byte	
NonInternetDirectInbound	The Non-Internet direct inbound traffic, the unit is Byte.	
NonInternetRoamInbound	The Non-Internet roaming inbound traffic, the unit is Byte.	
InternetDirectOutbound	The Internet direct outbound traffic, the unit is Byte	
InternetRoamOutbound	The Internet roaming outbound traffic, the unit is Byte.	
NonInternetDirectOutbound	The Non-Internet direct outbound traffic, the unit is Byte	
NonInternetRoamOutbound	The Non-Internet roaming outbound traffic, the unit is Byte.	

## 4.2.4 Requests

Enter the Statistics, click Requests, you can view the statistical information of the user requests.





#### Statistics description about the number of requests and return codes

Item	Description		
Time	The time period for querying the number of requests and the number of return		
	codes:		
	● Today		
	• Yesterday		
	• Last 7 Days		
	• Last 30 Days		
	• According to the calendar button, select and query the number of requests		
	and the number of return codes in any 90 days		
Query	The time granularity for the storage capacity query:		
	• <b>By 5 minutes</b> : Statistical information is displayed every 5 minutes, you can		
	choose to query Today, Yesterday, or select any day's data according to the		
	calendar.		
	• By hour: Statistical information is displayed every hour, you can choose to		
	query Today, Yesterday, Last 7 Days or select any 7 days of data		
	according to the calendar.		
	• By day: The statistical information is displayed on a daily basis, you can		
	query Today, Yesterday, Last 7 Days, Last		
Data Location	Data location:		
	• All Data Locations: Show the sum number of requests and the sum		
	number of return codes for all data locations.		
	• Specific data location: Choose according to the displayed data location and		
	view the number of requests and the number of return codes for the selected		
	data location.		
Bucket	Bucket for storage capacity query:		
	• All Buckets: Show the sum number of requests and the sum number of		
	return codes for all buckets.		
	• Specific bucket: Choose according to the displayed bucket and view the		
	number of requests and the number of return codes for the selected bucket.		
Request Type	The request type for querying the number of requests and the number of return		
	codes:		
	• All Requests.		
	• GET.		
	• HEAD.		
	• PUT.		
	• POST.		
	• DELETE.		
	• OTHERS.		



Storage Class	Storage class:			
	•	All Storage Class: Show the number of requests and the number of return		
		codes for <b>Standard Storage</b> and	Infrequent Access Storage	
		respectively.		
	•	Standard Storage.		
	•	Infrequent Access Storage.		

You can click the **Download** button to download the statistical information.

Item	Description
Date	Time of statistics
StorageClass	Storage class:
	• STANDARD: Standard storage.
	<ul> <li>STANDARD_IA: Infrequent Access storage.</li> </ul>
Requests	The number of requests.
Response200	The number of status code 200.
Response204	The number of status code 204.
Response206	The number of status code 206.
Response403	The number of status code 403.
Response404	The number of status code 404.
Response4XX	The number of status code 4XX except status code 403 and status
	code 404.

## **4.2.5 Concurrent Connections**

Enter the **Statistics**, click **Concurrent Connections**, you can view the statistical information of the concurrent connections.

Statistics	Collection Time 2023-12-07 08:55:00 UTC+0800
Storage Deleted Storage Traffic Requests Concurrent Connections Restore	
Time         Today         Yesterday         2023-12-06         By 5 minutes         \thesis	
All Data Locations        All Buckets	
Number of Concurrent Connections	$\star$
2	
1.5-	
1	
0.5	
023-12-06 00:05 2023-12-06 01:40 2023-12-06 03:15 2023-12-06 04:50 2023-12-06 06:25 2023-12-06 08:00 2023-12-06 09:35 2023-12-06 11:10 2023-12-06 12:45 2023-12-06 —O— Number of Concurrent Connections	14.20 2023-12.06 1555 2023-12.06 17.30 2023-12.06 19.95 2023-12.06 20.40 2023-12.06 22:15 2023-12.06

ltem	Description



Time	The time period for concurrent connections query:						
	• Today						
	• Yesterday						
	• According to the calendar button, select and query the concurrent						
	connections in any day						
Data Location	Data location:						
	• All Data Locations: Show the total number of concurrent connections for						
	all data locations.						
	• Specific data location: Choose according to the displayed data location and						
	view the number of concurrent connections for the selected data location.						
Bucket	Bucket for concurrent connections query:						
	• All Buckets: Show the total number of concurrent connections for all						
	buckets.						
	• Specific bucket: Choose according to the displayed bucket and view the						
	number of concurrent connections for the selected bucket.						
Connection Type	Connection type:						
	• All Connections: The total number of the Internet Connetctions and						
	Non-Internet Connections.						
	• Internet Connetctions.						
	<ul> <li>Non-Internet Connections.</li> </ul>						

You can click the **Download** button to download the statistical information.

Item	Description
Date	Time of statistics
Connection	The total number of the Internet Connetctions and Non-Internet
	Connections.
InternetConnection	The number of Ineternet concurrent connetions
NonInternetConnection	The number of non-Internet concurrent connection.

## 4.2.6 Restore

Enter the **Statistics**, click **Restore**, you can view the statistical information of the restore capacity.

#### Statistics Overview



Statis	tics								Colle	ction Time:2023-12-07 08:55:00 UTC	+0800 C
Sto	rage Delete	ed Storage Traffic	Requests Cor	current Connections	Restore						
Tim	e Today	Yesterday Last	7 Days Last 30 Da	ys 🗍 2023	-12-01 —	2023-12-07	By day	$\sim$			
	All Dat	a Locations $\sim$	All Buckets	<ul> <li>✓ All S</li> </ul>	torage Class	$\sim$					
	Restore										$ \pm $
	100MiB										
	80MiB										
	60MiB										
	40MiB										
	20MiB							/	/		
	омів —	2023-12-01	' '	023-12-02	2023-12-0:	3 Infrec	2023-12-04 juent Access Storage	2023-12-05	2023-12-06	2023-12-07	

#### Statistics description of restore capacity

Item	Description						
Time	The time period for restore capacity query:						
	• Today						
	• Yesterday						
	• Last 7 Days						
	▶ Last 30 Days						
	• According to the calendar button, select and query the restore capacity in						
	any 90 days						
Data Location	Data location:						
	• All Data Locations: Show the sum of the restore capacity for all data						
	locations.						
	• Specific data location: Choose according to the displayed data location and						
	view the restore capacity for the selected data location.						
Bucket	Bucket for restore capacity query:						
	• All Buckets: Show the total restore capacity for all buckets.						
	• Specific bucket: Choose according to the displayed bucket and view the						
	restore capacity for the selected bucket.						
Storage Class	Storage class:						
	• All Storage Class: Show the total restore capacity for all storage classes.						
	• Infrequent Access Storage.						

You can click the **Download** button to download the statistical information.

Item	Description
Date	Time of statistics.
StorageClass	Storage class.
RestoreStorageUsage(Bytes)	The restore capacity, the unit is Bytes. The restore capacity from
	Standard storage objects is 0.



## **5 Buckets**

For IAM users, they can operate buckets only if they have the corresponding permissions. The permissions required are as follows.

Operation	Permissions required
Creating a Bucket	oos:PutBucket, oos:GetRegions
	Suggested permission: oos:ListAllMyBucket
View the Bucket list	oos:ListAllMyBucket
Deleting a Bucket	oos:ListAllMyBucket, oos:DeleteBucket
Bucket Properties	oos:ListAllMyBucket, oos:GetBucketAcl, oos:PutBucket
Region Properties	oos:ListAllMyBucket, oos:GetBucketLocation, oos:PutBucket, oos:GetRegions,
	oos:GetBucketAcl
Security Policy	oos:ListAllMyBucket, oos:GetBucketPolicy, oos:PutBucketPolicy,
	oos:DeleteBucketPolicy
Website	oos:ListAllMyBucket, oos:GetBucketWebSite, oos:PutBucketWebSite,
	oos:DeleteBucketWebSite, oos:GetRegions
Logging	oos:ListAllMyBucket, oos:GetBucketLogging, oos:PutBucketLogging
Lifecycle	oos:ListAllMyBucket, oos:GetLifecycleConfiguration, oos:PutLifecycleConfiguration
Cross-Origin Resource	oos:ListAllMyBucket, oos:GetBucketCORS, oos:PutBucketCORS
Sharing (CORS)	
Compliance Retention	oos:ListAllMyBucket, oos:GetBucketObjectLockConfiguration,
	oos:PutBucketObjectLockConfiguration, oos:DeleteBucketObjectLockConfiguration
Inventory Configuration	oos:ListAllMyBucket, oos:PutBucketInventoryConfiguration,
	oos:GetBucketInventoryConfiguration

## 5.1 Bucket Management

## 5.1.1 Creating a Bucket

On the **Buckets** page, when creating a Bucket, you need to enter the bucket name and set its access permission, data location, metadata location.



#### **Create Bucket**

 $\times$ 

 $\hat{}$ 

<ul> <li>Bucket name</li> <li>Bucket name</li> <li>Each labe</li> <li>Each Labe</li> </ul>	must be globally uniqu must be between 3 an must be a series of on el can consist only of lo rel must begin with a lo	ie. d 63 characters long e or more labels,se wercase letters, dig wercase letter or di	g. parated by a single gits, and hyphens (-) git	dot (.).			
<ul> <li>Each Lab</li> <li>Bucket name</li> <li>Bucket name</li> </ul>	el must end with a low must not all be a comb must not contain doub	rercase letter or digit pination of one or mo le dots (), dash dot	t ore sets of "digit.dig ts (), and dot dashe	it" (for example, 192 es ().	2.168.0.1).		
Description o Public-Read- in unexpected Therefore, we to Public-Read: Public-Read: Anyone (inclu permission c Private: Only ti Object). Other	Af access permissi Write: Anyone (includin l access to the bucket a recommend that you o d-Write, please contac Only the account and I/ ding anonymous) can f arefully! he account and IAM us people (including ano	on g anonymous) can r and high costs. Your to not set the bucket t CTYUN customer s AM users with corres read objects in the b ers with correspond nymous) can only a	read/write/delete obj r legitimate rights ar t ACL to Public-Rea service for evaluation sponding permissio pucket. This may res ling permissions ca ccess objects in the	jects in the bucket (ir nd interests may be i d-Write except in spe n and verification bef ons can write/delete o sult in unexpected ac an read/write/delete o bucket if they are au	ncluding Get, Put and nfringed if someone i ecial cases. Note: If yo ore activating this fun objects in the bucket of cess to the bucket an ibjects in the bucket ( thorized by the bucket	Delete Object). Thi uploads illegal info ou want to set acce lotion. (including Put and I id high costs. Pleas including Get, Put a t policy or share a	is may result rmation. ss permission Delete Object). se use this and Delete link.
ket Name		Dublic Dead	O Dublic Deed W	-1-			
a Location	Private	Specify locati	on Re-specify	ite			
	O white hearby	•					
	QingDao	WuHu	WuLuMuQi	ShenYang	LaSa	SuZhou	
	QingDao ZhengZhou	WuHu ShenZhen	WuLuMuQi GuiYang	ShenYang LanZhou	LaSa ChengDu	SuZhou WuHan	
	QingDao ZhengZhou ShangHai2	WuHu ShenZhen	WuLuMuQi GuiYang	ShenYang LanZhou	LaSa ChengDu	SuZhou WuHan	
adata Location	QingDao ZhengZhou ShangHai2 QingDao	WuHu ShenZhen	WuLuMuQi GuiYang	ShenYang LanZhou	LaSa ChengDu	SuZhou WuHan	
adata Location ⑦ a Scheduling ⑦	QingDao ZhengZhou ShangHai2 QingDao	WuHu ShenZhen	WuLuMuQi GuiYang	ShenYang LanZhou	LaSa ChengDu	SuZhou WuHan	

1) Bucket naming convention

The bucket naming convention is as follows:

- Bucket name must be globally unique.
- Bucket name must be between 3 and 63 characters long.
- Bucket name can only consist of lowercase letters, digits, dashes (-) and dots (.).
- Bucket name must be a series of one or more labels, separated by a single dot (.).
  - Each label can consist only of lowercase letters, digits, and hyphens (-).
  - Each Label must begin with a lowercase letter or digit.
  - Each Label must end with a lowercase letter or digit.



- Bucket name must not all be a combination of one or more sets of "digit.digit" (for example, 192.168.0.1).
- Bucket name must not contain double dots (..), dash dots (-.), and dot dashes (.-).
- Illegal sensitive characters are not allowed, such as information related to violence and terrorism.

#### 2) Access permission

OOS provides access permissions. Bucket has three access permissions: public-read-write, private, and public-read:

 Public-Read-Write: Anyone (including anonymous) can read/write/delete objects in the bucket (including Get, Put and Delete Object). This may result in unexpected access to the bucket and high costs. Your legitimate rights and interests may be infringed if someone uploads illegal information. Therefore, we recommend that you do not set the bucket ACL to Public-Read-Write except in special cases.

**Note:** If you want to set access permission to Public-Read-Write, please contact CTYUN customer service for evaluation and verification before activating this function.

- **Public-Read**: Only the account and IAM users with corresponding permissions can write/delete objects in the bucket (including Put and Delete Object). Anyone (including anonymous) can read objects in the bucket. This may result in unexpected access to the bucket and high costs. Please use this permission carefully!
- **Private**: Only the account and IAM users with corresponding permissions can read/write/delete objects in the bucket (including Get, Put and Delete Object). Other people (including anonymous) can only access objects in the bucket if they are authorized by the bucket policy or share a link.

#### 3) Metadata location

The metadata location refers to the position where the metadata of the object is stored. The metadata location is specified when the bucket is created. After the creation is successful, the bucket metadata location cannot be changed.

#### 4) Data Location

The data location refers to the location where the object data is stored,

- Select Write nearby, that is, OOS writes the data to the region closest to the user's access point.
- **Specify location**, OOS will write data to the user-specified region in order, you can select multiple regions.

#### 5) Scheduling strategy

You can also set OOS data scheduling strategy to allow OOS to flexibly handle data location storage:

- Enable data scheduling strategy: OOS can automatically schedule data storage locations according to the actual usage of the user's selected data location, so as to provide users with faster access speed.
- Disabled data scheduling strategy: user data can only be stored in the specified data location.



#### 5.1.2 Bucket List

The bucket list displays all the buckets created by the user and the corresponding bucket information, including the region and creation time.

You can enter the name of the Bucket to be queried in the search box in the upper right corner, supporting fuzzy matching queries.

Object-Oriented Storage	Buckets				
Statistics Overview •	Create Bucket C Each user can create up to 10 Buckets.				
Cloudtrail 🔻	Bucket Name	Region	Creation Date	Operation	
IAM 👻		Object Storage Network	2022-07-05 10:16:25 UTC+0800	Properties Delete	
Resource Package	Contract of the second s	Object Storage Network	2023-04-14 17:55:37 UTC+0800	Properties Delete	
		Object Storage Network	2020-03-16 13:36:20 UTC+0800	Properties Delete	
	united in the second	Object Storage Network	2023-06-16 15:47:24 UTC+0800	Properties Delete	
		Object Storage Network	2023-07-07 14:05:48 UTC+0800	Properties Delete	
	An and Anna Anna Anna Anna Anna Anna Ann	Object Storage Network	2023-03-27 15:34:24 UTC+0800	Properties Delete	
					total 6 10 -> -< 1 >
Item		Description			
Bucket N	lame	Bucket name.			

Bucket Name	Bucket name.
Region	The bucket region, including Object Storage Network, Other
	Regions, Hongkong. Please refer to Region Switch for details.
Creation Date	The time when the bucket was created.
Operation	You can view and modify the properties of the bucket and
	delete it.
	The properties of a bucket include Bucket Properties, Region
	Properties, Security Policy, Website, Logging, Lifecycle, Cross-
	Origin Resource Sharing (CORS), and Compliance Retention.

### 5.1.3 Deleting a Bucket

The user can delete the bucket only when the bucket does not contain any object. Click **Delete** button to delete the bucket.



Buckets			
Create Bucket C Each user can create up to 10 Buckets.			
Bucket Name	Region	Creation Date	Operation
	Object Storage Network	2022-07-05 10:16:25 UTC+0800	Properties Delete
	Object Storage Network	2023-04-14 17:55:37 UTC+0800	Properties Delete
Commenced and	Object Storage Network	2020-03-16 13:36:20 UTC+0800	Properties Delete
	Object Storage Network	2023-06-16 15:47:24 UTC+0800	Properties Delete
	Object Storage Network	2023-07-07 14:05:48 UTC+0800	Properties Delete
	Object Storage Network	2023-03-27 15:34:24 UTC+0800	Properties Delete
			total 6 10 ~ < 1 >

**Buckets** 

When the user clicks **Delete**, the deletion can be performed after a second confirmation in the pop-up window.

0 Delete Bucket		×
Are you sure you want to delete t		
	Cancel	Confirm

### **5.1.4 Bucket Properties**

Click Bucket > Properties > Bucket Properties, view the bucket properties.

Buckets / Properties
Creation Date 2022-07-05 10:16:25 UTC+0800
Bucket Properties         Region Properties         Security Policy         Website         Logging         Lifecycle         Cross-Origin Resource Sharing (CORS)         Compliance Retention         Inventory Configurations
• Note: When creating a new bucket, the default permission is Private, and the user can modify it to other permissions as needed. For details, please refer to the (Object-Oriented Storage API Reference) .
Access Permission   Public-Read  Public-Read  Public-Read  Public-Read-Write
Save

You can modify the access permissions of the bucket on this page:

- **Private**: Only the account and IAM users with corresponding permissions can read/write/delete objects in the bucket (including Get, Put and Delete Object). Other people (including anonymous) can only access objects in the bucket if they are authorized by the bucket policy or share a link.
- Public-Read: Only the account and IAM users with corresponding permissions can write/delete objects in the bucket (including Put and Delete Object). Anyone (including anonymous) can read objects in the bucket. This may result in unexpected access to the bucket and high costs. Please use this permission carefully!



 Public-Read-Write: Anyone (including anonymous) can read/write/delete objects in the bucket (including Get, Put and Delete Object). This may result in unexpected access to the bucket and high costs. Your legitimate rights and interests may be infringed if someone uploads illegal information. Therefore, we recommend that you do not set the bucket ACL to Public-Read-Write except in special cases.

**Note**: If you want to set access permission to Public-Read-Write, please contact CTYUN customer service for evaluation and verification before activating this function.

## **5.1.5 Region Properties**

Click **Bucket** > **Properties** > **Region Properties**, enter **Region Properties** page. You can modify the data location and data scheduling strategy, but you can not modify the metadata location. Note: The Hongkong node only displays **EndPoint**.



## 5.1.6 Security Policy

Click **Bucket** > **Properties** > **Security Policy**, enter **Security Policy** page. In the security policy, you can set the bucket policy to define the access permission of OOS resources. For the detailed bucket policy format, please refer to the *Object-Oriented Storage API Reference*.

**Note**: If the access permission of a bucket is Private or Public-Read, when configuring the policy that allows any user to put objects to the bucket, it is necessary to contact CTYUN customer service for filing.



Buckets / Properties
Creation Date 2022-07-05 10:16:25 UTC-0800
Bucket Properties Region Properties Security Policy Website Logging Lifecycle Cross-Origin Resource Sharing (CORS) Compliance Retention Inventory Configurations
• Note: OOS provides you with the function of object access security policy settings. You can control external access to certain objects by configuring Policy, including restricting the IP range of the access source and Reference header. For more information, please click. View details
Editing Policy

Examples of Bucket Policy are as follows:

1) Referer setting.

Configure the bucket policy for a bucket (named example bucket): Allow a specific sub user (test1, whose root user ID is 32fefj64y54gc) to access this bucket resource, and require the request to include a specific Referer header (http://www.mysite.com/ Or http://mysite.com/).

```
{
  "Version":"2012-10-17",
  "Id":"*",
  "Statement":[
    {
      "Sid":"*",
      "Effect":"Allow",
      "Principal":{ "CTYUN": ["*"] },
      "Action":"oos:GetObject",
     "Resource":"arn:ctyun:oos:::example-bucket/*",
      "Condition":{
       "StringLike":{
         "ctyun:Referer":[
           "https://www.mysite.com/*",
           "https://mysite.com/*"
         ]
       }
     }
   }
  ]
```

2) IP Setting.

If you want to allow only IP addresses in the range of 192.168.143.0/24 to access bucket named example-bucket, but not allow IP addresses 192.168.143.188/32 to access this bucket, you can use the following configuration method.

{



```
"Version": "2012-10-17",
   "Id": "OOSPolicyId1",
   "Statement": [
       {
           "Sid": "IPAllow",
           "Effect": "Allow",
           "Principal": {
              "CTYUN": "*"
           },
           "Action": "oos:GetObject",
           "Resource": "arn:ctyun:oos:::example-bucket/*",
           "Condition" : {
               "IpAddress" : {
                  "ctyun:SourceIp": "192.168.143.0/24"
              },
              "NotIpAddress" : {
                  "ctyun:SourceIp": "192.168.143.188/32"
              }
           }
       }
   ]
}
```



### 5.1.7 Website

Click **Bucket** > **Properties** > **Website**, enter **Website** page. On this page, you can configure the website hosting properties of the bucket. After configuration, users can use the registered static website domain to access the data stored in the bucket. **Note**:

- If static website hosting is configured, when anonymous users directly access the domain name of the storage bucket, the static website files will be downloaded locally. If you want to preview website content instead of downloading static website files when accessing a static website, the static website domain name must be a registered custom domain name bound to the storage bucket. To bind a custom domain name to the storage bucket, please contact CTYUN customer service for application.
- The hosted domain name of the OOS website does not support HTTPS access, and the custom domain name supports HTTPS access. If you want users to access your custom domain name via HTTPS, you need to attach the domain name certificate when you apply to CTYUN customer service for binding your custom domain name. OOS supports the following certificate format: crt+key or PEM. Please ensure that the provided certificate is within its validity period, it is recommended that the certificate be valid for at least 1 year and avoid using free certificates.
- Avoid using "." in the target bucket name, otherwise client verification certificate errors may occur when accessing through https.

Website hosting configuration steps:

- 1) Create a bucket and set Public-Read permission.
- 2) Please contact CTYUN customer service for evaluation and review before binding.
- 3) Add an alias in the domain name management.
  - If you do not use CDN acceleration, add the bucket's CNAME Record Value (*bucketname*.ooswebsite-cn.oos-xx.ctyunapi.cn) as an alias to the domain name management system.
  - If you use CDN acceleration, add the alias provided by the CDN manufacturer to the domain name management system, then configure the CNAME Record Value on the OOS side in the CDN backto-source address, and configure the back-to-source host as your custom domain name (such as yourdomain.com).

**Note**: The Endpoint displayed when the bucket is creating is oos-cn.ctyunapi.cn. The Endpoint is the domain name for the entire object storage network. When the domain name is resolved, it will resolve to different endpoint addresses based on the user data location. If there are multiple data locations when a bucket is created, the system selects the first valid data location as the CNAME Record Value by default (*bucketname.oos-website-cn.oos-xx.ctyunapi.cn*). If only one data location is available when a bucket is created, the CNAME Record Value is *bucketname.oos-website-cn.oos-xx.ctyunapi.cn*). If only one data location is available when a bucket is created, the CNAME Record Value is *bucketname.oos-website-cn.oos-cn.ctyunapi.cn*. Therefore, if you use website hosting, it is recommended that you select the CNAME Record Value of the data location you want to use as the alias in the domain name management system according to the data location in the bucket area property. For example, when you create a bucket, the valid data locations are ShenYang, LanZhou, ChengDu, and GuiYang, and the CNAME Record Value displayed in the bucket is *bucketname.oos-website-cn.oos-website-*



lnsy.ctyunapi.cn. You can set bucketname.oos-website -cn.oos-lnsy.ctyunapi.cn as an alias, you can also use the CNAME Record Value of the domain name of LanZhou, ChengDu or GuiYang as your alias.

4) Upload files.

Upload all the files (html, CSS, js, images, etc.) of the website to the bucket created before, and pay attention to keeping the relative path between the files.

5) Configure Bucket website properties.

Enter the Website, select Enable.

Bu	ckets / Properties								
	-								
	Creation Date 2024-03-1	3 14:11:14 UTC+0800							
	Bucket Properties	Region Properties	Security Policy	Website	Logging	Lifecycle	Cross-Origin Resource Sharing (CORS)	Compliance Retention	Inventory Configurations
	• Note: OOS provides you with a website hosting function. Please decide whether to enable website hosting according to the radio button below. If hosting by "Current Bucket", you need to set the homepage, error page, redirection rules and click Save. If hosting by "Redirection", you need to set the redirected bucket or uri and click Save, and then all requests to the bucket will be redirected to this address. You need to be the the registered custom domain name for the bucket [Please contact CTVUIK customer service for evaluation before activating this function], and then add a CNAME record in the domain name management system, the record value is the following CNAME Record Value (for example: """"""""""""""""""""""""""""""""""""								
	CNAME Record Value			112					
	Website	Enable	e 🔿 Disable						
	Host By	Curren	t Bucket Redirection	n					
	Home Page	Example	e: index.html Only suppor	ts files in the r	oot directory of	the bucket			
	Error Page - optional	Example	e: error.html						
	Redirection Rule - optional	Redirec	tion rules in JSON format						
						11.			
	Save								

#### • Host By Current Bucket

- Home Page: The home page is the page you jump to when you visit the website. For example, if the Home Page is set to index.html, when the website is accessed, the http://yourdomain.com/index.html page will be opened by default.
- Error Page (optional): The error page is the page to jump to when an error occurs when visiting the website. For example, if the Error Page is set to error.html, when an error occurs when accessing the website, it will jump to http://yourdomain.com/error.html.
- Redirection Rule (optional): By configring redirection rules, requests that meet the conditions can be redirected to a specified host or page. The console supports configuring redirection rules in JSON format. Multiple redirection rules can be configured, and each redirection rule has one Condition and one Redirect. E.g:



```
"KeyPrefixEquals": "string"
    },
"Redirect": {
        "HostName": "string",
        "Protocol": "Protocol",
        "ReplaceKeyPrefixWith": "string"
        }
}
```

#### **Description of redirection rules**

Element	Description						
Condition	The Condition element may not be configured. If configure, the containing element cannot						
	be empty.						
	Elements that can be included in Condition: KeyPrefixEquals,						
	HttpErrorCodeReturnedEquals. KeyPrefixEquals is Object name prefix to use when						
	redirecting requests. HttpErrorCodeReturnedEquals is the HTTP error code matched						
	during redirect requests.						
	• When there are multiple values for an element, the last value takes effect.						
	• When both KeyPrefixEquals and HttpErrorCodeReturnedEquals exist, it takes						
	effect only when they need to match at the same time.						
	<ul> <li>If Condition is not configured, it is equivalent to match all rules.</li> </ul>						
Redirect	Redirect must be configured. Redirect can be empty and can contain elements.						
	Elements that can be included in Redirect: Protocol, HostName,						
	ReplaceKeyPrefixWith and ReplaceKeyWith. Protocol is the protocol used when						
	redirecting the request, the value is http or https. HostName is the site name used when						
	redirecting the request. ReplaceKeyPrefixWith is the object name prefix used when						
	describing the redirecting request. ReplaceKeyPrefixWith is the object name used when						
	describing the redirecting request.						
	• When there are multiple values for an element, the last value takes effect.						
	• ReplaceKeyPrefixWith and ReplaceKeyWith cannot exist at the same time.						

 Host By Redirection: You need to set the redirected Bucket access domain name or URL, and all requests to the Bucket will be redirected to this address. For example, if you configure the redirect page to www.example.com, all requests to your domain name (eg http://yourdomain.com) will be redirected to www.example.com.

#### CO 天翼云 State Cloud

#### Buckets / Properties

Creation Date 2024-03-1	-0800
Bucket Properties	erties Security Policy Website Logging Lifecycle Cross-Origin Resource Sharing (CORS) Compliance Retention Inventory Configurations
Note: OOS provides Save. If hosting by * CTYUN customer se webbad curves as	base hosting function. Please decide whether to enable website hosting according to the radio button below. If hosting by "Current Bucket", you need to set the homepage, error page, redirection rules and click ou need to set the redirected bucket or un and click Save, and then all requests to the bucket will be redirected to this address. You need to bind the registered custom domain name for the bucket [Please contact ation and verification before activating this function], and then add a CNAME record in the domain name management system, the record value is the following CNAME Record Value (for example: to divise the website through a custom domain name. For more information, please click to View details
CNAME Record Value	
Website	Enable 🔿 Disable
Host By	Current Bucket Redirection
Redirect To	Enter a bucket access domain name or a URL.


# 5.1.8 Logging

The log function can help you record all operation records. You can enable/disable the log function by clicking the radio button on the right. At the same time, you can also specify the storage location of the log by setting the target bucket and path.

Buckets / Properties	
Creation Date 2022-07-05 10:16:25 UTC+0800	
Bucket Properties Region Properties Security Policy Website	Logging Lifecycle Cross-Origin Resource Sharing (CORS) Compliance Retention Inventory Configurations
• Note: The log function can help you record all operation records. You can enable/	disable the log function by clicking the radio button on the right. At the same time, you can also specify the storage location of the log by setting the target bucket and path.
Log Type Status Prefix	Destination Bucket
Local Log   Enable  Disable log	×
Save	

### 5.1.9 Lifecycle

You can set bucket life cycle rules on this page.

- By setting the bucket lifecycle rules, you can delete objects in the bucket that match the lifecycle rules. When the lifecycle of objects expires, OOS deletes them asynchronously. There may be a delay between the expiration time configured in the lifecycle rule and the actual deletion time. But after the object is deleted after expiration, the user will not need to pay for the expired object. After OOS deletes the expired object, it will record a log in the bucket log, the operation item is OOS.EXPIRE.OBJECT. Note: If the lifecycle rules of an object set the object to be deleted after it expires, the object will be permanently deleted after it expires and cannot be restored
- By setting the bucket lifecycle rules, objects that match the lifecycle rules can be converted from standard storage to infrequent access storage. You can set whether lifecycle rules take effect from the last modification time of the object or from the last access time of the object. After OOS converts the storage class to infrequent access storage, a log will be recorded in the bucket logs, and the operation item is OOS.TRANSITION\_SIA.OBJECT.

Buckets / Properties												
Creation Date 2022-07	-05 10:16:25 UTC+0800											
Bucket Properties	Region Properties	Security Policy	Website	Logging	Lifecycle	Cross-Origin Resource Sharing (C	CORS)	Compliance Retention	Inventory Configurations			
Note: You can set	t bucket lifecycle rules. All (	objects in this bucket th	at meet the spe	cified prefix wil	l be automatical	ly deleted by OOS after a predetermined p	period of tim	IØ.				
Rule Name		Scope			Rula				Status	On	peration	
delete1		Prefix:aa			1. De	lete the object after 60 days since the obje	ect is updati	ed;	Enable	Dis	sable Edit Delete	
Add Rule												



Name Description Rule Name Lifecycle name. The scope of application of the lifecycle rule. Scope Rule The rule detail. Status The status of the lifecycle rule: • Enable: The lifecycle is enabled. Disable: The lifecycle is disabled. • Operation You can enable/disable, edit or delete the specified lifecycle rule.

After clicking Add Rule, add a new lifecycle rule in the pop-up window.

#### Add Lifecycle Rules

<ul> <li>1.Object deletion is</li> <li>2.When the Infrequence</li> <li>See billing standar</li> <li>3.Please make sure</li> <li>4. There may be a comparison</li> </ul>	irreversible, please ent Access Storage ds for details. e that the time of de certain delay when t	configure the object lif class objects are smal leting the object is late he lifecycle policy is ex	ecycle time plan r l or the storage ti than the time of ecuted.	easonably accord me is short, additi converting the sto	ding to your needs. ional costs will be incu orage class of the obje	rred. ct.
Rule Name	Enter rule nar	ne				
Object Transformation Strategy:	Days	Date				
Scope	Prefix	Entire Bucket				
refix	Enter prefix					
ransition to Infrequent access Storage Class	Last N	Nodified time $\smallsetminus$				
ermanently Delete	Last N	Nodified time $\smallsetminus$				
					Cancel	Conf

#### Lifecycle Rules Description

Item	Description
Rule Name	Lifecycle rule name.
<b>Object Transformation Strategy</b>	The strategy for file conversion according to life cycle rules:

×



	• Days: Specifies the number of days from when the objects
	are last modified or last accessed to when the lifecycle rule
	takes effect.
	• Date: Specifies the effective date of the lifecycle rule. OOS
	will execute the lifecycle rule on objects that were last
	modified before this date.
Scope	The scope of application of the lifecycle rule:
	• <b>Prefix</b> : Specifies the object prefix of the lifecycle rule. Only
	objects that match the object prefix can be affected by this
	rule. For objects that do not match the prefix, no lifecycle
	rules are executed.
	• Entire Bucket: The created lifecycle rule applies to all
	objects in the bucket.
Transition to Infrequent	Objects that match the lifecycle rule are converted into Infrequent
Access Storage Class	Access storage objects after expiration.
	• If <b>Object Transformation Strategy</b> is <b>Days</b> , you can
	select:
	Last Modified time: After this number of days since
	the last modified, according to lifecycle rule, the object
	is converted to infrequent access storage class.
	Last Access time: After this number of days since the last access diagonalize to life available when the access to access the second
	last accessed, according to lifecycle rule, the object is
	<ul> <li>If Object Transformation Strategy is Date according</li> </ul>
	to lifecycle rule, the object modified before this date will be
	converted to infrequent access storage class on this date.
Permanently Delete	Objects that match the lifecycle rule will be deleted after
	expiration.
	• If <b>Object Transformation Strategy</b> is <b>Days</b> , after this
	number of days since the last modified, according to lifecycle
	rule, the object will be deleted.
	If Object Transformation Strategy is Date, according to life usely only the object
	to intecycle rule, the object modified before this date will be
	ueieiea.

#### Note:

- If lifecycle rules of the Bucket are modified when the lifecycle rules are being executed, the modification will not take effect until the original lifecycle rules are executed.
- A maximum of 1000 lifecycle rules can be created for each bucket.
- In the same bucket, the lifecycle rules of the same type (deleted after expiration or converted to Infrequent Access storage) cannot have superimposed prefixes. For example, if the prefix of the created lifecycle rule is ABC, then the lifecycle rule with the prefix ABCD or AB or A cannot be created.



 When you set lifecycle rules for the Bucket, these rules will be applied to both existing objects and newly created objects in the future. For example, if you add a lifecycle rule today, and objects with certain prefixes expire after 30 days, OOS will add all objects created 30 days ago to the queue to be deleted.

OOS calculates the expiration time by adding the last modified time or last access time of the object to the lifecycle time, and approximates the time to zero GMT on the next day. For example, if an object is created at 10:30 on January 15, 2016 GMT, with a lifecycle of 3 days, then the expiration time of the object is 00:00 on January 19, 2016 GMT. When modifying an object, OOS will recalculate the expiration time of the object based on the last modified time.

## 5.1.10 Cross-Origin Resource Sharing (CORS)

The browser restricts the initiation of cross-origin HTTP requests within the script, that is, the same-origin policy. For example, when the JavaScript code in the page from the A website wants to visit the B website, the browser will refuse the access because the two websites A and B belong to different domains. By configuring CORS, you can solve the problem of mutual access between different domains. CORS defines the way a client web application interacts with resources in another domain in one domain. The following are examples of using CORS scenarios:

- Scenario 1: Your website www.example.com uses OOS in the backend. The web application provides the function of uploading objects using JavaScript, but in this web application, you can only send requests to www.example.com, and requests sent to other websites will be rejected by the browser. As a result, the data uploaded by users must be transferred from www.example.com. If cross-domain access is set, users can upload directly to OOS without transferring from www.example.com.
- Scenario 2: Assume that the user hosts the website in a bucket named website, and the endpoint of the website is http://website.oos-website-cn.oos-xx.ctyunapi.cn. Now, the user wants to use JavaScript on the web page (stored in this bucket) to send GET and PUT requests to the bucket through the OOS API endpoint oos-xx.ctyunapi.cn. Browsers usually prevent JavaScript from sending these requests, but with CORS, users can configure buckets to support cross-domain requests from website.oos-website-cn.oos-xx.ctyunapi.cn.

Buckets / Properties						
-						
Creation Date 2022-07-05 10:16	:25 UTC+0800					
Bucket Properties Region	n Properties Security Policy Websit	e Logging Lifecycle Cross-Orig	in Resource Sharing (CORS)	Compliance Retention Inventory Config	urations	
Note: You can set cross-orig	gin rules for buckets to solve JavaScript cross-origi	n access issues For more information, please clici	< View details			
ID	Allowed Origin	Allowed Methods	Allowed Headers	Exposed Headers	Max Age Seconds	Operation
1. testcors	•	GET PUT HEAD POST DELETE			5	Edit Delete
Add Cross-Origin Rule						

Click Add Cross-Origin Rule to add a new cross-origin rule:



#### Buckets

 $\times$ 

#### Cross-Origin Rule

<ul><li>① OI</li></ul>						
★ Allowed Origin (?)						11.
* Allowed Methods	GET	D PUT	HEAD	POST	DELETE	
Allowed Headers (?)						li.
Exposed Headers  ?						li.
Max Age Seconds						

Cancel

Item Description ID The unique identification of the rule. The maximum length is 255 characters. Allowed Origin The origin that you want to allow cross-domain requests from. Multiple origins can be set, one per line, each line can have at most one wildcard (\*). Allowed Methods Allowed methods, including GET, PUT, HEAD, POST, DELETE. Allowed Headers Allowed headers. Multiple Headers can be set, one per line, each line can have at most one wildcard (\*). **Exposed Headers** The header that you want customers to be able to access from their applications (for example, from a JavaScript XMLHttpReques object). Multiple exposed Headers can be set, one per line, wildcard (\*). characters are not allowed. Max Age Seconds The time in second of the results returned by the browser's OPTIONS request for a specific resource.

## 5.1.11 Compliance Retention (Object Lock Function)

You can add compliance retention rule on this page and enable the compliance retention function (Object Lock Function). After the compliance retention function is enabled, it will take effect for all objects in the bucket.



uckets / Properties									
Creation Date 2023-06	3-16 15:47:24 UTC+0800								
Bucket Properties	Region Properties	Security Policy	Website	Logging	Lifecycle	Cross-Origin Resource Sharing (C	CORS) Compliance Retent	ion Inventory Configurations	
OOS provides us carefully. See Co	ers with Bucket-level comp mpliance Reservation for d	pliance retention setting details	s. Objects can bi	e created and	accessed during	g the retention period, but objects cannot b	e modified or deleted. Once the set	ting is turned on, it cannot be turned off and the retention	n period cannot be shortened. Please set it
Rule Type				Scope		Rule	Status	Operation	
						There are no compliance retention rul	les for this bucket		

Item	Description
Rule Type	The rule type is Compliance Retention.
Scope	Scope of application of compliance retention rule. Currently, it is the entire bucket.
Rule	Compliance retention period.
Status	Status of compliance retention rule:
	Enable
	Disable
Operation	You can operation the compliance retention rule. Before enabling, the rule can be
	enabled, edited, and deleted. After enabling, it cannot be disabled and deleted, and
	the compliance retention period cannot be shortened, but the compliance retention
	period can be extended.

After the compliance retention function (object lock function) is enabled, no user (including the root user) can modify or delete objects in this bucket that are in the retention period.

You can enable a compliance retention rule as following:

1. Click Add Compliance Retention Rule to add compliance retention, Compliance Retention Rules box will pop up.

If compliance retention has been added and has not been enabled, you can click **Edit** in the **Operation** column to make modifications. If not modified, skip to step 3 to enable compliance retention.



Compliance F	Retention Rules	×
<ol> <li>1.Once open caution.</li> <li>2.The retenti Please set th</li> <li>3. See Comp</li> </ol>	ed, the compliance reservation cannot be closed. Please operate on period of compliance retention can only be extended, not shor re retention period reasonably. pliance Reservation for details.	e with tened.
Rule Type	Compliance Retention	
Scope	Entire Bucket	
Retention Period (day)	Enter the number of days to rete	
	Cancel	Confirm

2. After entering the retention period and clicking **Confirm**, a second confirmation will be made as to whether or not to create the compliance retention.

Compliance Retention Confirmation	×
You are setting up object compliance retention for your Bucket [ 21111] please confirm: 1. The retention period you set for the Bucket is [ 101 ] days. Objects stored within [ 101 ] days from the upload date cannot be changed or deleted. All objects in the Bucket will follow this rule; 2 .After the setting is completed, the compliance retention rules will not take effect immediately, and will only take effect after you enable them. Before enabling, you can also modify and delete the compliance retention rule.	m
Cancel	firm

3. After clicking **Confirm**, a compliance retention is created.

kets / Properties	5									
Creation Date 2023-06	6-16 15:47:24 UTC+0800									
Bucket Properties	Region Properties	Security Policy	Website	Logging	Lifecycle	Cross-Origin Resource Sharing (CORS)	Compliance Retention	Inventory Confi	igurations	
OOS provides us carefully. See Co	sers with Bucket-level comp impliance Reservation for d	bliance retention setting letails	s. Objects can I	be created and	accessed durin	ng the retention period, but objects cannot be modifie	d or deleted. Once the setting	is turned on, it cannot	be turned off and the retention period ca	annot be shortened. Please set it
OOS provides us carefully. See Co Rule Type	sers with Bucket-level comp impliance Reservation for d	vliance retention setting letails	s. Objects can l Scope	be created and	accessed durin	ng the retention period, but objects cannot be modifie	d or deleted. Once the setting	is turned on, it cannot Status	be turned off and the retention period ca	annot be shortened. Please set it
OOS provides us carefully. See Co Rule Type Compliance Retention	eers with Bucket-level comp Impliance Reservation for d	oliance retention setting letails	s. Objects can l Scope Entire Bucl	be created and	accessed durin	ng the refention period, but objects cannot be modifie Rule Retention period 101 days	d or deleted. Once the setting	is turned on, it cannot Status Disable	be turned off and the refention period ca Operation Enable Edit Delete	annot be shortened. Please set it
OOS provides us carefully. See Co     Rule Type     Compliance Retention     Add Compliance Ret	sers with Bucket-level comp impliance Reservation for d n tention Rule	oliance relention setting letails	s. Objects can I Scope Entire Buck	be created and	accessed durin	ng the retention period, but objects cannot be modifie Rule Retention period 101 days	d or deleted. Once the setting	is turned on, it cannot Status Disable	be turned off and the retention period co Operation Enable Edt Delete	annot be shortened. Please set it

After the compliance retention is created, it is disabled by default, and it needs to be enabled by the



user before it can take effect. If the compliance retention function is not enabled, the compliance retention period can be reset.

4. After Clicking **Enable**, a **Compliance Reservation Enabled** box will pop up. You need to enter the bucket name and click **Confirm** to enable the compliance retention rule.

				×	
You are enabling compliance	retention for your Bucke	t [, please confirm:			
1.Once the compliance reser	vation is enabled, <mark>it cann</mark>	ot be closed;			
2.The retention period of com	pliance retention can on	y be extended, not shortened;			
3. The retention period you set for the Bucket is [101] days. Objects stored within [101] days from the upload date cannot be change deleted. All objects in the Bucket will follow this rule;					
Type the name of the bucket.	Compliance retention ru	les have been confirmed to be enabled:			
			Cancel	Confirm	
			Cancel	Confirm	
After clicking <b>Confir</b>	m, the compliance	e retention is enabled.	Cancel	Confirm	
After clicking <b>Confir</b>	m, the compliance	e retention is enabled.	Cancel	Confirm	
After clicking <b>Confir</b> Buckets / Properties	m, the compliance	e retention is enabled.	Cancel	Confirm	
After clicking Confir Buckets / Properties	m, the compliance	e retention is enabled.	Cancel	Confirm	
After clicking Confir Buckets / Properties Creation Date 2023-06-16 15.4724 UTC+0800 Bucket Properties Region Properties Se	m, the compliance	e retention is enabled.	Inventory Configurations	Confirm	
After clicking Confir Buckets / Properties Creation Date 2023-06-16 15:47:24 UTC-8800 Bucket Properties Region Properties Se OCS provides users with Bucket-level compliance carefully. See Compliance Reservation for details	m, the compliance	e retention is enabled.	Cancel Inventory Configurations urred on, it cannot be turned off and the relention	Confirm n period cannot be shortened. Plea	
After clicking Confir Buckets / Properties Creation Date 2023-08-16 15:47:24 UTC-0800 Bucket Properties Region Properties Se Creative See Compliance Reservation for details Rule Type	m, the compliance curity Policy Website Logging 1 retention settings. Objects can be created and ac scope	e retention is enabled.  Jfecycle Cross-Origin Resource Sharing (CORS) Compliance Retention  researed during the retention period, but objects cannot be modified or deleted. Once the setting is in Rule	Cancel       Inventory Configurations       umed on, it cannot be turned off and the retention       Status     Operation	Confirm	
After clicking Confir Buckets / Properties Creation Date 2023-06-16 15:47:24 UTC-0800 Bucket Properties Region Properties Se OCOS provides users with Bucket-level compliance carefully. See Compliance Reservation for details Rule Type Compliance Retention	m, the compliance curity Policy Website Logging I retention settings. Objects can be created and ac Scope Entire Bucket	e retention is enabled.	Inventory Configurations         uned on, it cannot be turned off and the relention         Status       Operation         Enable       Enable       Edit       Delete	Confirm	

Note:

- Once the compliance retention function is enabled, it cannot be disabled, and the compliance retention period cannot be shortened, but the compliance retention period can be extended.
- The compliance retention time is accurate to the second. For example, set the compliance retention time for Bucket A to 10 days. Object A1 belongs to Bucket A. The last update time of A1 is 2019-03-1 12:00:00, and A1 will be pass the compliance retention period in 2019-03-11 12:00:01.
- No user (including the root user) can modify or delete objects in the compliance retention period.



- Objects in the compliance retention period cannot modify the storage class of the object by calling the API or console, but can only modify the storage class by modifying the lifecycle.
- The object is in the compliance retention period: If the lifecycle rule is to modify the object storage class, the lifecycle rule can take effect. If the lifecycle rule is to delete the object after expiration, the object must pass the compliance retention period, the lifecycle rule to take effect.

### 5.1.12 Inventory Configuration

You can use an inventory to obtain information about specific objects in the bucket, such as sizes, storage classes. Compared to the GET Bucket (List Objects) API, the inventory list file can output relevant information of specified objects in CSV format by day or week, without affecting the bucket's request rate. In scenarios where a large number of objects need to be listed, it is recommended to use the bucket inventory function.

**Note**: You can have up to 10 inventory configurations per bucket. The bucket for configuring the inventory and the bucket for storing the inventory list file can be different.

Buckets / Properties						
Creation Date 2022-07-05 10:16:25	UTC+0800					
Bucket Properties Region Pr	operties Security Policy Website	Logging Lifecycle Cros	ss-Origin Resource Sharing (CORS)	Compliance Retention	Inventory Configurations	
Rule Name	Object Prefix	Inventory Storage Bucket	Inventory Path	Frequency	Last Export	Operation
prefix-a	a		/dir1	Weekly	2023-09-14 09:30:15 UTC+0800	Disable Edit Delete
Add Dule						

Name	Description
Rule	The name of the inventory. The name must be unique in the bucket.
Object Prefix	The prefix of the object that matches the inventory configuration rule.
Inventory Storage Bucket	The destination bucket for storing the inventory list file.
Inventory Path	The storage path prefix for the inventory list file.
Frequency	The cycle for exporting the inventory list file.
Last Export	The last time the inventory list file were exported.
Operation	You can disable/enable, edit, and delete inventory configurations.

Click Add Rule, you can add the bucket inventory for the bucket.

 $\times$ 



Ad	d	Ru	le
	_		_

2 When the nu		
2. When the full	mber of objects is greater than 1 billion, it is recommended to export by	
week.		
Rule Name	Enter rule name	
Object Prefix	Enter object prefix	
Object Telix		
Inventory Storage	Select inventory storage bucket $\checkmark$	
Bucket		
Inventory Path	Enter inventory path	
_		
Frequency	O Daliy 💿 Weekiy	
Optional Fields	Object Size	
	Storage Class	
	Last Update Time	
	ETag	
	Multipart Upload	

Note: * indicates a	required field,	and without '	* indicates	an optional field.

Name	Description
Rule Name	The name of the inventory. The name must be unique in the bucket.
	Value: A string whose length is 1 to 64. Only lowercase letters, numbers,
	hyphens (-), and underscores (_) are allowed, and cannot start or end with
	hyphens (-) or underscores (_).
Object Prefix	The prefix of the object that matches the inventory configuration rule.
	Value: The value is a string whose length is 0 to 1024.
Inventory Storage Bucket	The destination bucket for storing the inventory list file.
	The bucket for configuring the inventory and the bucket for storing the
	inventory list file can be different.
Inventory Path	The storage path prefix for the inventory list file.
	• If the inventory list file is directly saved in the bucket root directory, this
	item is not filled in.
	• If you save the inventory list file in a non root directory of the bucket, you
	need to fill in the complete path, excluding the destination bucket name.

Cancel



	For example, save the inventory list file in the dir directory of the bucket
	named example, and fill in dir for this field. If saved in the dir/dir1
	directory of bucket named example, fill in dir/dir1 for this field.
	The value is a string whose length is 0 to 512.
Frequency	The cycle for exporting the inventory list file.
	• Daily: Export the inventory result file by day.
	<ul> <li>Weekly: Export inventory list files by week. On the day when the inventory is enabled, an inventory list export task will be initiated based on the inventory configuration, and a periodic inventory list export task will be initiated the next day. For example, if the inventory is enabled on Monday, the inventory list export task will be activated on Monday, and later on, the inventory list export task will be activated every Tuesday.</li> </ul>
	Note: A new inventory task will only be created after the current inventory list
	file is exported. If there are many objects (with a quantity greater than 1
	billion), it is recommended to export the inventory list file by week.
Optional Fields	<ul> <li>Items included in the inventory file, and multiple items can be specified.</li> <li>Object Size: The size of the object.</li> <li>Storage Class: The storage class of the object.</li> <li>Last Update Time: The last modified time of the object.</li> </ul>
	• ETag: The Etag value of the object, which is used to identify the content
	of the object.
	Multipart Upload: Specifies whether the object is uploaded by using
	multipart upload.
	Note: If no items are specified, the inventory list defaults to outputting the
	source bucket and key (object name).

After you configure an inventory for a bucket, the inventory list file will be output according the specified cycle and the following directory structure:





**Buckets** 

Name	Description				
dest_bucket	The destination bucket for storing the inventory list file.				
destination-prefix	The storage path prefix for the inventory list file. If no inventory path is configured,				
	omit the directory.				
src_bucket	This directory is the source bucket, which is the bucket of the inventory				
	configuration.				
inventory_id	This directory is the inventory name.				
YYYY-MM-DDTHH-	This directory is the time when scanning the source bucket started, with a				
MMZ	Greenwich Mean Time stamp, such as 2023-08-24T16-00Z. This directory				
	contains the manifest.json and manifest.checksum files.				
manifest.json	Provides metadata and other basic information about the inventory, including the				
	MD5 value of the inventory list compressed file. The manifest file that summarizes				
	the inventory list file will only be generated after the inventory list file is generated.				
manifest.checksum	A file containing MD5 values for the manifest.json file.				
data	This directory stores the inventory list files, which are formatted as CSV files				
	compressed using GZIP.				
Note: When there are a large number of objects in the source bucket, OO					
	automatically split the inventory list file into multiple CSV compressed files for				
	downloading and processing. CSV compressed files are incremented in order of				
	uuid.csv.gz, uuid-1.csv.gz, and uuid-2.csv.gz. You can obtain a list of CSV files				
	from the manifest.json file, then extract the CSV files in the above order and read				
	the manifest data. Each object will only appear in one manifest file.				
UUID.csv.gz	The inventory list file, stored in the data folder, contains the file information exported				
	by the inventory function. The report is stored in the format of csv.gz, and there				
	may be multiple inventory list files. For each generated file, a new file is added in				
	the data directory.				

manifest.json: Provides the metadata of inventory lists and related information. An example is as follows.



{

}

#### Description of manifest.json

Name	Description				
destinationBucket	The destination bucket for storing the inventory list file.				
fileSchema	Items included in the inventory file:				
	Bucket: The source bucket.				
	• Key: The object name.				
	• Size: The size of the object.				
	• StorageClass: The storage class of the object.				
	<ul> <li>LastModifiedDate: The last modified time of the object.</li> </ul>				
	• ETag: The Etag value of the object, which is used to identify the content				
	of the object.				
	• IsMultipartUploaded: Specifies whether the object is uploaded by using				
	multipart upload. If uploaded by using multipart upload, the value is				
	TRUE. If not uploaded by using multipart upload, the value is FALSE.				
	Note: The corresponding fields will only appear in the fileSchema when the				
	user has configured Size, StorageClass, LastModifiedDate, ETag,				
	IsMultipartUploaded in the "Optional Fields".				
creationTimestamp	Scan the time of the source bucket, Unix timestamp (UTC), accurate to				



	milliseconds.			
files	The content of the inventory list file:			
	• MD5checksum: MD5 of the inventory list file.			
	• size: The size of the manifest result file, in bytes.			
	• key: The name of the inventory list file name. the format is <i>destination</i> -			
	prefix/src_bucket/inventory_id/data/filename. The destination-prefix will			
	only appear in the path when the use has configured it.			
sourceBucket	The source bucket that configures the inventory.			
version	The inventory version number, the value is 2023-08-30.			
fileFormat	The format of the inventory list file.			

The content of the inventory list file is shown in the following example, which is the example of selecting all optional items in "Optional Fields".

4		Α	В	С	D	E	F	G
1	-		1. txt	6060576	Standard	2023-05-2	(6F7A30A13(	TRUE
2			1%2F	0	Standard	2023-05-2	D41D8CD98F	FALSE
3			1%2F1.txt	5	Standard	2023-05-2	D5397F1491	FALSE
4			1%2F2.txt	3	Standard	2023-05-2	4202CB962A(	FALSE
5			1%2F3.txt	3	Standard	2023-05-2	202CB962A0	FALSE
6			1%2F4.txt	3	Standard	2023-05-2	202CB962A0	FALSE
7	ţ.		1%2F5.txt	3	Standard	2023-05-2	202CB962A0	FALSE
8	1		2%2F	0	Standard	2023-05-2	D41D8CD98I	FALSE
9	8		2%2F1.txt	3	Standard	2023-05-2	202CB962A0	FALSE
10	р.		2%2F2.txt	1	Standard	2023-05-2	C4CA4238A(	FALSE
11	9		2%2F3.txt	3	Standard	2023-05-2	202CB962A(	FALSE
12	9		2%2F4.txt	3	Standard	2023-05-2	202CB962A(	FALSE
13			2%2F5.txt	3	Standard	2023-05-2	202CB962A(	FALSE
14		1	desexampleobject.txt	10	Standard	2023-04-0	350978E62	FALSE
15		3	exampleobject.txt	10	Standard	2023-05-1	350978E62:	FALSE
16		1	wry1%2F12345%2F2023-05-24T16-	32	Standard	2023-05-2	5032104F41	FALSE

The fields in the inventory list file left to right are described as follows.

Field Name	Description
Bucket	The bucket where the object is located.
Кеу	The object name.
	The object name is encoded using URL, and you need to decode and view it.
Size	The size of the object.
StorageClass	The storage class of the object:
	Standard: Standard storage.
	Standard_IA: Infrequent access storage



LastModifiedDate	The last modified time of the object.
ETag	The Etag value of the object, which is used to identify the content of the object.
IsMultipartUploaded	Whether the object is uploaded by using multipart upload.
	TRUE: The object is uploaded by using multipart upload.
	FALSE: The object is not uploaded by using multipart upload.



# 5.2 Object Management

Enter the specified bucket, you can operate the objects.

Buckets / Objects /					
c					
Current Path ef					
Upload Create Folder Download Delete Actions ~				Name 🗸	QC
Name	Size	Storage Class	Last Modified	Operation	
🗌 🛐 u 🧰 1	5.7324 k	Standard Storage	2023-11-30 14:15:08 UTC+0800	Preview Download More ~	
	2.5488 k	Standard Storage	2023-11-30 14:22:08 UTC+0800	Preview Download More ~	
	486 bytes	Standard Storage	2023-11-30 15:18:38 UTC+0800	Preview Download More ~	
	3.9453 k	Standard Storage	2023-11-30 16:05:38 UTC+0800	Preview Download More ~	
	788 bytes	Standard Storage	2023-12-01 10:53:26 UTC+0800	Preview Download More ~	
	487 bytes	Standard Storage	2023-12-04 11:10:26 UTC+0800	Preview Download More ~	
	561 bytes	Standard Storage	2023-12-04 13:46:56 UTC+0800	Preview Download More ~	
Image: A second seco	560 bytes	Standard Storage	2023-12-04 14:16:26 UTC+0800	Preview Download More ~	
	431 bytes	Standard Storage	2023-12-05 09:25:57 UTC+0800	Preview Download More ~	
	3.0566 k	Standard Storage	2023-12-05 09:31:27 UTC+0800	Preview Download More ~	
	486 bytes	Standard Storage	2023-12-05 13:40:53 UTC+0800	Preview Download More ~	
			Display record	is from 1 to 11, total number:11 < <	1 > >>

For IAM users, they can operate objects only if they have the corresponding permissions. The permissions required are as follows.

Operation	Permission
Upload File	oos:ListAllMyBucket, oos:ListBucket, oos:PutObject
DownLoad Object	oos:ListAllMyBucket, oos:ListBucket, oos:GetObject
Managing Object Metadata	oos:ListAllMyBucket, oos:ListBucket, oos:GetObject, oos:PutObject
Preview Object	oos:ListAllMyBucket, oos:ListBucket, oos:GetObject
Share Object	oos:ListAllMyBucket, oos:ListBucket, oos:GetObject
Create Folder	oos:ListAllMyBucket, oos:ListBucket, oos:PutObject
Delete Object	oos:ListAllMyBucket, oos:ListBucket, oos:DeleteObject
Move Object	Permissions required for both source and destination: oos:ListAllMyBucket,
	oos:ListBucket
	Permissions required for the source: oos:GetObject, oos:DeleteObject
	Permissions required for the destination: oos:PutObject
Modifying Storage Classes	oos:ListAllMyBucket, oos:ListBucket, oos:GetObject, oos:PutObject
Copy Object	Permissions required for both source and destination: oos:ListAllMyBucket,
	oos:ListBucket
	Permissions required for the source: oos:GetObject
	Required permissions for the destination: oos:PutObject
Search File	oos:ListAllMyBucket、oos:ListBucket



# 5.2.1 Viewing Object Details

On the **Buckets** page, click on the corresponding bucket to enter the **Objects** page. Click on the specific object to view the detailed information of the object.

В	uckets / Objects / Ob	bject Details /							
	Current Path Commonwerk /	iconta					Dow	mload Copy To Move To	
	Object overview								
	Storage region				Object name				
	Last modified	2023-11-30 14:15:08 UTC+	0080		URI	https://oos	00_1 🗇		
	Size	5.7324 k							
¢	Storage class Learn more							Edit	
	Storage class	Standard Storage							
	Metadata Metadata is option	nal information provided as a r	name-value (key-value) pair.					Edit	
	Туре		Кеу	Value					
	System defined		Content-Type	application/octet-stream					

Item	Description
Object overview	You can view the following information:
	<ul> <li>Storage region The data location where object is stored</li> </ul>
	Object name.
	<ul> <li>Last modified: The last modification time of the object.</li> </ul>
	URI: The specific URI of the object.
	• Size: The size of the object.
Storage class	The storage class of the object:
	Standard Storage.
	Infrequent Access Storage.
Metadata	The specific metadata information of the object. For more metadata information,
	please refer to Managing Object Metadata.



# 5.2.2 Uploading Objects

Note:

- You can upload objects via the console, or upload objects via the API. The size of objects uploaded via the console is limited, and an object cannot exceed 5GiB. If you need to upload an object larger than 5GiB, you can upload it via the API.
- Upload objects via the console, supporting up to 500 objects to be uploaded simultaneously.
- When uploading a object, if an object with the same name is encountered, the newly uploaded object will overwrite the original object.

On the **Buckets** page, click on the corresponding bucket to enter the **Objects** page, you can upload objects.

Click **Upload**, a pop-up window will appear for uploading files, select the storage class (**Standard Storage** or **Infrequent Access Storage**), and then upload the files.

#### **Buckets**



Jpload File					×
<ol> <li>Note: Object</li> </ol>	with the same n	ame under the bu	ucket will be overwritten		
Current Path	testw3/				
Storage Class Standard Sto	orage 🔿 In	frequent Access S	Storage		
Select File ᠀					
	Drag the S	e directory or mult Support up to 500	tiple files here, or click or cl files to upload at the same	idk Add files time	
Remove	Add files	Add folder		Search by file nar	ne Q
Name		Size	Folder	Object	Гуре
			No Data		
				total 0 5 ~	< 1 >
Metadata 🕐					
Туре	Key	1	Value		Operation
			No Data		
Add metadata	2				
Upload	Cancel				

ltem	Description
Current Path	The location of the files upload.
Storage Class	The storage class of files:
	• <b>Standard Storage</b> : The Standard storage has low access latency and high
	throughput, it can effectively support frequent access to various types of hot
	data. It is suitable for data storage of various audio and video services, image
	services, large-scale websites, big data analysis and other applications. If the
	storage class is not specified when uploading the object, OOS uses Standard
	storage by default.



	• Infrequent Access Storage: The Infrequent Access storage is suitable for							
	long-term storage of infrequently accessed data. For data that is not							
	frequently accessed but still needs real-time access, Infrequent Access							
	storage can be used, such as long-term backup of various mobi applications, smart devices, and corporate data.							
	Objects stored in Infrequent Access storage have the shortest storage							
	time. When objects with storage time shorter than 30 days are deleted or							
	changed in advance, a certain fee will be incurred.							
	<ul> <li>Infrequent access storage objects have a minimum chargeable size, that</li> </ul>							
	is if the size of the object is less than 64KiB it will be charged according							
	to 64KiB and the object is greater than or equal to 64KiB according to							
	the actual storage charge							
	Detersection for will be incurred when lafer went Assess stores.							
	Data restoration rees will be incurred when infrequent Access storage							
	data is acquired.							
Select File	You can upload files by dragging the directory or multiple files to the floating							
	window, or by clicking the Add files or Add folder button.							
	Support up to 500 files to upload at the same time.							
	If you want to remove files that will be uploaded, you can select the corresponding							
	files and click the <b>Remove</b> button to remove the files.							
	Explanation: You can use fuzzy matching to search for files that will be uploaded.							
Metadata	You can edit the metadata information of files that will be uploaded. For more							
	metadata information, please refer to Managing Object Metadata.							

You can upload files in the following ways:

- Drag a local directory or multiple files to the floating window, and the file you dragged into the floating window will be automatically uploaded to OOS from the service portal, and the directory hierarchy when you upload is retained.
  - For example: upload a photo file to OOS, the directory structure of photo is as follows:
  - photo/20190101/1.jpg
  - photo/20190102/2.jpg

After uploading to OOS, the directory hierarchy at the time of upload is retained, and the directory structure is as follows:

photo/20190101/1.jpg

Photo/20190102/2.jpg

- Click Add files, and a dialog box for uploading files will pop up. You can select one or more objects to upload.
- Click Add folder, and a dialog box for uploading folder will pop up. You can select the folder you want to upload.

During files upload process, you can view the upload status of each file:



- When the file is uploading, the status is the progress of file upload.
- The file has not started uploading yet, the status is Waiting.
- The file was successfully uploaded, the status is **Uploaded Successfully**.
- The file was unsuccessfully uploaded, the status is **Uploaded Failed**.

Upload File		- ×
File Name	Size	Status
( ,,	25.8142 M	26%
and the second sec	635.6377 k	Uploaded Successfully
	79.4805 M	9%
	19.5534 M	5%
	85.8825 M	10%

During the upload process, if the upload dialog box is closed, a prompt message box will pop up.

- **Confirm:** Terminate uploading files.
- Cancel: Continue uploading files.

Prompt		×
The object is uploading. A close?	Are you sure yo	u want to
	Cancel	Confirm



# 5.2.3 Downloading Objects

On the **Buckets** page, click on the corresponding bucket to enter the **Objects** page, you can download objects.

Select one or more objects and click **Download** to download a single object or batch objects.

Buckets / Objects /					
inviting 1					
Current Path Concest.					
Upload Create Folder Download Delete Actions	$\sim$		Ν	Jame 🗸	QC
Name	Size	Storage Class	Last Modified	Operation	
	25.8142 M	Infrequent Access Storage	2023-12-06 15:52:23 UTC+0800	Preview Download More $\!$	
Sector 2010 100 100 100 100 100 100 100 100 10	260.5884 M	Infrequent Access Storage	2023-12-06 15:52:23 UTC+0800	Preview Download More $\!$	
	84.7243 M	Infrequent Access Storage	2023-12-06 15:52:32 UTC+0800	Preview Download More $\!$	
	26.4365 M	Infrequent Access Storage	2023-12-06 15:52:35 UTC+0800	Preview Download More $\!$	
	635.6377 k	Infrequent Access Storage	2023-12-06 15:52:23 UTC+0800	Preview Download More $\!$	
			Display records fr	rom 1 to 5, total number:5 << <	1 > >>



# 5.2.4 Managing Object Metadata

Metadata is a description of the properties of a file, including system metadata and user metadata. You can manage the properties of files by editing metadata.

#### System metadata that users can modify

Note: Please fill in the system defined metadata values according to the HTTP standard.

Field	Description		
Cache-Control	The caching behavior of the object.		
	Value:		
	• no-cache: When you access a cache object, the server checks whether		
	the file has been updated. If the file has been updated, it indicates that		
	the local cache has expired and the file needs to be downloaded again		
	from the server. If the file has not been updated, it indicates that the		
	local cache has not expired, and the local cache is used at this time.		
	<ul> <li>no-store: The file will not be cached.</li> </ul>		
	• public: Files are allowed to be cached by any intermediary (possibly a		
	proxy server, similar to a CDN network).		
	• private: The file can only be cached by its terminal. It does not allow		
	any intermediaries to cache the corresponding resources.		
	<ul> <li>max-age=<seconds>: The relative expiration time of cache files,</seconds></li> </ul>		
	measured in seconds. This option is only available in HTTP 1.1.		
Content-Disposition	The presentation format of the file.		
	Value:		
	• Content-Disposition:inline: You can preview the file content directly.		
	<ul> <li>Content-Disposition:attachment: The file is downloaded to the</li> </ul>		
	specified path in the browser according to the original file name.		
	• Content-Disposition:attachment; filename="FileName": The file will be		
	downloaded to the specified path in the browser with the custom file		
	name.		
	FileName specifies the custom name of the downloaded object, such		
	as example.jpg.		
	When downloading files to the specified path in the browser:		
	<ul> <li>If the file name contains special characters such as asterisks (*)</li> </ul>		
	and forward slashes (/), special character escape may occur. For		
	example, when downloading <b>test</b> * <b>. jpg</b> locally, it may be		
	escaped as <b>test. jpg</b> .		
	• To ensure that the file name containing Chinese characters does		
	not appear garbled after downloading to the specified local path.		



	you need to encode the Chinese characters in the name into a
	URL. For example, after downloading "中文 <b>.txt</b> " from OOS to the
	local location, it is necessary to keep the file name as "中文 <b>.txt</b> "
	and set the Content Disposition format according to "attachment;
	file name="+URLEncoder. encode ("中文", "UTF-8")+". txt; file
	name *=UTF-8"+URLEncoder. encode ("中文", "UTF-8")+". txt",
	that is, attachment; File name=% E4% B8% AD% E6% 96%
	87.txt; Filename *=% E4% B8% AD% E6% 96% 87.txt.
Content-Encoding	The encoding method for the file. It is necessary to fill in according to the
	actual encoding type of the file, otherwise it may cause the client (browser)
	to fail to parse the encoding or file download. If the file is not encoded, this
	item will not be added.
	Value:
	<ul> <li>identity: The file has not been compressed or encoded.</li> </ul>
	• gzip: The file is encoded using Lempel Ziv (LZ77) compression
	algorithm and 32-bit CRC verification.
	• compress: The file is encoded using the Lempel Ziv Welch (LZW)
	compression algorithm.
	• deflate: The file is encoded using the zlib structure and deflate
	compression algorithm.
	<ul> <li>br: The file is encoded using the Brotli algorithm.</li> </ul>
	The default value is identity.
	For more information about Content Encoding, please refer to <u>RFC2616</u> .
Content-Type	The content type of the file.
	It is used to define the type of file and the encoding of the webpage. If no
	file type is specified, a value is generated based on the extension of the
	file name. If the file name does not have an extension, the default value for
	the file type is application/octet stream.
Content-Language	The language of the file. For example, if a file is written in Simplified Chinese,
	this option can be set to zh-CN.
Expires	The expiration time of cached content, in Greenwich Mean Time (GMT)
	format
	For example, Wed, 22 Nov 2023 14:18:58+0800. If Cache Control is set to
	max age= <seconds>, take max age=<seconds>as the standard.</seconds></seconds>
x-amz-website-redirect-location	Redirect requests for associated files to other files in the same bucket or
	external URLs. This value is unique for each individual file and will not be
	copied under the original setting. For more information, please refer to
	POST Object.



#### User metadata that users can modify

Field	Description
x-amz-meta-*	User metadata. The key must be a partial value of printable characters in ASCII.
	Unsupported characters can be found in the table below. The value is a character
	within ISO 8859-1, excluding (space).

#### Values that cannot be taken from 95 ASCII printable characters.

ASCII Decimal	Graphical	ASCII Decimal	Graphical
32	(space)	61	=
34	n	62	>
40	(	63	?
41	)	64	@
44	3	91	[
47	/	92	1
58	:	93	]
59	•	123	{
60	<	125	}

Click on **More>Edit metadata** in the **Operation** list or click **Actions>Edit metadata** in the navigation bar to edit object metadata.

**Note**: If multiple objects are selected to edit metadata at the same time, the original metadata information of the objects will not be displayed. If there is a key in the object that already has metadata and is the same as the key used to add metadata this time, its value will be updated to the latest value, and all other historical metadata in the file will be retained.



**Object metadata** 

#### Buckets

×

Cancel

~

2. It is recommende them yourself first, o	d to use digits and letters for keys therwise the information may be lo	and values. If you need to use other characters, plost.	ease encode
ect ne			
ype	Кеу	Value	Operation
ystem defined $\smallsetminus$	Content-Type 🗸	application/x-zip-compressed	Remove

### Click Add metadata, you can modify the system metadata or user metadata.

Items	Description		
Туре	The type of the object metadata:		
	• System defined: system metadata.		
	• User defined: user metadata.		
Кеу	The specific metadata:		
	If the type is <b>System defined</b> , values:		
	Cache-Control		
	Content-Disposition		
	Content-Encoding		
	Content-Type		
	Content-Language		
	• Expires		
	• x-amz-website-redirect-location		
	If the type is <b>User defined</b> , the value is x-amz-meta-*.		
Value	The value of the specific metadata.		
Operation	Click <b>Remove</b> , you can delete the metadata.		



# 5.2.5 Previewing an Object

On the **Buckets** page, click on the corresponding bucket to enter the **Objects** page. Click **Preview** button of the object to preview the object.

**Note**: When the previewed object is a picture or webpage, it will be downloaded to the local as an attachment.

в	uckets / Objects / V					
	wl2022					
	Current Path					
	Upload Create Folder Download Delete Actions	~			Name 🗸	QC
	Name	Size	Storage Class	Last Modified	Operation	
•						
		10.5398 M	Standard Storage	2023-12-06 15:21:35 UTC+0800	Preview Download More ~	
	Summer.	79.4805 M	Standard Storage	2023-12-06 14:33:00 UTC+0800	Preview Download More ~	
	□ <b>8</b>	19.5534 M	Standard Storage	2023-12-06 14:33:00 UTC+0800	Preview Download More ~	



## 5.2.6 Sharing Objects

On the **Buckets** page, click on the corresponding bucket to enter the **Objects** page, you can share one or multiple objects.

Note: When sharing pictures or webpages, visitors will download them locally for viewing.

### 5.2.6.1 Share an Object

Select the object, click on **More>Share** in the **Operation** list or click **Actions>Share** in the navigation bar to share the object.

в	Buckets / Objects /					
	energie -					
	Current Path					
	Upload Create Folder Download Delete Actions	~			Name 🗸	QC
	Name	Size	Storage Class	Last Modified	Operation	
4						
		10.5398 M	Standard Storage	2023-12-06 15:21:35 UTC+0800	Preview Download More	
		79.4805 M	Standard Storage	2023-12-06 14:33:00 UTC+0800	Preview ( Share	
		19.5534 M	Standard Storage	2023-12-06 14:33:00 UTC+0800	Preview C	

Click Share button and Object Share dialog box will pop up.



 $\times$ 

#### **Object Share**

Object Name	
Expiration Time (day)	1
Download Speed Limit	Enable Disable
Speed (KiB/s)	100
Download Concurrent Limit	Enable Disable
Concurrency	220
Link	https://oos-cn.ctyunapi.cn/
	Create Copy

Name	Description		
Object Name The name of the object to be shared.			
Expiration Time (day)	Set expiration time.		
	The value range is [1, 9999999], and the unit is days.		
	Note: If left blank, the sharing link will expire in 15 minutes by default.		
Download Speed	Whether to enable the download speed limit:		
Limit	Enable		
	Disable		
Speed (KiB/s)	Set download speed limit.		
	The value range is [1, 2147483647], and the unit is KiB/s.		
Download	Whether to enable the download concurrent limit:		
Concurrent Limit    Enable			
	Disable		
Concurrency	Set download concurrent limit:		
	The value range is [1, 2147483647].		
Link	The sharing link of the object.		

Click the **Create** button to generate a URL with signature authentication. The user can directly share the URL with others, and within the validity period, the object can be accessed through the URL.



### 5.2.6.2 Share Multiple Objects

Select multiple objects, click **Actions**>**Share** in the navigation bar to share objects, **Object Share** dialog box will pop up.

Object Share		
Expiration Time	1	
(day)		
Download Speed Limit	Enable	Disable
Speed (KiB/s)		
Download Concurrent Limit	Enable	Disable
Concurrency		

Create

Name	Description			
Expiration Time (day)	Set expiration time.			
	The value range is [1, 9999999], and the unit is days.			
	Note: If left blank, the sharing link will expire in 15 minutes by default.			
Download Speed	Whether to enable the download speed limit:			
Limit	Enable			
	Disable			
Speed (KiB/s)	Set download speed limit.			
	The value range is [1, 2147483647], and the unit is KiB/s.			
Download Whether to enable the download concurrent limit:				
Concurrent Limit	Enable			
	Disable			
Concurrency	Set download concurrent limit:			
	The value range is [1, 2147483647].			

Clicking the **Create** button will generate a CSV file, in which users can view the specific sharing links for each file.



### 5.2.7 Creating a Folder

On the **Buckets** page, click on the corresponding bucket to enter the **Objects** page. Click **Create Folder** and set the name of the folder to be created in the pop-up window. The created folder can contain Object. The folders here are not the concept of folders in the file system. In order to facilitate user data management, OOS provides a method to simulate folders. In OOS, an object is simulated as a folder by adding a slash (/) to the end of the object name on OOS Console. If you call the API to list objects, paths of objects are returned. In an object path, the content following the last slash (/) is the object name. If a path ends with a slash (/), it indicates that the object is a folder. The hierarchical depth of the object does not affect the performance of accessing the object.

Folder naming rules:

- The name is not empty.
- The name cannot contain the following special characters: ? ":/'\;
- The name cannot start or end with a vertical bar ().
- The name cannot be: dots (.) Or plus (+).

Buckets / Objects /				
Current Path				
Upload Create Folder Download Delete Actions	~		1	lame v Q C
Name	Size	Storage Class	Last Modified	Operation
Survey ozoozer enterner owner.	25.8142 M	Infrequent Access Storage	2023-12-06 15:52:23 UTC+0800	Preview Download More ~
	260.5884 M	Infrequent Access Storage	2023-12-06 15:52:23 UTC+0800	Preview Download More ~
	84.7243 M	Infrequent Access Storage	2023-12-06 15:52:32 UTC+0800	Preview Download More ~
	26.4365 M	Infrequent Access Storage	2023-12-06 15:52:35 UTC+0800	Preview Download More ~
	635.6377 k	Infrequent Access Storage	2023-12-06 15:52:23 UTC+0800	Preview Download More ~
			Display records fr	om 1 to 5, total number:5 << < 1 > >>



### 5.2.8 Deleting Objects or Folders

There are two ways to delete objects or folders:

Manually delete objects or folders through the console: On the Buckets page, click on the corresponding bucket to enter the Objects page. Select the objects or folders to be deleted and click Delete. When deleting objects or folders, users need to make a second confirmation to prevent accidental deletion.

Buckets / Objects /		
testoos1 Current Path		
Upload Create Folder Download Delete Actions V		Name v Q C
Name Size	Storage Class	Last Modified Operation
Belete object	Infrequent Access Storage	2023-12-06 15:52:23 UTC+0800 Preview Download More ~
If you want to delete the folder, please do not refresh or close the page when the folder is	Infrequent Access Storage	2023-12-06 15:52:23 UTC+0800 Preview Download More >
being deleted, otherwise the task may be interrupted. It will take some time to delete a folder. Please do not write objects to the folder during the deletion process, otherwise	Infrequent Access Storage	2023-12-06 15:52:32 UTC+0800 Preview Download More ~
the object may be deleted.	Infrequent Access Storage	2023-12-06 15:52:35 UTC+0800 Preview Download More ~
Cancel Confirm	Infrequent Access Storage	2023-12-06 15:52:23 UTC+0800 Preview Download More ~
		Display records from 1 to 5, total number 5 $\ \ll \ \ 1 \ \ > \ >$

• Delete objects or folders by configuring lifecycle rules, as detailed in Lifecycle chapter.





# 5.2.9 Copying Objects

On the **Buckets** page, click on the corresponding bucket to enter the **Objects** page. Select objects to be copied, click **Actions**>**Copy To** in the navigation bar, **Object Copy** window will pop up, and you can copy selected objects to other buckets.

**Note**: Using the console operation, the single object copied is no larger than 5 GiB. If it exceeds 5 GiB, please call the API interface **PUT Object -Copy** or **Copy Part** to operate.

Buckets	/ Objects /					
testoo Current l	s1 Path					
Upload	d Create Folder Download Dele	Actions				Name v Q C
. N	lame		Size	Storage Class	Last Modified	Operation
	Object Copy	×	5.8142 M	Infrequent Access Storage	2023-12-06 15:52:23 UTC+0800	Preview Download More ~
	Copy to		60.5884 M	Infrequent Access Storage	2023-12-06 15:52:23 UTC+0800	Preview Download More ~
•			4.7243 M	Infrequent Access Storage	2023-12-06 15:52:32 UTC+0800	Preview Download More ~
			6.4365 M	Infrequent Access Storage	2023-12-06 15:52:35 UTC+0800	Preview Download More ~
			35.6377 k	Infrequent Access Storage	2023-12-06 15:52:23 UTC+0800	Preview Download More ~
					Display records	from 1 to 5, total number:5 $\ll$ < 1 $>$ >>
		Cancel Confirm				



## 5.2.10 Moving Objects

On the **Buckets** page, click on the corresponding bucket to enter the **Objects** page. Select objects to be moved, click **Actions**>**Move To** in the navigation bar, **Object Move** window will pop up, and you can move selected objects to other buckets.

**Note**: Using the console operation, the single object moved is no larger than 5GiB. If it exceeds 5GiB, please call the API interface **PUT Object -Copy** or **Copy Part**, DELETE Object to operate.

Buckets	s / Objects /					
Curre	ost 1 Path					
Uplo	ad Create Folder Download D	Actions ~	/		1	lame v Q C
	Name		Size	Storage Class	Last Modified	Operation
	Object Move	×	5.8142 M	Infrequent Access Storage	2023-12-06 15:52:23 UTC+0800	Preview Download More ~
	Copy to		60.5884 M	Infrequent Access Storage	2023-12-06 15:52:23 UTC+0800	Preview Download More ~
			4.7243 M	Infrequent Access Storage	2023-12-06 15:52:32 UTC+0800	Preview Download More ~
			6.4365 M	Infrequent Access Storage	2023-12-06 15:52:35 UTC+0800	Preview Download More ~
			35.6377 k	Infrequent Access Storage	2023-12-06 15:52:23 UTC+0800	Preview Download More ~
					Display records fr	om 1 to 5, total number:5 $\ll$ $<$ $1$ $>$ $>$
		Cancel Confirm				



### 5.2.11 Modifying Storage Classes

On the **Buckets** page, click on the corresponding bucket to enter the **Objects** page. Select objects that need to modify their storage type, click **Actions**> **Modify Storage Class** in the navigation bar, **Modify Storage Class** window will pop up, and you can modify storage classes for selected objects.

- Standard storage: High performance, data will be accessed frequently.
- Infrequent access storage: Long-term data storage, low access frequency, requiring real-time access.

Buckets	/ Objects / · · ·		
	4		
Current	ath		
Upload	Create Folder Download Delete Actions V		Name v Q C
N	Modify Storage Class	Storage Class	Last Modified Operation
		Infrequent Access Storage	2023-12-06 15:52:23 UTC+0800 Preview Download More ~
	You can modify the storage class of the selected object.	Infrequent Access Storage	2023-12-06 15:52:23 UTC+0800 Preview Download More >
•		Infrequent Access Storage	2023-12-06 15:52:32 UTC+0800 Preview Download More ~
	Storage Class Standard Storage Infrequent Access Storage	Infrequent Access Storage	2023-12-06 15:52:35 UTC+0800 Preview Download More >
	Infrequent Access Storage: Long-term data storage, low access frequency requiring	Infrequent Access Storage	2023-12-06 15:52:23 UTC+0800 Preview Download More ~
	real-lime access.		Display records from 1 to 5, total number 5 $~\ll~<~1~~>~~\gg~$
	Cancel Contirm		



# 5.2.12 Searching for a File or Folder

On the Buckets page, click on the corresponding bucket to enter the Objects page.

When there are many stored objects, you can search for the eligible files and folders by searching for the object prefix.

Buckets / Objects /				
Current Path				
Upload Create Folder Download Delete Actions	×			Name V N Q C
Name	Size	Storage Class	Last Modified	Operation
Name	Size 260.5884 M	Storage Class	Last Modified	Operation 00 Preview Download More ~
Name	Size 260.5884 M	Storage Class	Last Modified 2023-12-06 15:52:23 UTC+00 Display rec	Operation           000         Preview Download More ~           ords from 1 to 1, total number: 1 << < 1 > >>
Name	Size 260.5884 M	Storage Class	Last Modified 2023-12-06 15:52:23 UTC+00 Display rec	Operation Preview Download More   prds from 1 to 1, total number:1   Classical   Preview Download More   Preview Download More


## 5.2.13 Copy the Object Name

On the **Buckets** page, click on the corresponding bucket to enter the **Objects** page.

When you need to copy the object name, you can place the mouse on the object to be copied, a copy

button (  $\square$  ) will appear next to the object name, click this button to copy the object name.

Buckets / Objects / www.				
-featured				
Current Path				
Upload Create Folder Download Delete Actions	~		Ν	ame v Q C
Name	Size	Storage Class	Last Modified	Operation
(For Customer)Quidway S2352EI Ethernet Switches Product Documentati	25.8142 M	Infrequent Access Storage	2023-12-06 15:52:23 UTC+0800	Preview Download More ~
	260.5884 M	Infrequent Access Storage	2023-12-06 15:52:23 UTC+0800	Preview Download More ~
	84.7243 M	Infrequent Access Storage	2023-12-06 15:52:32 UTC+0800	Preview Download More ~
	26.4365 M	Infrequent Access Storage	2023-12-06 15:52:35 UTC+0800	Preview Download More ~
	635.6377 k	Infrequent Access Storage	2023-12-06 15:52:23 UTC+0800	Preview Download More ~
			Display records fro	om 1 to 5, total number:5 $\ll$ $<$ 1 $>$ $>$



# 6 Cloudtrail

For IAM users, they can operate Cloudtrail only if they have the corresponding permissions. The permissions required are as follows.

Operation	Permissions required		
View mananement Events	cloudtrail:LookupEvents		
View cloudtrail List	cloudtrail:DescribeTrails, cloudtrail:GetTrailStatus		
Create a cloudtrail	oos:ListAllMyBuckets, cloudtrail:CreateTrail,		
	cloudtrail:PutEventSelectors, cloudtrail:StartLogging		
View trails	cloudtrail:DescribeTrails, cloudtrail:GetTrailStatus,		
	cloudtrail:GetEventSelectors		
Edit a Trail	oos:ListAllMyBuckets, cloudtrail:UpdateTrail,		
	cloudtrail:PutEventSelectors, cloudtrail:DescribeTrails,		
	cloudtrail:GetEventSelectors, cloudtrail:GetTrailStatus,		
	cloudtrail:StartLogging, cloudtrail:StopLogging		
Delete a trail	cloudtrail:DescribeTrails, cloudtrail:DeleteTrail,		
	cloudtrail:GetTrailStatus		

## 6.1 Management Events Record

Enter **Cloudtrail** > **Manage Events**, you can view the management events of the last 6 months. If you want to view and save the operation records for a longer period of time, please select **Create trail** to create a trail. The management event log file will be saved in the specified bucket.

Object-Oriented Storage	Management Event History						
	You can view the management events of the last 6 months. If you want to view and save the operation records for a longer period of time, please select Create Inst.						
Statistics Overview *							
Buckets	IAM User Name V Please enter an	IAM User Name All	V 🔲 Start date	- End date Search	Custom Column V		
Cloudtrail 🔺							
Manage Events	Event Time	User Name	Event Name	Resource Type	Resource Name		
Trails List	> 2023-09-12 10:11:20 UTC+0800	Root User	LookupEvents	-	-		
IAM *	> 2023-09-12 10:11:06 UTC+0800	Root User	LookupEvents				
Resource Package	> 2023-09-12 10:11:02 UTC+0800	Root User	LookupEvents	-	-		
	> 2023-09-12 10:10:59 UTC+0800	Root User	LookupEvents		-		
	> 2023-09-12 10:10:58 UTC+0800	Root User	DescribeTrails		-		
	> 2023-09-12 10:07:09 UTC+0800	Root User	GetRegions		-		
	> 2023-09-12 10:07:09 UTC+0800	Root User	GetService		-		
	> 2023-09-12 10:06:38 UTC+0800	Root User	LookupEvents				
	> 2023-09-12 10:06:20 UTC+0800	Root User	LookupEvents				
	> 2023-09-12 10:06:18 UTC+0800	Root User	LookupEvents				
					Display records from 1 to 10 10/page $\checkmark$ << >		

You can select the IAM User Name, AccessKeyId, Event ID, Event Name, Event Source, Resource Name, and Resource Type to query according to your needs, and you can also select the operation type (including: all types, read operations, and write operations), start and end time to search. All management operations are displayed by default.

In the Custom Column, you can select the items to be displayed at the time: Event Time, User Name, Event Name, Resource Type, Resource Name, Event Source, Event ID, Request ID, AccesskeyId, Source IP Address, Operation Type, and Error Code. The Event Time, User Name, Event Name,



**Resource Type**, and **Resource Name** are displayed by default.

## 6.1.1 View Event Details

Click the corresponding event to view the detailed information of the event.

2023-08-07 16:48:21 UTC+0800	Root User	GetBucketObjectLockConfiguration	OOS Bucket	e	
Request Time:	2023-08-07 16:48:21 UTC+0800		AccessKeyld:		
Event ID:	7531973935267728365		Request ID:	c1b977972d4a4e729f191b12141ad9dbdecfd1d3d5d7d9dbdd	
Event Source :	oos-cn.ctyun.cn		Event Name:	GetBucketObjectLockConfiguration	
User Name:	Root User		Operation Type:	Read	
Resource Type:	OOS Bucket		Resource Name:	e	
Source IP Address:	<u> </u>		Error Code:	-	

### **Event details description**

Item	Description				
Request Time	The request time.				
Eevent ID	The ID generated by the trail to uniquely identify each event.				
Event Source	The server that processes the request:				
	Object Storage Network:				
	OOS: oos-cn.ctyunapi.com				
	Cloudtrail: oos-cn-cloudtrail.ctyunapi.cn				
	IAM: oos-cn-iam.ctyunapi.cn				
	Statistics API: oos-cn-mg.ctyunapi.cn				
	Console: oos-cn.ctyun.cn				
	Hongkong Node:				
	<ul> <li>OOS: oos-cnhk-hqnet.ctyunapi.cn (Hongkong Highquality Network), or oos-cnhk-nqnet.ctyunapi.cn (Hongkong Normal Network)</li> <li>Cloudtrail: oos-cnhk-cloudtrail.ctyunapi.cn</li> <li>IAM: oos-cnhk-iam.ctyunapi.cn</li> </ul>				
	Statistics API: oos-cnhk-mg.ctyunapi.cn				
	Console: oos-cnhk-hqnet.ctyun.cn (Hongkong Highquality				
	Network), or oos-cnhk-nqnet.ctyun.cn (Hongkong Normal				
	Network)				
User Name	User name.				
Resource Type	The resource type to which the management event belongs:				
	OOS Bucket.				
	CloudTrail.				
	• IAM User.				
	• IAM Group.				
	IAM Policy.				



	IAM AccessKey.				
	IAM MfaDevice.				
	• -: All resources of the resource type corresponding to the event, or no				
	resources are involved.				
Source IP Address	The source IP address of the request initiated by the user.				
AccessKeyId	The key ID used by the user to initiate the operation.				
	-: Indicates console access.				
Request ID	After sending the request, the server returns the x-amz-request-id				
	response.				
Event Name	Event name.				
Operation Type	Operation type:				
	● Read.				
	• Write.				
Resource Name	Resources accessed by operations.				
	-: Indicates all resources corresponding to the event.				
Error Code	Error code.				
	-: Indicates correct access without error code.				

Click the button View event record, you can the event detailed information.

```
{
 "eventId": "7531973935267728365",
 "resource": "{\"Resources\":[{\"name\":\"examplebucket1-a\",\"type\":\"00S
Bucket\",\"arn\":\"arn:ctyun:oos::32fefj64y54gc:bucket/examplebucket1-a\"}]}",
 "eventVersion": "1.06",
 "eventSource": "oos-cn.ctyun.cn",
 "requestParameters": "{\"bucketName\":\"examplebucket1-a\"}",
 "userAgent": "oos-cn.ctyun.cn",
 "readOnly": true,
 "userIdentity": {
   "accountId": "32fefj64y54gc",
   "principalId": "32fefj64y54gc",
   "type": "Root",
   "arn": "arn:ctyun:iam::32fefj64y54gc:root"
 },
 "eventType": "ApiCall",
 "serviceName": "OOS",
 "sourceIp": "36.111.136.72",
 "requestId": "c1b977972d4a4e729f191b12141ad9dbdecfd1d3d5d7d9dbdd",
 "requestURL": "http://oos-cn.ctyun.cn/",
```



"eventTime": "2023-08-07 16:48:21 UTC+0800", "eventName": "GetBucketObjectLockConfiguration", "requestRegion": "cn", "managementEvent": true

```
}
```

Event information description

Field	Description
eventId	The ID generated by the trail to uniquely identify each event.
resource	The resource information.
eventVersion	Cloudtrail version.
eventSource	Event resource.
requestParameters	Request parameters.
userAgent	User agent.
	The client proxy identity that sends API requests. Except for the console, it is displayed
	according to the User Agent request header issued by the client API. If it cannot be
	obtained, it is not displayed.
	The request is sent by the user through the console, displaying oos-cn.ctyun.cn.
readOnly	Whether the event is a read-only operation:
	• true.
	• false.
userIdentity	User information.
eventType	Event request type.
serviceName	Service name.
sourcelp	Source IP.
requestId	Request ID.
requestURL	Request URL.
eventTime	The request time.
eventName	Event name.
requestRegion	Request region.
managementEvent	Whether the event is a management operation:
	• true.
	• false.

## 6.1.2 Event List

Category	Event
Bucket	DeleteBucket
	DeleteBucketLifecycle
	GetBucketLifecycle



	GetBucketLocation
	CreateBucket
	PutBucketLifecycle
	PutBucketLogging
	GetBucketAcl
	PutBucketAcl
	GetBucketPolicy
	PutBucketPolicy
	DeleteBucketPolicy
	GetBucketWebsite
	PutBucketWebsite
	DeleteBucketWebsite
	ListMultipartUploads
	GetBucketLogging
	GetBucketCors
	PutBucketCors
	DeleteBucketCors
	PutBucketObjectLockConfiguration
	GetBucketObjectLockConfiguration
	DeleteBucketObjectLockConfiguration
	PutBucketInventoryConfiguration
	GetBucketInventoryConfiguration
	DeleteBucketInventoryConfiguration
Services	GetService
	GetRegions
Statistics	GetCapacity
	GetBilledStorageUsage
	GetRestoreCapacity
	GetDeleteCapacity
	GetTraffics
	GetRequests
	GetReturnCode
	GetConcurrentConnection
	GetUsage
	GetBandwidth
Console	ConsoleLogin
	LogoutUser
	CheckMfa
Cloudtrail	CreateTrail
	DeleteTrail
	DescribeTrails
	GetTrailStatus
	PutEventSelectors



	GetEventSelectors
	UpdateTrail
	StartLogging
	StopLogging
	LookupEvents
IAM	CreateGroup
	DeleteGroup
	GetGroup
	ListGroups
	AddUserToGroup
	RemoveUserFromGroup
	CreateUser
	DeleteUser
	GetUser
	ListUsers
	ListUserTags
	ListGroupsForUser
	CreateAccessKey
	DeleteAccessKey
	ListAccessKeys
	GetAccessKeyLastUsed
	UpdateAccessKey
	GetSessionToken
	TagUser
	ChangePassword
	CreateLoginProfile
	CreateVirtualMFADevice
	DeactivateMFADevice
	DeleteAccountPasswordPolicy
	GetAccountLoginSecurityPolicy
	UpdateAccountLoginSecurityPolicy
	DeleteAccountLoginSecurityPolicy
	DeleteLoginProfile
	DeleteVirtualMFADevice
	EnableMFADevice
	GetAccountPasswordPolicy
	GetLoginProfile
	ListVirtualMFADevices
	UpdateAccountPasswordPolicy
	UpdateLoginProfile
	CreatePolicy
	DeletePolicy
	AttachGroupPolicy



DetachGroupPolicy
GetPolicy
ListAttachedUserPolicies
AttachUserPolicy
ListAttachedGroupPolicies
ListPolicies
GetAccountSummary
DetachUserPolicy
ListEntitiesForPolicy
UnTagUser
ListMFADevices

## 6.2 Trails List

Enter Trails List, you can view all trails information under the current account, including: Trail Name, Bucket Name, Log File Prefix, Status, and Operation.

Trails				
Create			Please enter a trail name	ALL $\checkmark$ Search C
Trail Name	Bucket Name	Log File Prefix	Status	Operation
m		1111	Bucket access denied, please replace or fix it.	Enable Management Delete
888	1	555	Disable	Enable Management Delete
aaa20200		aaa2020	Bucket access denied, please replace or fix it.	Enable Management Delete
test0601		test0601	Disable	Enable Management Delete
test1		test	Bucket access denied, please replace or fix it.	Enable Management Delete
test1111	1 - 1 - 1	tea	Disable	Enable Management Delete
test111111	(province)	aaa	Disable	Enable Management Delete
test2	Sector and P	test2	Bucket access denied, please replace or fix it.	Enable Management Delete
trail		trail	Enable	Disable Management Delete

## 6.2.1 Create Trail

You can follow the steps below to create a trail:

- 1. Click **Create trail** on the **Manage Events** page, or click **Create** on the **Trails List** page to enter the **Create Trail**.
- 2. Create a trail.



Trails / Create Trail
Set Basic Information
Trail Name     Please enter trail name
Set Management Event Management events show information about management operations performed on resources in your OOS account
Management Event 🕘 All Operation
Read
○ Write
Set Storage Location Set the bucket where the trail log is stored
Storage Location Choose a bucket V C
If there is no bucket in the list, You can also create a new bucket
Prefix Prefix (optional)
Trail status 🗾
No fees will be charged during the trial operation stage Cancel Confirm

- Set Basic Information: Fill in the Trail Name, the rules for trail name are as follows:
  - The value can contain ASCII letters (a-z, A-Z), numbers (0-9), periods (.), underscores (\_), or hyphens (-).
  - > The value must start with a letter or number, and end with a letter or number.
  - > The value cannot be an IP address (such as 192.162.5.4).
  - The value cannot contain any combination of adjacent period (.), underscores (\_), and hyphens (-). Such as the value cannot contain similar combinations of dots (..), dots and underscores (.\_).
- Set Management Event:
  - > All Operation: including Read and Write.
  - Read.
  - ➢ Write.
- Set Storage Location:
  - Storage Location: It can be stored in an existing bucket (the user needs to have the corresponding bucket permission), or you can create a new bucket in the account (the user needs to have the permission to create a new bucket), and store the trail log in the newly created bucket.
  - > **Prefix:** The value is a string whose length is 0 to 200.
    - The storage path of the specified Prefix is: oos://<bucket>/<Prefix>/00SLogs/<AccountID>/CloudTrail/<year>/<mon th>/<day>/<Log data file>



■ The storage path without specified the **Prefix** is:

oos://<bucket>/00SLogs/<AccountID>/CloudTrail/<year>/<month>/<day>

/<log data file>

- > Trail status:
  - **ON**: The trail is turned on.
  - **OFF**: The trail is turned off.

## 6.2.2 Modify the Trail

On the **Trail List** page, when you need to modify the trail, you can click **Enable/Disable**, **Management**, or **Delete** to modify the trail.

Trails					
Create			Please enter a trail name	ALL $\vee$	Search C
Trail Name	Bucket Name	Log File Prefix	Status	Operation	
	bucket-test-w1	1111	Bucket access denied, please replace or fix it.	Enable Management Delete	
	bucket.test.wu1	555	Disable	Enable Management Delete	
	bucket.test.wu1	aaa2020	Bucket access denied, please replace or fix it.	Enable Management Delete	
	bucket.test.wu1	test0601	Disable	Enable Management Delete	
cuit .	bucket-test-w1	test	Bucket access denied, please replace or fix it.	Enable Management Delete	
	bucket.test.wu1	tea	Disable	Enable Management Delete	
	bucket.test.wu1	aaa	Disable	Enable Management Delete	
(B)	bucket-test-w1	test2	Bucket access denied, please replace or fix it.	Enable Management Delete	
	wl2022	trail	Enable	Disable Management Delete	

Click Management to enter the trail detailed page. Click Edit Trail Rules, you can click Edit Trail Rules to reset the Management Event, Storage Location, Prefix and Trail status.

Trails / trail
trail Edit Trail Rules Trail status
Management Event Management events show information about management operations performed on resources in your OOS account
Management Event All Operation
Storage Location Set the bucket where the trail log is stored
Storage Location
Prefix trail
Lest log file delivered 2023-07-11 15/01/28 UTC+0800



# 7 **IAM**

For IAM users, they can perform IAM-related operations on the console only if they have the corresponding permissions. The permissions required are as follows.

Operation		Permissions required
IAM User	Create IAM users	iam:CreateUser, iam:CreateAccessKey, iam:CreateLoginProfile,
		iam:GetAccountPasswordPolicy, iam:GetUser
		Suggested permissions: iam:AddUserToGroup,
		iam:AttachUserPolicy, iam:ListUsers, iam:ListGroups,
		iam:ListPolicies
	Delete IAM users	iam:ListUsers, iam:DeleteAccessKey, iam:DeleteUser,
		iam:RemoveUserFromGroup, iam:DeactivateMFADevice,
		iam:DeleteLoginProfile, iam:DetachUserPolicy
	View IAM user	iam:ListAccessKeys, iam:ListUsers, iam:ListUserTags,
	information	iam:ListGroupsForUser, iam:ListAttachedUserPolicies,
		iam:ListEntitiesForPolicy, iam:ListMFADevices, iam:GetUser
	Security Credential	iam:GetLoginProfile, iam:ListUsers, iam:GetUser,
		iam:GetAccountPasswordPolicy, iam:CreateLoginProfile,
		iam:DeleteLoginProfile, iam:UpdateLoginProfile
	AccessKeys	iam:ListAccessKeys, iam:ListUsers, iam:GetUser,
		iam:CreateAccessKey, iam:GetAccessKeyLastUsed,
		iam:DeleteAccessKey, iam:UpdateAccessKey
	Permissions	iam:ListUsers, iam:ListGroupsForUser, iam:ListPolicies,
		iam:ListAttachedGroupPolicies, iam:ListAttachedUserPolicies,
		iam:GetUser, iam:RemoveUserFromGroup,
		iam:AttachUserPolicy, iam:DetachUserPolicy
	User Group	iam:ListUsers, iam:ListGroups, iam:ListGroupsForUser,
		iam:GetUser, iam:GetGroup, iam:AddUserToGroup,
		iam:RemoveUserFromGroup
	Tag	iam:ListUsers, iam:GetUser, iam:TagUser, iam:UntagUser
IAM user	Create User Group	iam:CreateGroup
group		Suggested permissions: iam:ListGroups, iam:ListPolicies,
		iam:AttachGroupPolicy
	View User Group	iam:ListGroups, iam:ListAttachedGroupPolicies, iam:GetGroup
	Modify User Group	iam:ListUsers, iam:ListGroups, iam:ListGroupsForUser,
		iam:ListPolicies, iam:ListAttachedGroupPolicies, iam:GetGroup,
		iam:AddUserToGroup, iam:RemoveUserFromGroup,
		iam:AttachGroupPolicy, iam:DetachGroupPolicy
	Delete User Groups	iam:ListGroups, iam:DeleteGroup, iam:RemoveUserFromGroup,
		iam:DetachGroupPolicy
Policy	View the Policy	iam:ListPolicies、iam:ListEntitiesForPolicy、iam:GetPolicy
	Create the Custom	iam:CreatePolicy, iam:GetPolicy



	Policy	Suggested permissions: iam:ListPolicies				
	Modify the Custom	iam:CreatePolicy, iam:GetPolicy, iam:ListPolicies				
	Policy					
	Delete the Custom	iam:ListPolicies, iam:DeletePolicy, iam:DetachUserPolicy,				
	Policy	iam:DetachGroupPolicy				
	Attach/Deattach	iam:ListUsers, iam:ListGroups, iam:ListPolicies,				
	Users/Groups	iam:ListAttachedGroupPolicies, iam:ListAttachedUserPolicies,				
		iam:ListEntitiesForPolicy, iam:AttachUserPolicy,				
		iam:DetachUserPolicy, iam:AttachGroupPolicy,				
		iam:DetachGroupPolicy				
Security Edit Password		iam:GetAccountPasswordPolicy,				
Setting	Policy	iam:UpdateAccountPasswordPolicy				
	Delete Password	iam:GetAccountPasswordPolicy,				
	Policy	iam:DeleteAccountPasswordPolicy				
	Edit Login Security	iam:GetAccountLoginSecurityPolicy,				
	Policy	iam:UpdateAccountLoginSecurityPolicy				
	Delete Login	iam:UpdateAccountLoginSecurityPolicy,				
	Security Policy	iam:DeleteAccountLoginSecurityPolicy				
Security	AccessKeys	iam:ListAccessKeys, iam:GetUser, iam:CreateAccessKey,				
Credential		am:DeleteAccessKey, iam:UpdateAccessKey				
	Password	iam:GetLoginProfile, iam:GetUser, iam:ChangePassword				
	MFA	iam:ListMFADevices, iam:GetUser, iam:CreateVirtualMFADevice,				
		iam:DeleteVirtualMFADevice, iam:EnableMFADevice,				
		iam:DeactivateMFADevice				

## 7.1 Getting Started

Go to IAM > Overview, click Create User, enter Create User, and start creating an IAM user.

1. Set User: You can add one or more IAM users, and Select OOS Access Type for IAM users.



IAM / Users / Create User				
<b>1</b> —	2	(3)	(4)	5
Set User Set User Details You can add one or * User Name	Set Permissions more users with the same access type and permissions at once test-aa Add another liser	Ser rag	KONOW	Succeed
Select OOS Access Type	Enables a password that allows users to login to	the OOS Management Console		
* Access Type	Console Access Programmatic Access			
Console Password	Custom Passw     Show	Password		
Password Reset	The user must reset the password after the system/administrator	generates the password 💿		
				Cancel Next, Permissions

- 2. **Set Permissions** (Optional): To add permissions for IAM users, there are three ways to add permissions (only one can be selected).
  - Add User to Group (Prerequisite: There is already a user group): The IAM user will have all the permissions of the user group.
  - **Copy Permissions From Existing User** (Existing IAM users have a policy of being authorized through direct attachment): Only one IAM user's permissions can be copied at a time. You can only copy the policies directly attached by an existing IAM user, not the policies of the IAM user's group.
  - Attach Existing Policies Directly.



IAM / Us	sers / Create User								
	<i>⊙</i> ———	2							
	Set User	Set Permissions	Set Tag	Review	Succeed				
Set Per	Set Permissions(Optional) Add User to Group Copy Permissions From Existing User Attach Existing Policies Directly								
0 A	dd user to an existing group or create a new one and use the grou	ıp's permissions							
Creat There ar	e Group e currently 8 items, 2 has been selected groupte, group-read				Group Name Q C				
	Group Name	Crea	ation Time	Attached Policies					
1	group-read	202	3-07-11 15:38:50 UTC+0800	IAMReadOnlyA					
×	groupte	202	0-06-02 11:17:02 UTC+0800	bucket-read					
	oos-read	202	0-05-13 14:48:03 UTC+0800	OOSReadOnlyA					
	test	202	3-07-10 11:20:05 UTC+0800	None					
	test1	202	2020-06-02 15:39:41 UTC+0800 None						
	test12345	202	0-08-04 17:37:45 UTC+0800	None					
	test_wu1	202	1-09-24 10:05:20 UTC+0800	None					
	testa	202	3-04-18 17:10:12 UTC+0800	None					

3. Set Tag (Optional): You can add tag keys and tag values for new IAM users. Each IAM user can add up to 10 tags.

IAM / Users / Create User				
⊘ ———	Ø	3		
Set User	Set Permissions	Set Tag	Review	Succeed
Set Tag(Optional)				
Add tags to users, and up to 10 can be added				
Add New Tag				
Кеу	Value (optional)		Operation	
test	test5		×	
				Previous Next,Information Review

4. **Review**: Review the information of the newly created IAM user(s). If you need to change it, you can click the corresponding edit icon on this page, and then go to the corresponding page to make changes.

Previous Next,Tag



IAM / Users / Create User				
Ø —	Ø	⊘	4	
Set User	Set Permissions	Set Tag	Review	Succeed
User Details The following IAM users with	ill be created 🛛			
User Name	test-aa			
Access Information				
Access Type	Console Access			
Console Password Type	Custom Password			
Require Password Reset	No			
Permissions Summary The following	policies will be attached to the user 🛛			
Model		Group Name		
Group		groupte		
Group		group-read		
The new view will be added the following	ing long 174			
lags The new user will receive the followi	ng tag 🖉			
Кеу		Value		
test		test5		
				Previous Next,Create User

5. Succeed: You can view User, AccessKeyID, SecretAccessKey, Password. You can click Download Certificate, view UserName, AccessKeyID, SecretAccessKey, ConsoleLoginLink.

IAM / Users / Create User				
· · · · · · · · · · · · · · · · · · ·	Ø			6
Set User	Set Permissions	Set Tag	Review	Succeed
Created				
User created successfully You have successfully created a user. The user's pass downloaded once and cannot be obtained again after Download Certificate	sword or access key is shown below. You can view and downlor r the page jumps. Please keep the relevant access key ID an	ad the user's security credentials. Users with consol d private key property.	e access permission can login through the IAM user login link	: The credential information can only be
User	Password			
🖉 test-aa	*******			٢
		Vour user has been	created you can choose to return to the user list or continue	to create Return to Lisers Continue to Create



## 7.2 IAM Users

If you are a root user, that is, a registered user who has activated the OOS service, you can allocate resources to different sub-users (IAM users), and assign corresponding permissions to each IAM user. By default, IAM users do not have any permissions. The root user or related sub-users with IAM authorization can authorize IAM sub-users. After authorization, IAM users can operate on resources according to their permissions.

## 7.2.1 Create an IAM User

### Steps:

Enter IAM > Overview, click Create User, or enter IAM > Users Management > Users, click Create User.

1. Create user on **Set User** page.

IAM / Users / Create User				
0				
Set User	Set Permissions	Set Tag	Review	Succeed
Set User Details You can add o	ine or more users with the same access type and permissions at on test-aa Add Another User	ce		
Select OOS Access Type				
* Access Type	Console Access 🛛 🗌 Programmatic Access 🚱			
Console Password	Autogenerated Password	_		
	Custom Password	Show Password		
Password Reset	The user must reset the password after the system/administ	trator generates the password 🔮		
				Cancel Next , Permissions

- User Name: The user name for logging in to OOS, the administrator (the root user or related IAM users with IAM authorization) can add 1-10 IAM users with the same access type and access permissions at a time. The user name must follow the following principles:
  - > The name of the IAM user must be unique within the OOS account.
  - The value is a string of 1 to 64 insensitive letters, numbers, or special characters. The special characters only include underscores (\_), hyphens (-), comma (,), period (.), plus sign (+), equal sign (=), and at sign (@).
- Access Type: IAM user login method IAM, select Console Access or Programmatic Access, at least one access method must be selected.
  - Console Access: Enables a password that allows users to login to the OOS Management Console.
  - **Programmatic Access**: Enables an AccessKeyID and SecretAccessKey for the OOS API, SDK.
- Console Password:

IAM



- > Autogeneraged Password: Random password generated by the system.
- Custom Password: The login password set by the administrator for the IAM user. The password must conform to the password policy of the OOS account (if it exists). If no password policy has been set, follow the default password rules. The default password rule is: the password must be an 8-128 string containing lowercase letters and numbers.
- Password Reset: Set whether a new IAM user needs to reset the password when logging in for the first time. After selecting, the user must create a new password at next login.

Note: Only when you choose Console Access, Console Password and Password Reset will appear.

### 2. Set Permissions

After finishing setting up users, enter Set Permission to set permissions for IAM users.

	Set User	2 Set Permissions	3 Set Tag	Review	5 Succeed
et Pe	er to Group Copy Permissions From Existing User	Attach Existing Policies Directly			
A	dd user to an existing group or create a new one and use the grou	p's permissions			Group Name Q
ere ar	e currently 8 items, 2 has been selected :groupte, group-read Group Name	Creation Ti	me	Attached Policies	
~	group-read	2023-07-11 2020-06-02	15:38:50 UTC+0800 211:17:02 UTC+0800	IAMReadOnlyA	
	oos-read	2020-05-13	3 14:48:03 UTC+0800	OOSReadOnlyA	
	test	2023-07-10	11:20:05 UTC+0800	None	
	test1 test12345	2020-06-02 2020-08-04	2 15:39:41 UTC+0800	None	
	test_wu1	2021-09-24	10:05:20 UTC+0800	None	
	testa	2023-04-18	3 17:10:12 UTC+0800	None	

- Add User to Group (Prerequisite: There is already a user group): The user will have all the permissions of the user group. A user can join up to 10 groups.
- **Copy Permissions From Existing User** (Existing users have a policy of being authorized through direct attachment): Only one user's permissions can be copied at a time. You can only copy the policies directly attached by an existing user, not the policies of the user's group.
- Attach Existing Policies Directly: Directly add existing policies to users, and each user can directly add up to 10 policies.

When the user sets permissions, he can only select one of the above three methods to authorize the user. When the user has selected a certain permission setting method and checked it, and then switch to other authorization methods, a prompt box will pop up.



Change Permiss	ion Type	×
If you change permission	n types, the informatio	n you entered will be
lost. Are you sure?		

Change Type: Confirm that the existing permission type is changed, and the existing permission information will not be retained after the change.

**Note**: You can add a policy to the user when creating a user, or you can add a policy to the user after the user is created. Each user can directly attach up to 10 policies, excluding the policies attached with the group.

### 3. Set Tag

Administrators can set tags for IAM users, which are additional attributes of IAM users.

IAM / Users / Create User				
o <u> </u>	- 📀	3		
Set User	Set Permissions	Set Tag	Review	Succeed
Set Tag(Optional)				
Add tags to users, and up to 10 can be added				
Add New Tag				
Кеу	Value (optional)		Operation	
test	test5		×	
				Previous Next, Information Review

A user can have up to 10 tags  $_{\circ}$ 

• Key: The value can include letters, digits, spaces, plus (+), equals (=), period (.), 'At' symbol (@), underscores (\_), hyphens (-), colons (:), forward slash (/).

The tag key is not case sensitive, but case is preserved. For example, Department and department tag keys cannot exist at the same time. If you use the Department=foo tag to mark the user and then add the department=bar label, it will replace the first tag and the tag value becomes bar.

• Value: Key value. The value can be empty.



You cannot specify multiple values for a single tag, but multiple tag keys can have the same tag value.

### 4. Review

Review the information of the newly created user(s). If you need to change it, you can click the corresponding edit icon on this page, and then go to the corresponding page to make changes.

IAM / Users / Create User				
Set User	Set Permissions	Set Tag	4 Review	5 Succeed
User Details The following IAM users w User Name	ill be created 🛛 🕅 test-aa			
Access Information 2 Access Type Console Password Type Require Password Reset	Console Access Custom Password No			
Permissions Summary The following	policies will be attached to the user 🛛			
Group		Group Name groupte		
Group		group-read		
Tags The new user will receive the following	ing tag 🛛			
Key		Value		
test		test5		
				Previous Next,Create User

### 5. Download Certificate

Click Download Certificate, save the UserName, Password, AccessKeyID, SecretAccessKey, ConsoleLoginLink.

**Note**: The certificate can only be downloaded once, so be sure to keep it in a safe place. If the accesskey of a user is lost, you can delete the original accesskey on the user details page, and then obtain the new accesskey by creating a new accesskey. If the password is lost, a user with the permission to modify the password is required to reset the user's password on the console.



/ Users / Create User				
				5
Set User	Set Permissions	Set Tag	Review	Succeed
reated				
User created successfully     You have successfully reated a user. The user     downloaded once and cannot be obtained aga     Download Centificate	r's password or access key is shown below. You can view and download ain after the page jumps. Please keep the relevant access key ID an	ad the user's security credentials. Users with conso d private key property.	le access permission can login through the IAM user login	link. The credential information can only be
User	Password			
🕑 test-aa	*******			0
		Your user has bee	n created you can choose to return to the user list or contin	ue to create Return to Users Continue to L

## 7.2.2 View and Modify the IAM User

Click IAM > Users Management > Users, and the user list will appear.

You can click Custom Column to choose to display the corresponding user information according to your needs, and can choose from the following items to display:

- User Name
- Password Usage Time
- Password Remaining Usable Time
- Console Last Login
- User ID
- ARN
- MFA
- Programmatic Access
- Console Access

The User Name and Operation are fixed display items. If not selected, the User Name, Password Usage Time, Password Remaining Usable Time, Console Last Login, Operation will be displayed by default.



IAM / Us	ers				
Create	Create User Delete Custom Column > Custom Column > C				
There are	currently 11 items, 0 has been selected User Name	Password Usage Time 🛛	Password Remaining Usable Time 🛛	Console Last Login	Operation
	888	163days	Permanent	2023-01-30 10:14:47 UTC+0800	Add Permissions Add to Group Delete Management
	test	1070days	Permanent	2020-08-05 17:18:51 UTC+0800	Add Permissions Add to Group Delete Management
	test111	None	Permanent	None	Add Permissions Add to Group Delete Management
	test12345	1083days	Permanent	None	Add Permissions Add to Group Delete Management
	test1_bucket	1133days	Permanent	2020-06-04 14:47:11 UTC+0800	Add Permissions Add to Group Delete Management
	test3	1days	Permanent	None	Add Permissions Add to Group Delete Management
	test4	1days	Permanent	None	Add Permissions Add to Group Delete Management
	test_a1	2days	Permanent	None	Add Permissions Add to Group Delete Management
	test_a2	2days	Permanent	None	Add Permissions Add to Group Delete Management
	test_aa	85days	Permanent	None	Add Permissions Add to Group Delete Management
	testabc	84days	Permanent	2023-04-19 15:34:21 UTC+0800	Add Permissions Add to Group Delete Management

Item	Description
User Name	IAM user name.
User ID	The unique identifier of the IAM user, randomly generated by the system when the
	user is created.
Password Usage	The number of days since the password was created successfully. If there is no
Time	console access permission, <b>None</b> is displayed.
Password	Password remaining time:
Remaining Usable	• If the user's password has no expiration time, it will be displayed as <b>Permanent</b> .
Time	• The password has not expired, and the remaining days are displayed.
	• The password has expired, the number of days that have expired is displayed,
	and the day the password has expired is displayed as <b>0</b> days.
Console Last Login	The last time the IAM user successfully accessed the console.
ARN	The ARN of the IAM user name, which uniquely identifies the IAM user.
MFA	MFA status:
	• Enable
	• Disable
Programmatic	Whether to enable programmatic access:
Access	• Enable
	• Disable
Console Access	Whether to enable console access:
	• Enable
	• Disable
Operation	Add Permissions: Add the required policies for this IAM user.
	• Add to Group: Add the IAM user to user groups.
	• Delete: Delete this IAM user.
	• Management: Enter the IAM user page.

Click the corresponding user name or Management to view the detailed information of the IAM user.

$\sim$	天翼云
$ \cup$	State Cloud

IAM / Users / test			
Basic Information           User Name         tett@32fef5645fagc         C         Creation Time:         2020-08-05 15:58:01 UTC-0000           User ID:         6917xa327c32648ed8167554555271433         User Type:         UAM User			
Security Credential AccessKeys	Permissions Groups Tags		
Console Login Settings			
Console Access	Enable Management Console Access		
Console Login Link	Console Legin Link h		
Login and Sensitive Information			
Last login Time	2020-08-05 17:18:51 UTC+0800		
Last login IP	Last login IP 221.216.25.1		
Last Sensitive Operation	Lest Servitive Operation View Details		
Secondary Identity Verification			
Operation Protection	MFA device verification is not enabled		
Assigned MFA Device	Not Assigned		

#### **Basic Information Description**

Item	Description	
User Name	<iam name="" user="">@<account id="">.</account></iam>	
	When the IAM user logs in, the user name is <i><iam i="" name<="" user="">&gt;.</iam></i>	
Creation Time	The time when the IAM user was created.	
User ID	IAM user ID.	
User Type	User type:	
	Root User	
	IAM User	

### 7.2.2.1 View and Modify Security Credential

Click **Security Credential** to enter **Security Credential** page, you can modify the **Console Access** status, and copy the IAM user Console Login Link.

IAM / Users / test

Basic Information
User Name

User Name

etal@32iefg6/x5gc 0

Creation Time

200-20-20 51 53801 UTC-000

Security Credential AccessKeys Permissions Groups Tags

Creation Time

Security Credential

AccessKeys

Permissions

Groups Tags

Console Login Settings

Console Login Table

Mained Access

Security Credential

AccessKeys

Permissions

Groups Table

Mained Access

Security Credential

AccessKeys

Permissions

Groups Table Management Console Access

Console Login Table

Mained Access

Security Credential

AccessKeys

Permissions

Groups Access

Security Credential

AccessKeys

Permissions

Groups Access

Console Login Table

Mained Access

Security Credential

AccessKeys

Permissions

Security Credential

AccessKeys

Permissions

Security Credential

AccessKeys

Permissions

Groups Access

Security Credential

AccessKeys

Permissions

Security Credential

AccessKeys

Permissions

Security Credential

AccessKeys

Permissi

Click Management Console Access, you can reset the console access settings.



### Console Login Settings: test@32fefj64y54gc

Console Password	$\bigcirc$	Enable			
		Disable Dis	abling will remove pre-	existing passwor	d
Set Login Password	0	Keep Existing Passw	vord		
		Autogenerated Pass	sword		
		Custom Password			
Password Reset		User must create a r	new password at next lo	gin 🕜	
				Cancel	Confirm

### Console Login Settings description

ltem	Description		
Console Password	Whether the console password login is enabled:		
	• Enable: Enable console password login. When there is no console login		
	password, a new login password will be generated.		
	• <b>Disable</b> : Disable console password login and delete the current		
	password.		
Set Login Password	Set login password:		
	• Keep Existing Password: Use the current login password, this item will		
	only be available when the current password exists.		
	• Autogenerated Password: The system randomly generates the login		
	password again.		
	• <b>Custom Password</b> : The administrator resets the login password.		
Password Reset	Set whether a new IAM user needs to reset the password when logging in for		
	the first time. After selecting, the user must create a new password at next		
	login.		

 $\times$ 

Confirm

### 7.2.2.2 View and Modify AccessKeys

Click Accesskeys, you can create, active/inactive, delete accesskey.

- Note:
- Only when there are less than 2 AccessKeys can a new AccessKey be created (a user can only create 2 AccessKeys at most).
- If the AccessKey is lost, the original AccessKey can be deleted, and then a new AccessKey can be • obtained by creating a new AccessKey, and the AccessKey download certificate can be performed. The AccessKey can only be downloaded once, and the AccessKey information cannot be seen again after closing the pop-up window.



IAM / Users / test1

IAM / Users / aaa						
Basic Information						
User Name: aa	a@32fefj64y54gc 🗇			Creation Time:	2023-01-30 10:13:50 UTC+0800	
User ID: 1fa	15f43af3644636a6955e8076b328	13		User Type:	IAM User	
Security Credential Acces	ssKeys Permissions	Groups Tags				
AccessKeyld		Creation Time	Last Used Time		Status	Operation
95786a4ed2e0ebfd3670 🗇		2023-04-18 15:33:25 UTC+0800	None		Active	Make inactive Delete

## 7.2.2.3 View and Modify Permissions

Click Permissions, you can view IAM user permissions, add permissions for the IAM user, remove permissions for the IAM user, and remove the IAM user from group.

Basic Information User Name: User ID:	test1@32fef64y54gc 🗇 976c87d2dcbf4aa1887583043115fd7c	Creation Time: User Type:	2024-03-13 15:54:38 UTC+0800 IAM User	
Security Credential	AccessKeys Permissions Groups Tags			
There are currently 2 items	s, 0 has been selected : Attached Type -	Policy Type >	Description	Operation
I IAMPolicy	Attached directly	Custom Policy	Create IAM policy	Remove Permission
IAMPolicy	Attached from group (IAM1)	Custom Policy	Create IAM policy	Remove from group

• Click **Add Permissions** to pop up the **Add Permissions** dialog box, you can associate a new policy for the user, and the gray policy in the dialog box indicates the policy that the user has associated.



×

#### Add Permissions

olicies		Search by policy name	Q				
here are c	currently 10 items, 1 has been s	elected		There are	currently 2 items, 0 has been	selected	
	Policy Name	All 🗸			Policy Name	Policy Type	
	IAMPolicy Create IAM policy	Custom Policy	^		IAMPolicy Create IAM policy	Custom Policy	
	oosread oos read	Custom Policy			cloudtrail cloudtrail	Custom Policy	
1	ooswrite oos write	Custom Policy	<				
	AdministratorAccess Provides full access to service s and resources.	e System Policy					
	IAMReadOnlyAccess Provides read only access to	System Policy					

• Select policies that need to be removed, click **Remove Permissions** to delete multiple policies for the IAM user; click the **Remove Permission** to remove the associated policy; click **Remove from group**, the user will be removed from the corresponding group, and disconnect the policy associated with the group.

### 7.2.2.4 View and Modify the Group

Click **Groups**, you can view the IAM group, add the IAM user to the group or remove the IAM user from the group.

IA	M / Users / test1							
	Basic Information	test1@32fefj64y54gi	c 🗇			Creation Time:	2024-03-13 15:54:38 UTC+0800	
	Security Credential	AccessKeys	Permissions	Groups	Tags	озет туре.	JAN USET	
4	Add to Groups	Remove from Group						
	There are currently 1 items Group Name	, 0 has been selected :			Attached Policy		Operation	
	IAM1				IAMPolicy		Remove from Group	

• Click Add to Groups to pop up the Add to Groups dialog box, you can select the group that the user needs to join, and click Confirm. The gray user group in the pop-up box indicates the user group that the user has joined.



Add to (	Groups				×
Groups		Search by group name Q			
There are cu	urrently 5 items, 1 has bee	n selected		There are currently 1 items, 0 has been selecte	d
	Group Name			Group Name	
~	aaa			IAM1	
	IAM1				
	OOSuser1				
	test		<		
	testa				
					>
					Cancel Confirm

• Select groups to be removed and click **Remove from Group** to remove the user from multiple groups; or click **Remove from Group** button of the corresponding group to remove the user from the group.

### 7.2.2.5 View and Modify the Tag

Click Tags, you can view, edit, add or delete tags for IAM user.

IAM / Users / test					
Basic Information User Name: User ID:	test@32fef64y54gc []] 6917a327e32648ed8167f5d55e371433		Creation Time: User Type:	2020-08-05 1558:01 UTC+0800 JAM User	
Security Credential A	ccessKeys Permissions Groups Tags				
There are currently 1 items, 0 h	as been selected				
Кеу		Value(Optional)		Operation	
□ 1		test		Edit Delete	

- Add tags: Click Add Tags, and fill in the tag and value. The value can be empty, a user can have up to 10 tags.
- **Delete tags**: select tags to be deleted and click **Delete Tags** to delete multiple tags; or click **Delete** to delete the tag.
- Edit tag: Click Edit to modify the tag value.



## 7.2.3 Delete the IAM User

On the **Users** page, select IAM users to be deleted and click **Delete** to delete multiple IAM users; or click **Delete** behind the corresponding user to delete the IAM user.

When deleting a user, a dialog box will pop up to confirm whether to delete the selected user.

## 7.2.4 IAM User Login

For root users or IAM users with management user permissions, go to **Users Management > Users** and enter the specific user page. On the user details page, click **Security Credential**, and copy the **Console Login Link** to get the login link of the IAM user. Enter the user name and login password, and follow the prompts to log in.

The interfaces of IAM users and root users are basically the same, and the functions of IAM users are determined by authorization. If you need more permissions, you can apply to the root user or IAM users with management user permissions.

## 7.3 IAM User Groups

Administrators create user groups and authorize user groups. Users in the group can obtain the same authority policy, which is convenient for managing users.

Enter **Users** Management > User Groups, you can create a new user group, add permissions for the user group, delete user group, add IAM users for the user group, manage user groups.

IAM 🕗 U	VI / User Groups								
Create	Create Group Delete Q								
There are	currently 7 items, 0 has been selected								
	Group Name	Users	Polices	Creation Time	Operation				
	groupte	4	0	2020-06-02 11:17:02 UTC+0800	Add Permissions Add Users Delete Management				
	oos-read	3	1	2020-05-13 14:48:03 UTC+0800	Add Permissions Add Users Delete Management				
	test	0	3	2023-07-10 11:20:05 UTC+0800	Add Permissions Add Users Delete Management				
	test1	0	1	2020-06-02 15:39:41 UTC+0800	Add Permissions Add Users Delete Management				
	test12345	0	0	2020-08-04 17:37:45 UTC+0800	Add Permissions Add Users Delete Management				
	test_wu1	0	0	2021-09-24 10:05:20 UTC+0800	Add Permissions Add Users Delete Management				
	testa	1	1	2023-04-18 17:10:12 UTC+0800	Add Permissions Add Users Delete Management				

## 7.3.1 Create an IAM User Group

Click IAM > Users Management > User Groups > Create Group, enter Create Group to create an IAM user group.

1. Set Group



IAM / User Groups	/ Create Group			
	1 Set Group	2 Set Permissions	3 Review	(d) Succeed
Set Group Name Group Name	The group name cannot be modified after it is succe	ssfully created, please name it carefully		
				Cancel Next, Permissions

Set user group name: After the user group name is created successfully, it cannot be modified. The naming of user groups shall comply with the following rules:

- The name of the IAM user group must be unique within your OOS account.
- The value is a string of 1 to 128 insensitive letters, numbers, or special characters. The special characters only include underscores (\_), hyphens (-), comma (,), period (.), plus sign (+), equal sign (=), and at sign (@).

	Set Group	2 Set Permissions	3 Review	(4) Succeed
ttach f	Permissions Policies (optional)			
Create	Policy		IIA	✓ Policy Name Q
urrently	selected 1 items:IAMReadOnlyAccess			
	Policy Name viewpolicy	Policy Type Custom Policy	Description 盘石线略	
	viewuser	Custom Policy	宣石IAM用户	
	web	Custom Policy	网站管理	
	AdministratorAccess	System Policy	Provides full access to services and resource	es,
~	IAMReadOnlyAccess	System Policy	Provides read only access to IAM.	
	OOSCloudTrailFullAccess	System Policy	Provides full access to OOS CloudTrail.	
	OOSCI oud TrailRead Only Access	System Policy	Provides read only access to OOS CloudTra	il.
	OOSFullAccess	System Policy	Provides full access to all buckets.	
	OOSIAMFullAccess	System Policy	Provides full access to IAM.	
	OOSReadOnlyAccess	System Policy	Provides read only access to all buckets.	

#### 2. Set Permissions

You can search for matching policies in the search box, and the searched matching policies are displayed in the form of a list. You can add policies to the user group by checking the corresponding policies.

**Note**: You can add a policy to the user group when you create the user group, or you can add a policy to the user group after the user group is created. An IAM user can have up to 10 policies.



### 3. Review

The information of the newly created user group can be audited. If there is any need to modify, you can click the edit icon to modify.

IAM / User Groups / Create Group	Set Permissions	Beview	(d) Succeed
Group 🗹 Group Name group-read			
Permissions The following policies will be attached to the gr	up 🖸		
Policy Name	Policy Type	Description	
IAMReadOnlyAccess	System Policy	Provides read only access to IAM.	
			Previous Next, Create Group

### 4. Succeed

IAM / User Groups / Create Group				
$\odot$		$\odot$	 $\bigcirc$	 4
Set Group		Set Permissions	Review	Succeed
Created Group created successfully You have successfully created a user group Return to Group	), you can add IAM users to the group for management			



## 7.3.2 View and Modify the IAM User Group

Click IAM > Users Management > User Groups, you can view and edit the user group.

IAM / U	ser Groups				
Create	Group Delete				Search by user group name Q C
There are	currently 8 items, 0 has been selected				
	Group Name	Users	Polices	Creation Time	Operation
	group-read	0	1	2023-07-11 15:38:50 UTC+0800	Add Permissions Add Users Delete Management
	groupte	4	0	2020-06-02 11:17:02 UTC+0800	Add Permissions Add Users Delete Management
	oos-read	3	1	2020-05-13 14:48:03 UTC+0800	Add Permissions Add Users Delete Management
	test	0	3	2023-07-10 11:20:05 UTC+0800	Add Permissions Add Users Delete Management
	test1	0	1	2020-06-02 15:39:41 UTC+0800	Add Permissions Add Users Delete Management
	test12345	0	0	2020-08-04 17:37:45 UTC+0800	Add Permissions Add Users Delete Management
	test_wu1	0	0	2021-09-24 10:05:20 UTC+0800	Add Permissions Add Users Delete Management
	testa	1	1	2023-04-18 17:10:12 UTC+0800	Add Permissions Add Users Delete Management

### 7.3.2.1 Add or delete IAM users

#### Add IAM users

Add Users

On the User Groups page, click Add Users in the corresponding user group operation, and the Add Users dialog box pops up to add users to the user group.

Users		Search by user name	Q
There are o	urrently 10 items, 0 has been se	lected	
	User Name		
	test		^
	test111		
	test12345		
	test1_bucket		
	test3		
	test4		
	test_a1		
	test_a2		~

Click the corresponding user group name or Management to enter the user group details page, and click User > Add User to add users to the user group.

IAM

 $\times$ 

Cancel



### • Remove IAM users

Click the corresponding user group name or **Management** to enter the user group details page. Click **User**, select users to be removed, and click **Remove User** to delete multiple users for the user group; Or click **Remove User** behind the corresponding user to remove the corresponding user for the user group.



### 7.3.2.2 View and Modify Permissions

IAM / User Groups /	IAM1				
Basic Information					
Group Name	IAM1@32fefj64y54gc 🗇		Creation Time	2024-03-13 17:11:13 UTC+0800	
Group ARN	Group ARN am.ctyuniam:32fefj64y54gc.group/IAM1				
User Permission	IS				
Add Permissions	Remove Permissions				
There are currently 1 item	s, 0 has been selected				
Policy Name		Policy Type ~	Description		Operation
LAMPolicy		Custom Policy	Create IAM policy		Remove Permissions

### • Add permissions

Enter User Groups, click Add Permissions, and the Add Permissions dialog box pops up to add policies for the user group. The gray policy in the pop-up box indicates the policy associated with the user group.

licies	Search by policy name	a			
ere are currently 10 items, 1 h	as been selected		There are o	currently 2 items, 0 has been selecte	d
<ul> <li>Policy Name</li> </ul>	All $\sim$			Policy Name	Policy Type
loudTrail.		^		IAMPolicy	Custom Policy
OOSCIoudTrailRead ss Provides read only	IOnlyAcce System Policy access to			Create IAM policy	System Policy
OOS CloudTrail.				Provides read only access to IAM.	
OOSFullAccess Provides full access kets.	to all buc System Policy	<			
OOSIAMFullAccess Provides full access	to IAM. System Policy				
OOSReadOnlyAcce	ss access to System Policy				

Click the corresponding user group name to enter the user group detailed information page, click
 Permissions > Add Permissions to add policies for the user group.

#### • Remove Permissions

On the user group details page, click **Permissions**, select the policy to be removed, and click **Remove Permissions** to delete the policies for the user group; or click **Remove Permissions** behind the corresponding policy to delete the corresponding policy for the user group.



## 7.3.3 Delete the User Group

On the **User Groups** page, select user groups to be deleted and click **Delete** to delete multiple user groups; or click **Delete** behind the corresponding user group to delete the user group.



## 7.4 Policy Management

A policy describes a collection of permission information in a JSON format. The IAM user created by the administrator does not have any permissions before there is no authorization policy. Only when the policy is authorized to the user group or user, the user has the corresponding authority. IAM supports the system policy and custom policy:

• **System policy**: The policy is created by the OOS, users can directly use according to their own needs. But the user can only use it and cannot modify the policy.

• **Custom policy**: The policy is created by the user, and the user can modify and delete the policy.

Enter **IAM** > **Policy Management**, you can view policies, create the custom policy, delete the custom policy and manage the policies.

Object-Oriented Storage	IAM / Policy Management						
Statistics Overview	Create Delete					Search by policy name	
Buckets	There are currently 36 items, 0 has been selected						
Cloudtrail 👻	Policy Name	Citations	Last modified time	Description	Policy Type ~	Operation	
IAM 🍵	viewpolicy	1	2020-06-04 09:09:24 U IC+0800	金石浅梢	Custom Policy	Attach Delete Management	
Overview	viewuser	0	2020-05-02 11:22:43 UTC+0800	查看IAM用户	Custom Policy	Attach Delete Management	
Users Management 👻	web	0	2020-05-28 16:31:09 UTC+0800	网站管理	Custom Policy	Attach Delete Management	
Policy	AdministratorAccess	0	2020-05-11 09:21:30 UTC+0800	Provides full access to services and resources.	System Policy	Attach Management	
Management	IAMReadOnlyAccess	2	2020-05-11 09:31:25 UTC+0800	Provides read only access to IAM.	System Policy	Attach Management	
Security Setting	OOSCloudTrailFullAccess	1	2020-05-11 09:32:10 UTC+0800	Provides full access to OOS CloudTrail.	System Policy	Attach Management	
Resource Package	OOSCloudTrailReadOnlyAccess	1	2020-05-11 09:32:56 UTC+0800	Provides read only access to OOS CloudTrail.	System Policy	Attach Management	
	OOSFullAccess	-1	2020-05-11 09:22:20 UTC+0800	Provides full access to all buckets.	System Policy	Attach Management	
	OOSIAMFullAccess	1	2020-05-11 09:25:00 UTC+0800	Provides full access to IAM.	System Policy	Attach Management	
	OOSReadOnlyAccess	1	2020-05-11 09:23:05 UTC+0800	Provides read only access to all buckets.	System Policy	Attach Management	

## 7.4.1 System Policy

The currently supported system policies are as follows:

Policy	Description					
AdministratorAccess	All permissions are the same as those of the root user.					
IAMReadOnlyAccess	IAM related get and list permissions.					
OOSCloudTrailFullAccess	Related permissions required for CloudTrail, including:					
	• OOS: CreateBucket, DeleteBucket, GetBucket,					
	HeadBucket, GetService, GetObject.					
	ClouldTrail: All CloudTrail operations.					
OOSCloudTrailReadOnlyAccess	CloudTrail related read permissions, including:					
	GetTrailStatus, , DescribeTrails, LookupEvents,					
	GetEventSelectors, GetObject, GetService.					
OOSFullAccess	All permissions of OOS, including all operations of Bucket and					
	Object.					
OOSIAMFullAccess	All permissions of IAM.					
OOSReadOnlyAccess	OOS related read permissions, including Bucket and Object					
	GET and List related operations.					



## 7.4.2 Custom Policy

### 7.4.2.1 Create the Custom Policy

Click IAM > Policy Management > Create to enter Create Policy.

Note: For specific resources and APIs corresponding to each Action, please refer to Action List and

### Corresponding API.

IAM / Policy / Create Policy	/			
Basic Information Policy Name Policy Description		li.		
Basic Information Use visu Visual Policy Editor JSC	al editor or JSON for policy editing DN re, and the added statement will be	shown policy statement list. For more information, please see how to	create policy.	
Add Policy Statement Service Effect	Action	Resource	Condition	Operation
		No policy statements have been a	dded yet.	Canad Same

Name	Description
Policy Name	The value is a string of 1 to 128 insensitive letters, numbers, or special
	characters. The special characters only include underscores (_), hyphens
	(-), comma (,), period (.), plus sign (+), equal sign (=), and at sign (@).
	Note: The policy name must be unique.
Policy Description	Optional. A brief description of the policy.
Policy Content	It can be achieved through Visual Editor or JSON programming.

### • Visual Editor

Click **Add Policy Statement**, the Add Policy Statement dialog box pops up, and you can configure permissions for the policy as needed.



Select Product/Service	005		$\sim$				
Effect	Allow Deny						
Action Type	Action NotAction						
Actions	You can also search the actions you need Q						
	• 🗌 All Actio	ns	Exp	and all $ imes$			
	▼ □ List						
	🗌 Lis	tBucket					
	🗌 Lis	tAIIMyBucket					
	Ge	tRegions					
	Read						
Write							
	Permissions Management						
Resource Type	Resource	NotResource					
Resources	All Resources      Specific						
Conditions							
	Condition					×	
	Condit Key	Select condition key	· · · · · · · · · · · · · · · · · · ·	~			
	Operat	Select operator	· · · · · · · · · · · · · · · · · · ·	~			
	Condit Value	Condition Value					
						)	
					Cancel	Save	

Iteam	Description		
Select	You can define the type of selected service:		
Product/Service	• 00S		
	• cloudtrail		
	• statistics		
	• iam		
Effect	Effect on selection operation:		
	• Allow: According to the selected operation category, the performance of the		
	selected operation effect is allowed.		

×


Т

Г

	• Deny: According to the selected operation category, the performance of the				
	selected operation effect is denied.				
Action Type	<ul> <li>Select the action type. You can search fuzzy or precise search in the search box, and the searched operation will be displayed in the action list.</li> <li>Action Type:</li> <li>Action: Match the specified operation.</li> <li>NotAction: The policy element that matches the operation other than the specified operation. When using NotAction:</li> <li>If Allow effects are used, all applicable operations or services not listed are permitted.</li> <li>If the Deny effect is used, such unlisted operations or services will be denied.</li> </ul>				
Actions	You can select the policy that needs to be implemented for the operation in the action list. See the <b>Action List</b> for the policies contained in each service				
Resource Type	The resource is the entity on which the policy takes effect:				
	<ul> <li>Resource: The resource for which the policy takes effect.</li> </ul>				
	<ul> <li>NotResource: For resources other than the specified resource, the policy takes effect.</li> </ul>				
Resources	You can specify All Resources or Specific resources. When selecting a specific				
	resource, a specific resource ARN must be added.				
	For statistics, resources cannot be selected, all resources are defaulted.				
Conditions	The conditions under which the user policy takes effect.				
(optional)	<b>Note</b> : If the input of the condition value is time, convert the time that needs to be set				
	to UTC+0 time.				

#### Action List

Product/Service	Description		
OOS	List:		
	<ul> <li>ListBucket</li> </ul>		
	<ul> <li>ListAllMyBucket</li> </ul>		
	• GetRegions		
	Read:		
	<ul> <li>ListBucketMultipartUploads</li> </ul>		
	• GetBucketAcl		
	GetBucketLocation		
	• GetBucketPolicy		
	<ul> <li>GetLifecycleConfiguration</li> </ul>		
	<ul> <li>GetBucketWebsite</li> </ul>		
	• GetBucketCORS		
	<ul> <li>GetBucketLogging</li> </ul>		
	• GetObject		



	<ul> <li>ListMultipartUploadParts</li> </ul>				
	<ul> <li>GetBucketInventoryConfiguration</li> </ul>				
	Write:				
	• DeleteBucket				
	<ul> <li>PutLifecycleConfiguration</li> </ul>				
	<ul> <li>PutBucketWebsite</li> </ul>				
	<ul> <li>DeleteBucketWebsite</li> </ul>				
	<ul> <li>PutBucketCORS</li> </ul>				
	<ul> <li>PutBucketLogging</li> </ul>				
	<ul> <li>PutObject</li> </ul>				
	• DeleteObject				
	<ul> <li>DeleteMultipleObjects</li> </ul>				
	AbortMultipartUpload				
	• PutBucket				
	<ul> <li>PutBucketInventoryConfiguration</li> </ul>				
	Permissions Management:				
	<ul> <li>PutBucketPolicy</li> </ul>				
	<ul> <li>DeleteBucketPolicy</li> </ul>				
cloudtrail	List				
	• DescribeTrails				
	<ul> <li>LookupEvents</li> </ul>				
	Read:				
	• GetEventSelectors				
	• GetTrailStatus				
	Write:				
	• PutEventSelectors				
	• StopLogging				
	• CreateTrail				
	• UpdateTrail				
	• DeleteTrail				
	• StartLogging				
statistics	GetAccountStatistcsSummary				
iam	List:				
	• GetAccountSummary				
	• GetLoginProfile				
	• ListAccessKeys				
	• ListUsers				
	• ListUserTags				
	• ListGroups				



•	ListGroupsForUser
•	ListPolicies
•	ListAttachedGroupPolicies
•	ListAttachedUserPolicies
•	ListEntitiesForPolicy
•	ListVirtualMFADevices
•	ListMFADevices
Re	ead:
•	GetUser
•	GetGroup
•	GetPolicy
•	GetAccountPasswordPolicy
•	GetAccountLoginSecurityPolicy
Wr	ite:
•	CreateAccessKey
•	DeleteAccessKey
•	UpdateAccessKey
•	CreateUser
•	DeleteUser
•	TagUser
•	UntagUser
•	CreateGroup
•	DeleteGroup
•	AddUserToGroup
•	RemoveUserFromGroup
•	ChangePassword
•	UpdateAccountPasswordPolicy
•	DeleteAccountPasswordPolicy
•	UpdateAccountLoginSecurityPolicy
•	DeleteAccountLoginSecurityPolicy
•	CreateVirtualMFADevice
•	DeleteVirtualMFADevice
•	EnableMFADevice
•	DeactivateMFADevice
•	CreateLoginProfile
•	DeleteLoginProfile
•	UpdateLoginProfile
Pe	rmissions Management:
	CreatePolicy

IAM



•	DeletePolicy
•	AttachUserPolicy
•	DetachUserPolicy
•	AttachGroupPolicy
•	DetachGroupPolicy

#### **Condition description**

Condition Keys	Condition Operators	Condition Values
ctyun:CurrentTime	<ul> <li>DateEquals: Match the specified date.</li> <li>DateNotEquals: Not equal to the specified date.</li> <li>DateLessThan: Before the specified date.</li> <li>DateLessThanEquals: Before or equal to the specified date.</li> <li>DateGreaterThan: Later the specified date.</li> <li>DateGreaterThanEquals: Later or equal to the specified date.</li> </ul>	The format is yyyy-MM- dd'T'HH:mm:ss'Z'. Such as 2019-12- 18T09:00:00Z. DateEquals and DateNotEquals are accurate to days, others are accurate to seconds. Note: Convert the time to be set to the time in UTC+0 time zone.
ctyun:Sourcelp	<ul> <li>IpAddress: Match the specified IP address or IP range.</li> <li>NotIpAddress: Match all IP addresses except the specified IP address or IP range.</li> </ul>	IPv4: The value is in dotted decimal notation. IPv6: The address is a 32- digit hexadecimal number, in the format of X:X:X:X:X:X:X:X. If an address range is specified, a mask is added after the IP address, such as 192.163.1.5/3.
ctyun:userid	<ul> <li>StringEquals: Matches exactly the specified value and is case sensitive.</li> <li>StringNotEquals: Does not match the specified value and is case sensitive.</li> <li>StringEqualsIgnoreCase: Matches exactly the specified value and is not case sensitive.</li> <li>StringNotEqualsIgnoreCase: Does not match the specified value and is not case sensitive.</li> <li>StringLike: Matches exactly the specified value and is not case sensitive.</li> <li>StringLike: Matches exactly the specified value by padding wildcards, wildcards can be multicharacter matching wildcards (*) or single-</li> </ul>	The value is a string of 1 to 32 lowercase letters and numbers. The operators for StringLike and StringNotLike can include wildcard characters.



	character matching wildcards (?).	
	• StringNotLike: Does not match the specified	
	value and is case sensitive, or does not match	
	the specified value by padding wildcards.	
ctyun:username	• StringEquals: Matches exactly the specified	The value is a string of 1 to
	value and is case sensitive.	64 insensitive letters,
	• StringNotEquals: Does not match the	numbers, or special
	specified value and is case sensitive.	characters. The special
	• StringEqualsIgnoreCase: Matches exactly	underscores () hyphens
	the specified value and is not case sensitive.	(-), comma (,), period (.),
	• StringNotEqualsIgnoreCase: Does not match	plus sign (+), equal sign (=),
	the specified value and is not case sensitive.	and at sign (@).
	• StringLike: Matches exactly the specified	Note: The condition
	value, or is similar to the specified value by	operators for StringLike
	padding wildcards, wildcards can be multi-	and StringNotLike can
	character matching wildcards (*) or single-	
	character matching wildcards (?).	
	• StringNotLike: Does not match the specified	
	value and is case sensitive, or does not match	
	the specified value by padding wildcards.	
ctyun:UserAgent	• StringEquals: Matches exactly the specified	A string that can contain
	value and is case sensitive.	special characters.
	• StringNotEquals: Does not match the	
	• StringNotEquals: Does not match the specified value and is case sensitive.	
	<ul> <li>StringNotEquals: Does not match the specified value and is case sensitive.</li> <li>StringEqualsIgnoreCase: Matches exactly</li> </ul>	
	<ul> <li>StringNotEquals: Does not match the specified value and is case sensitive.</li> <li>StringEqualsIgnoreCase: Matches exactly the specified value and is not case sensitive.</li> </ul>	
	<ul> <li>StringNotEquals: Does not match the specified value and is case sensitive.</li> <li>StringEqualsIgnoreCase: Matches exactly the specified value and is not case sensitive.</li> <li>StringNotEqualsIgnoreCase: Does not match</li> </ul>	
	<ul> <li>StringNotEquals: Does not match the specified value and is case sensitive.</li> <li>StringEqualsIgnoreCase: Matches exactly the specified value and is not case sensitive.</li> <li>StringNotEqualsIgnoreCase: Does not match the specified value and is not case sensitive.</li> </ul>	
	<ul> <li>StringNotEquals: Does not match the specified value and is case sensitive.</li> <li>StringEqualsIgnoreCase: Matches exactly the specified value and is not case sensitive.</li> <li>StringNotEqualsIgnoreCase: Does not match the specified value and is not case sensitive.</li> <li>StringLike: Matches exactly the specified</li> </ul>	
	<ul> <li>StringNotEquals: Does not match the specified value and is case sensitive.</li> <li>StringEqualsIgnoreCase: Matches exactly the specified value and is not case sensitive.</li> <li>StringNotEqualsIgnoreCase: Does not match the specified value and is not case sensitive.</li> <li>StringLike: Matches exactly the specified value, or is similar to the specified value by</li> </ul>	
	<ul> <li>StringNotEquals: Does not match the specified value and is case sensitive.</li> <li>StringEqualsIgnoreCase: Matches exactly the specified value and is not case sensitive.</li> <li>StringNotEqualsIgnoreCase: Does not match the specified value and is not case sensitive.</li> <li>StringLike: Matches exactly the specified value, or is similar to the specified value by padding wildcards, wildcards can be multi-</li> </ul>	
	<ul> <li>StringNotEquals: Does not match the specified value and is case sensitive.</li> <li>StringEqualsIgnoreCase: Matches exactly the specified value and is not case sensitive.</li> <li>StringNotEqualsIgnoreCase: Does not match the specified value and is not case sensitive.</li> <li>StringLike: Matches exactly the specified value, or is similar to the specified value by padding wildcards, wildcards can be multicharacter matching wildcards (*) or single-</li> </ul>	
	<ul> <li>StringNotEquals: Does not match the specified value and is case sensitive.</li> <li>StringEqualsIgnoreCase: Matches exactly the specified value and is not case sensitive.</li> <li>StringNotEqualsIgnoreCase: Does not match the specified value and is not case sensitive.</li> <li>StringLike: Matches exactly the specified value, or is similar to the specified value by padding wildcards, wildcards can be multicharacter matching wildcards (*) or single-character matching wildcards (?).</li> </ul>	
	<ul> <li>StringNotEquals: Does not match the specified value and is case sensitive.</li> <li>StringEqualsIgnoreCase: Matches exactly the specified value and is not case sensitive.</li> <li>StringNotEqualsIgnoreCase: Does not match the specified value and is not case sensitive.</li> <li>StringLike: Matches exactly the specified value, or is similar to the specified value by padding wildcards, wildcards can be multicharacter matching wildcards (*) or single-character matching wildcards (?).</li> <li>StringNotLike: Does not match the specified</li> </ul>	
	<ul> <li>StringNotEquals: Does not match the specified value and is case sensitive.</li> <li>StringEqualsIgnoreCase: Matches exactly the specified value and is not case sensitive.</li> <li>StringNotEqualsIgnoreCase: Does not match the specified value and is not case sensitive.</li> <li>StringLike: Matches exactly the specified value, or is similar to the specified value by padding wildcards, wildcards can be multicharacter matching wildcards (*) or singlecharacter matching wildcards (?).</li> <li>StringNotLike: Does not match the specified value and is case sensitive, or does not match</li> </ul>	
	<ul> <li>StringNotEquals: Does not match the specified value and is case sensitive.</li> <li>StringEqualsIgnoreCase: Matches exactly the specified value and is not case sensitive.</li> <li>StringNotEqualsIgnoreCase: Does not match the specified value and is not case sensitive.</li> <li>StringLike: Matches exactly the specified value, or is similar to the specified value by padding wildcards, wildcards can be multicharacter matching wildcards (*) or singlecharacter matching wildcards (?).</li> <li>StringNotLike: Does not match the specified value by padding value by padding wildcards (?).</li> </ul>	
ctyun:Referer	<ul> <li>StringNotEquals: Does not match the specified value and is case sensitive.</li> <li>StringEqualsIgnoreCase: Matches exactly the specified value and is not case sensitive.</li> <li>StringNotEqualsIgnoreCase: Does not match the specified value and is not case sensitive.</li> <li>StringLike: Matches exactly the specified value, or is similar to the specified value by padding wildcards, wildcards can be multicharacter matching wildcards (*) or singlecharacter matching wildcards (?).</li> <li>StringNotLike: Does not match the specified value and is case sensitive, or does not match the specified value by padding wildcards.</li> <li>StringEquals: Matches exactly the specified</li> </ul>	A string that can contain



	<ul> <li>StringNotEquals: Does not match the specified value and is case sensitive.</li> <li>StringEqualsIgnoreCase: Matches exactly the specified value and is not case sensitive.</li> <li>StringNotEqualsIgnoreCase: Does not match the specified value and is not case sensitive.</li> <li>StringLike: Matches exactly the specified value, or is similar to the specified value by padding wildcards, wildcards can be multicharacter matching wildcards (*) or single-character matching wildcards (?).</li> </ul>	
	value and is case sensitive. or does not match	
	the specified value by padding wildcards.	
ctyun:SecureTransport	Bool: Boolean match.	• true
		• false
ctyun:MultiFactorAuthP	Boo1: Boolean match.	• true
resent	Note: Only IAM service supports this condition	• false
	operator.	An integer
ae	NumericEquals: Match the specified value.	An integer.
3~	<ul> <li>NumericNotEquals: Negatively match the apacified volus</li> </ul>	
	Specified value.	
	value	
	<ul> <li>NumericlessThanEquals: Less than or equal to</li> </ul>	
	the specified value	
	<ul> <li>NumericGreaterThan: Greater than the</li> </ul>	
	specified value.	
	<ul> <li>NumericGreaterThanEquals: Greater than or</li> </ul>	
	equal to the specified value.	
	Note: Only IAM service supports this condition	
	operator.	
oos:prefix	• StringEquals: Matches exactly the specified	The value is a string.
	value and is case sensitive.	Note: The condition key is
	• StringNotEquals: Does not match the	only valid for the operation
	specified value and is case sensitive.	oos:ListBucket.
	• StringEqualsIgnoreCase: Matches exactly	
	the specified value and is not case sensitive.	
	• StringNotEqualsIgnoreCase: Does not match	



		the specified value and is not case sensitive.	
	•	StringLike: Matches exactly the specified	
		value, or is similar to the specified value by	
		padding wildcards, wildcards can be multi-	
		character matching wildcards (*) or single-	
		character matching wildcards (?).	
	•	StringNotLike: Does not match the specified	
		value and is case sensitive, or does not match	
		the specified value by padding wildcards,	
		wildcards can be multi-character matching	
		wildcards (*) or single-character matching	
		wildcards (?).	
oos:x-amz-acl	•	StringEquals: Matches exactly the specified	The value is a string.
		value and is case sensitive.	The value:
	•	StringNotEquals: Does not match the	private: only the
		specified value and is case sensitive.	owner can operate the
	•	StringEqualsIgnoreCase: Matches exactly	• public-read: all can
		the specified value and is not case sensitive.	read the bucket.
	•	StringNotEqualsIgnoreCase: Does not match	• public-read-write:
		the specified value and is not case sensitive.	all can operate the
	•	StringLike: Matches exactly the specified	bucket, including read
		value, or is similar to the specified value by	and write operations.
		padding wildcards, wildcards can be multi-	hucket you can use this
		character matching wildcards (*) or single-	condition key to control the
		character matching wildcards (?).	type of bucket ACL. The
	•	StringNotLike: Does not match the specified	condition key is only valid for
		value and is case sensitive, or does not match	the operation authority of
		the specified value by padding wildcards,	oos:PutBucket.
		wildcards can be multi-character matching	
		wildcards (*) or single-character matching	
		wildcards (?).	

• JSON programming authorization

You can use the JSON to add the content of the policy. Take the following policy as an example to illustrate the grammatical structure of the JSON programming policy.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
```



```
"Effect": "Allow",
     "Action": [
       "oos:ListAllMyBuckets",
       "oos:GetBucketLocation"
     ],
     "Resource": " arn:ctyun:oos::02elbe4neijs7:* ",
     "Condition" : {
               "DateGreaterThan" : {
                  "ctyun:CurrentTime" : "2019-01-16T12:00:00Z"
                },
               "DateLessThan": {
                  "ctyun:CurrentTime" : "2019-01-16T12:00:00Z"
                },
                "IpAddress" : {
                   "ctyun:SourceIp" : ["192.0.2.0/24", "203.0.113.0/24"]
               }
         }
     }
   ]
}
```

#### JSON programming parameter table

Parameter		Description	Value
Version		Policy version	2012-10-17
Version Statement: Policy authorization statement. There can be multiple Statements, representing different	<ul> <li>Action: Match the specified</li> </ul>	Policy versionEffectonselectionoperation.Action type.	<ul> <li>2012-10-17</li> <li>Allow: Allow execution.</li> <li>Deny: Deny execution.</li> <li>Note: When the Effect in the same Action contains both Allow and Deny, the Deny priority principle is followed.</li> <li>The format is as follows:</li> <li>Service:</li> </ul>
authorization structures.	<ul> <li>operation.</li> <li>NotAction: The policy element that matches the operation other than the specified operation.</li> <li>Note: For a Statement, choose one of Action and NotAction.</li> </ul>		<ul> <li>oos</li> <li>cloudtrail</li> <li>statistics</li> <li>iam</li> <li>Actions: For details, see Action List.</li> </ul>



<ul> <li>Resource : The</li> </ul>	Resource type.	The format can be:
resource for which		arn:ctyun:service::accountid
the policy takes		:resource
effect.		arn:ctyun:service::accountid
<ul> <li>NotResource: For</li> </ul>		:resourcetype/resource
resources other		Note:
than the specified		<ul> <li>service: Service name.</li> </ul>
resource. the		• accountid: Account ID.
policy takes effect.		• <i>Resource</i> : Specific resources.
p		When specifying resources, you
		can use wildcards, where *
		represents any combination of
		characters, ? Represents any
		single character. For example, oos
		can be represented as:
		arn:ctyun:oos:: <i>accountID:buc</i>
		<i>ket/object</i> , where <i>bucket</i> and
		object are the actual resource
		names of the user.
		• <i>Resourcetype</i> : Resource Type.
		The wildcard * represents all
		resource types. Different services
		have different corresponding
		resourcetypes:
		■ The resource type of iam can
		be: <i>user</i> , <i>group</i> , <i>policy</i> , <i>mfa</i> or
		*.
		The resource type of cloudtrail
		can be: <i>trail</i> or *.
		The resource of statistic can
		be *.
Condition	The conditions	Condition syntax structure is as follows:
	under which the	"Condition": {"Condition
	user policy takes	Operator A": {"Condition
	effect.	Key A":["Condition Value
		A1", "Condition Value
		A2",]}, "Condition
		Key B"·["Condition Value
		B1", "Condition Value



	B2",…	] } }				
	Note:	The C	Conditio	n eleme	nt o	can
	consist	of	multip	le con	ditio	ons.
	Conditi	ons inc	lude: con	dition ope	erato	ors,
	conditio	on keys	s, and co	ndition va	lues	s. A
	conditio	on ke	y can	correspo	nd	to
	multiple	e condi	tion value	es.		

#### • ...IfExists Condition Operators

IfExists: If keywords exist in the request, the keywords are processed according to the conditions described in the policy. If the keyword does not exist, the condition element will evaluate to true. Currently, Only Bool and numeric operators support the IfExists condition operator. The expression: Operator IfExists, such as BoolIfExists, NumericEqualsIfExists. About the use of ...IfExists, see **Example1** and **Example2**.

#### Example1

• Deny console requests that do not use MFA authentication, do not deny the console requests that use MFA authentication, and API requests that use keys. However, if the console requests that use MFA authentication, and API requests are allowed, you need to write explicit allow statements.

```
"Effect" : "Deny",
"Condition" : { "Bool" : { "ctyun:MultiFactorAuthPresent" : false } }
```

 Deny console requests that do not use MFA authentication and API requests that use keys, do not deny the console requests that use MFA authentication. However, if the console requests that use MFA authentication are allowed, you need to write explicit allow statements.

```
"Effect" : "Deny",
"Condition" : { "BoolIfExists" : { "ctyun:MultiFactorAuthPresent" : false } }
```

#### Example2

• Allows requests using MFA authentication within 1800 seconds and API requests using keys.

```
"Effect" : "Allow",
"Condition" : { " NumericLessThanEqualsIfExists" : { "ctyun:MultiFactorAuthAge " :
1800 } }
```

 Allows requests using MFA authentication within 1800 seconds, but requests using MFA authentication greater than 1800 seconds and not using MFA authentication (including API requests) are not allowed.

```
"Effect" : "Allow",
"Condition" : { " NumericLessThanEquals" : { "ctyun:MultiFactorAuthAge " : 1800 } }
```



### 7.4.2.2 Modify the Custom Policy

Enter IAM > Policy Management, click the corresponding policy name or Management, enter the policy details page, click Policy Content > Edit Policy, you can edit the policy through Visual Editor or JSON programming. For detailed editing method can refer to Create the Custom Policy.

IAM / Policy Ma	M / Policy Management / bucket-read				
OOS IAM Cons	sole (bucket-read	Ð			
Visual Editor	JSON				
• Each time	the visual editor ad	ids a statement, the added statement will be displa	yed in the policy summary list below		
Add Policy Sta	tement				
Service	Effect	Action	Resource	Condition	Operation
005	oos Allow oosListBucket more 14 items * X				
Please confirm whether you have the right to create a policy and its related permissions. If the permissions are insufficient, it may not be able to save successfully.					

### 7.4.2.3 Delete the Custom Policy

On the **Policy Management** page, select polices to be deleted and click **Delete** to delete multiple policies; or click **Delete** behind the corresponding policy to delete the policy.

IAM / Policy Management					
Create Delete There are currently 36 items, 0 has be	een selected				Search by policy name Q
Policy Name	Citations	Last modified time	Description	Policy Type ~	Operation
iamsecurity	0	2020-07-15 14:50:59 UTC+0800	IAM策略	Custom Policy	Attach Delete Management
lifecycle	0	2020-05-29 10:24:05 UTC+0800	生命周期	Custom Policy	Attach Delete Management
listallbucket	0	2020-05-28 15:22:50 UTC+0800	容器列表	Custom Policy	Attach Delete Management
ListBucket	0	2023-01-30 17:22:14 UTC+0800	验证ListBucket	Custom Policy	Attach Delete Management
ListBucket1	0	2023-01-30 17:25:04 UTC+0800	None	Custom Policy	Attach Delete Management
loaddownobject	0	2020-05-29 14:45:45 UTC+0800	下载	Custom Policy	Attach Delete Management
log	0	2020-05-28 16:42:57 UTC+0800	日志	Custom Policy	Attach Delete Management
□ MFA	1	2020-08-04 17:44:30 UTC+0800	修改MFA	Custom Policy	Attach Delete Management
moveobject	0	2020-05-29 16:31:35 UTC+0800	移动对象	Custom Policy	Attach Delete Management
newfolder	0	2020-05-29 15:36:49 UTC+0800	创建文件本	Custom Policy	Attach Delete Management 🗸



## 7.4.3 View the Policy Basic Information

Enter **IAM** > **Policy Management**, click the corresponding policy name or **Management**, enter the policy details page. On this page, you can view the policy basic information and modify the policy.

The basic information including Policy Name, Policy Type, Creation Time, Last Modified Time and Description.

IAM / Policy Mana	gement / buo	ket-read				
Basic Information	I.					
Policy Name	buck	tet-read 🗇		Policy Type	Custom Policy	
Creation Time	2023	-07-11 16:10:19 UTC+0800		Last Modified Time	2023-07-11 16:10:19 UTC+0800	
Policy Content	Users/Group	s				
Edit Policy						
Service	Effect	Action	Resource		Condition	
Service	Lineer	10001	Resource		constant	
005	Allow	oos:ListBucket more 14 items	•			



## 7.4.4 Attach Policy

#### View attached users/groups •

Enter **Policy** Management, Click the corresponding policy name or Management, enter the policy details page. On this page, click Users/Groups, you can view the users and user groups associated with the current policy, and you can attach and detach the policy for users or user groups.

AM / Policy Management / bucket-read				
Basic Information				
Policy Name bucket-read 🗇		Policy Type	Custom Policy	
Creation Time 2023-07-11 16:10:19 UTC+0800		Last Modified Time	2023-07-11 16:10:19 UTC+0800	
Policy Content Users/Groups				
Attach Policy Detach Policy				
Users/Groups	Туре ~		Operation	
groupte	Group		Detach Policy	

#### Attach Policy

On the Policy Management page, click Attach, and the Attach Users/Groups page will pop up. Select users or user groups that need to be attached. The gray users or user groups in the pop-up box indicates the user or user group that has been attached with the policy.

At	tach l	Users/Groups								$\times$
Cur	rrent Sele	ection	All ~							
Use	rs/Group	05	Search by user/user group nai	a						
The	re are cu	irrently 19 items, 0 has been sel	ected			٦	There are cu	rrently 2 items, 0 has been	selected	
		User/Group Name	Ali ~					User/Group Name	Туре	
		groupte	Group	^				groupte	Group	
		oos-read	Group					group-read	Group	
		test	Group		>					
		test1	Group		<					
		test12345	Group							
		test_wu1	Group							
		testa	Group							
		aaa	User	~						

Cancel



## 7.5 Security Setting

Click **IAM** > **Security Setting**, you can set password policy and login security policy.

M / Security Setting				
Password Policy 🛛 🛱				
<ul> <li>A password policy is a set of rule</li> </ul>	s that define the types of passwords that IAM users can set. The polices will be applied to IAM users to set login passwords.			
Password Settings				
Password Length	10 -128 characters			
Required Elements in Password				
Password Operation				
Password Validity Period	Permanent			
Password Self-management	not allow users to change their own password			
After Password Expires	Restrict user login, and requires administrator to reset password			
Prevent Password Reuse	Disable			
Login Security Policy 🛛 🖄				
<ul> <li>A login security policy is a set of</li> </ul>	login rules that IAM users can set. The rules will be applied to IAM users.			
Loola Constitu Oconstitue				
Peret Lockout Counter after	15 minuter			
Number of failed logins	Simes			
Lockout Duration	15 minutes			
Single Users Simultaneous Login	Enabled			
Session Timeout	30 minutes			

## 7.5.1 Password Policy

## 7.5.1.1 Edit Password Policy

Click Edit Password Policy to reset the password policy.

Password Policy	Password Policy 🛛				
A password policy is a set of rules that	• A password policy is a set of rules that define the types of passwords that IAM users can set. The polices will be applied to IAM users to set login passwords.				
Password Settings					
Password Length	10 8 to 128 characters				
Required Elements in Password	Uppercase Letter Digits Digits Digits Simbols Digits Digit				
Password Operation					
Password Validity Period	0 Days (Maximum value: 1095. A value of 0 means the password never expire)				
Password Self-management	sword Self-management Allow users to change their own password				
After Password Expires Restrict user login and allow users to reset their password 🛞 Restrict user login, and requires administrator to reset password					
Prevent Password Reuse	Remember 0 password(s) (Maximum value 24. A value of 0 means not to prevent password reuse.) Cancel	Save			

Item	Description		
Password Length	Set the password length for the IAM user. The value range is an integer from		
	8 to 128.		
Required Elements in	You can select any one or more of the following:		
Password	<ul> <li>Uppercase Letters: A~Z.</li> </ul>		
	<ul> <li>Lowercase Letters: a~z.</li> </ul>		



	• Digits: 0~9.
	• Symbols: IAM user password must contain at least one of the following
	special characters: !@#\$%^&*()_+-=[]{} '.
	The default rule is that the password must contain lowercase letters and
	numbers.
Password Validity Period	The number of days that an IAM user password is valid. The value is 0 to
	1095, the unit is day. 0 means never expire. The default value is 0.
Password Self-	<ul> <li>Allow users to change their own password.</li> </ul>
management	• If this item is not checked, only the administrator can change the
	password.
After Password Expires	<ul> <li>Restrict user login and allow users to reset their password.</li> </ul>
	• Restrict user login, and requires administrator to reset password.
Prevent Password Reuse	Specify the number of previous passwords that IAM users are prevented from
	reusing. The value is 0 to 24, 0 means that the IAM user can reuse the
	previous passwords. The default value is 0. The previous passwords do not
	contain the currently used password and the current password can not be as
	the new password.
	Prevent passwords are passwords that have been used in history in addition
	to the current password. For example, if the <b>Prevent Password Reuse</b> is
	set to 1, the current password is Password1, the previous password is
	Password0, and the new password that the user wants to set is Password2,
	Password2 cannot be the same as the previous password Password0 and
	the current password Password1.

#### The relationship between After Password Expires and Password Self-management:

Item	Allow users to change their own	Do not allow users to change their
	password	own password
Restrict user login and	At any time, IAM users can change	Only after the password expires, the
allow users to reset their	their passwords by themselves.	IAM user is allowed to change the
password		password once.
Restrict user login, and	At any time, the IAM user cannot	IAM users cannot change their
requires administor to	modify the password through the	passwords by themselves at any time.
reset password	console, but can be modified through	
	the API.	

### 7.5.1.2 Delete Password Policy

Click **Delete Password Policy**, it will be changed to the default password policy, the default password policy is as follows:

- **Password Length**: 8 128 characters.
- **Required Elements in Password**: Lowercase Letters, Digits.
- Password Validity Period: Permanent.



- After Password Expires: Restrict user login and allow users to reset their password.
- **Prevent Password Reuse**: Disable. When the user changes the password, the new password cannot be the same as the current password, because the current password is not a prevent password.

## 7.5.2 Login Security Policy

A login security policy is a set of login rules that IAM users can set. The rules will be applied to IAM users.

## 7.5.2.1 Edit Login Security Policy

Click Edit Login Security Policy to reset the login security policy.

Login Security Policy 🛛				
A login security policy is a set of login rules that IAM use	ers can set. The rule	s will be applied to IAM users.		
Login Security Operation				
Reset Lockout Counter after	15	minutes (Valid values: 15-60 minutes)		
Number of failed logins	5	times (Valid values 5-10 times)		
Lockout Duration	15	minutes (Valid values: 15-60 minutes)		
Single Users Simultaneous Login	Enabled	O Disable		
Session Timeout	30	minutes (Valid values: 10-30 minutes)		
			Cancel	Save

Item	Description
Reset Lockout Counter after	The limited time for the number of failed logins.
	If the IAM user reaches the number of failed logins within the limited login
	limited time, he will be locked for a period of time. After the lockout period
	expires, he can log in again.
	The value is an integer that ranges from 15 to 60, the unit is minutes.
Number of failed logins	The number of consecutive login failures allowed for an IAM user within a
	limited time.
	The value is an integer that ranges from 5 to 10.
Lockout Duration	The time the IAM user was locked out.
	The value is an integer that ranges from 15 to 60, the unit is minutes.
Single Users Simultaneous Login	Whether to allow IAM users to log in at the same time from different
	applications. If the configuration is Disabled, when the IAM user logs in at
	the same time from different applications, the last login will be maintained,
	and the previous login will be forced offline.
Session Timeout	After the IAM user logs in to the console, the session time is saved when
	there is no operation.
	The value is an integer that ranges from 10 to 30, the unit is minutes.



### 7.5.2.2 Delete Login Security Policy

Click **Delete Login Security**, it will be changed to the default login security policy, the default login security policy is as follows:

- **Reset Lockout Counter after**: 15 minutes.
- Number of failed logins: 5.
- Lockout Duration: 15 minutes.
- Single Users Simultaneous Login: Enabled.
- **Reset Lockout Counter after**: 30 minutes.

## 7.6 Security Credential

## 7.6.1 Accesskeys

Click IAM > Security Credential, you can view the user security credential information, including User ID, Creation Time, User Type, and AccessKeys.

**Note**: A user has at most 2 Accesskeys. If all Accesskeys are deleted, the user cannot use the deleted AK/SK to sign.

M / Security Credential					
Account Details User ID User Type	32fefjólyS4gc Root User		Creation Time 2020-03-	16 08:00:00 UTC + 0800	
AccessKeys					
• AccessReyD and SecretAccessRey are the keys for accessing the object storage API. The root user's key has the full authority of the account. For the security of your property and services, it is recommended that you use a sub user. Please keep it property and change the key regularly. When you change the key regularly. When you change the key regularly. When you change the key regularly and change the key regularly. When you change the key regularly. The master key and common key of the old key are retained, and they can be activated, deactivated and viewed. But the conversion between the common key and the master key is no longer possible. After deletion, it cannot be reserved and a new ky connot be created after the number (mit is acceeded. Flease deleties with caution.					
Create AccessKey E	ach user can have up to two access keys (including active or inac	tive)			
AccessKeyID		Creation Time	Last Used Time	Status	Operation
0ad28f4598692586b859	l i i i i i i i i i i i i i i i i i i i	2023-06-16 15:38:16 UTC+0800	None	Active	Make inactive Delete
26e4075aa0f1d6ffbe22 🗇		2023-07-03 18:01:42 UTC+0800	None	Active	Make inactive Delete

#### **AccessKeys Description**

ltem	Description		
AccessKeyID	AccessKey ID. Click the copy button to copy the AccessKey ID.		
SecretAccessKey	Secret AccessKey. Click the view button to view the key value.		
	Note: The AccessKey created before December 15, 2019 has this item.		
Creation Time	Accesskey creation time.		
	None: Indicates that the AccessKey was created before December 15, 2019.		
Last Used Time	The time when the AccessKey was last used.		
Туре	• Master Key		
	• Common Key		
	Note: The AccessKey created before December 15, 2019 has this item.		



Status	AccessKey status:		
	• Active		
	• Inactive		
Operation	You can operate on the AccessKey:		
	• Make inactive		
	<ul> <li>Make active</li> </ul>		
	• Delete		

IAM

## 7.6.2 Password

Only the IAM users who have the permission to change the password can change the password. The password of the root user can be modified on login page.

IAM / Security Credential				
Account Details				
User Name	testa@32fefj64y54gc	Creation Time	2023-07-11 17:05:25 UTC+0800	
User ID	138e8e2771cd4742b803e417b5370367	User ARN	arn:ctyun:iam::32fefj64y54gc:user/testa	
User Type	IAM User			
AccessKeys Passwor	d MFA			
• You need a password to access the management console. The current password has been used for 1 day. We recommend that you change your password regularly.				
Change Password				

## 7.6.3 MFA

MFA authentication is only supported by IAM users, but if MFA authentication is not authorized, the IAM users cannot perform MFA authentication. IAM users with MFA authorization can perform MFA binding on the **Security Credentials** > MFA page.

IAM / Security Credentia	1		
Account Details			
User Name	testa@32fefj64y54gc	Creation Time	2023-07-11 17:05:25 UTC+0800
User ID	138e8e2771cd4742b803e417b5370367	User ARN	arn:ctyun:iam::32fefj64y54gc:user/testa
User Type	IAM User		
AccessKeys Passwo	ord MFA		
<ul> <li>Virtual MFA devices i security element), the system</li> </ul>	is a software app that runs on a phone or other device and emulates a physical stem will also ask you to provide the dynamic security code generated by the vi	device, and is easy to use. After the user enables the virtual MFA function in the ac rtual MFA application (the second Security elements). The combination of multip	count center, when logging in to the cloud platform, in addition to verifying the user name and password (the first le elements can provide higher security protection for the account.
Assign MFA Device			

The MFA binding steps are as follows:

1. Click Assign MFA Device to enter Install Applications.



IAM / Assign MFA Device		
0		
Install Applications	Assign Virtual MFA Device	Completed
Assign Virtual MFA Device		
Please download and install the dynamic password authentication tool on the mobile phone After completion, click Next to enter the assigning page, if it is installed, go directly to the next step		
		Cancel Next

**Note**: You need to install a Time-based One-Time Password (TOTP) authentication tool on the mobile phone.

Assign Virtual MFA Device: Codes can be obtained by scanning acquisition or manual acquisition.
 Note: The entered first group of security codes and second group of security codes must be consecutive.

IAM / Assign MFA Device			
	Ø —	- 2	
	Install Applications	Assign Virtual MFA Device	Completed
Scan Acquisition Ma	nual Acquisition		
Use Authenticator to scan the	following QR code to get a 6-digit verification code		
Please enter the two consecut • The first security code	ive sets of security codes you obtained from the Authenticator app: lease enter verification code		
			Previous Next

3. Completed

**Note**: Please note that if you no longer use virtual MFA and want to uninstall the installed dynamic password tool, please unbind the assigned Virtual MFA device first. If you uninstall the dynamic password tool without unbingding virtual MFA, it may cause the relevant users to be unavailable, please operate with caution!



IAM / Assign MFA Device						
	$\odot$		$\bigcirc$		3	
	Install Applications		Assign Virtual MFA Device		Completed	
Assigned Successfully						
Please note that if you no log with caution!	nger use virtual MFA and want to	uninstall the installed dynamic password tool, please unbind the assi	gned Virtual MFA device first. If you uni	nstall the dynamic password tool without unbindi	ing virtual MFA, it may cause the relevant users to be unavailable, pl	ease operate
You have successfully Assigned	d a Virtual MFA device					
						Cancel

## 7.7 Best Practices

## 7.7.1 Recommendations for Using IAM

#### • Create Individual IAM Users

One account can create multiple IAM users, and you can create individual IAM users for different operators through IAM. According to the functional scope of the operator, the corresponding management authority is granted. At the same time, it is recommended that you also create an IAM user for the root user, and grant the IAM user management permissions. This IAM user can perform daily management work to protect account security.

#### • Separate Console Login Users and Programming Users

It is recommended to separate login users and programming users to better assign permissions:

- > Login users: Users who log in through the console only need to set the console login password.
- > Programming users: Users who access via API only need to create Accesskeys.

#### • Authorize in Groups

When the account has multiple IAM users, the IAM users are classified through user groups, and IAM users with the same permissions are grouped into one group. By authorizing the user group, the IAM users in the group can obtain the permissions that the user group has.

#### • Grant Least Privilege

It is a standard security measure to grant users only permissions required to perform specific tasks. You can achieve this by using IAM's system policy or custom policies. The principle of least privilege helps you establish secure access to your OOS resources.

#### • Set a Strong Password Policy for IAM Users

To ensure that IAM users only use complex passwords and change them periodically, set a password policy to define strong password requirements, such as minimum password length, the elements must



be included in the password, the password is not the same as the prevent password, and the password is forced to change regularly etc.

#### Enable Virtual MFA

Enable Multi-factor authentication (MFA) for IAM users to improve account security and add another layer of security protection in addition to user names and passwords.

#### • Use Policy Restrictions

You can set in the IAM policy that the IAM user can only operate the specified OOS resource under the conditions of a specific time and a specific request IP, but not under other conditions.

#### • The Root Account does not Use the AccessKey

Since the root account has complete control over the resources under its name, in order to avoid the risks caused by the disclosure of the AccessKey, it is not recommended that the root user use the AccessKey.

It is recommended that you also create an IAM user for the root user, and grant the IAM user management permissions. This IAM user can perform daily management work to protect account security.

#### • Enable Cloudtrail Function

Enable Cloudtrail function of OOS to record what operations the user has done in the account and what resources are used. The cloudtrail log records the type of operation, time, source IP of the operation, operator, etc., and can be stored in the OOS bucket for a long time.

Combining IAM with the cloudtrail function, you can perform account management from two levels: control and monitoring.

## 7.7.2 Assigning Permissions to IAM users

A company has multiple staffs who need to access and operate storage resources. Because each staff has different job responsibilities, they need different permissions:

- Separate console login users and programming users.
- Users can be assigned permissions according to different tasks.
- Only the administrator can perform more sensitive daily operations.
- Different managers can view different aspects of confidential data.

Currently the company hopes:

- Supervisor A and Supervisor B have the right to view confidential data.
- Supervisor A can manage and change IAM users under MFA authentication.
- Supervisor B can operate cloudtrail management and view the operation record of the account.
- Staff C and Staff D can view bucket objects.
- Programming users can upload objects to the bucket.

#### Create user groups and attach policies

IAM user group IAM Users		Polciy Description	Access Type		
Confidential Data	Supervisor	А	and	They can view the confidential data in	Console Access



Authority Group	Supervisor B	secretBucket, but they cannot change	
		it.	
IAM Managem	ent Supervisor A	Related management operations for	Console Access
Group		IAM.	
Cloudtrail	Supervisor B	Related management operations for	Console Access
Management		cloudtrail. Have permission to view	
Group		the data in the operation tracking	
		bucket.	
View Obj	ect Staff C and staff D	View object permissions.	Console Access
Group			
Upload Obj	ect Programming users	Upload data to the specified bucket	Programmatic
Group		through the API.	Access

Confidential Data Authority Group policy

```
{
   "Version": "2012-10-17",
   "Statement": [
       {
               "Effect": "Allow",
               "Action": [
                  "oos:ListAllMyBucket"
               ],
               "Resource": "*"
       },
   {
       "Sid": "AllowGroupToSeeBucket",
       "Action": [
           "oos:ListBucket",
           "oos:Get*"
       ],
       "Effect": "Allow",
       "Resource": [
           "arn:ctyun:oos::10rc2arpn6306:secretBucket",
           "arn:ctyun:oos::10rc2arpn6306:secretBucket/*"
       ]
   }
 ]
}
```

IAM Management Group policy

```
{
    "Version": "2012-10-17",
    "Statement": [
```



```
{
    "Sid": "AllowGroupToManageIAM",
    "Effect": "Allow",
    "Action": "iam:*",
    "Resource": "*",
    "Condition": {
        "Bool": {
            "ctyun:MultiFactorAuthPresent": "true"
        }
    }
    }
}
```

Cloudtrail Management Group policy

```
{
   "Version":
                 "2012-10-17",
   "Statement": [
       {
               "Effect": "Allow",
               "Action": [
                   "oos:ListAllMyBucket"
               ],
               "Resource": "*"
       },
       {
       "Sid": "AllowGroupToManageTrail",
       "Effect": "Allow",
       "Action": "cloudtrail:*",
       "Resource": "*"
       },
       {
       "Sid": "AllowGroupToSeeBucket",
       "Effect": "Allow",
       "Action": [
           "oos:GetObject",
           "oos:ListBucket"
           ],
       "Resource": [
           "arn:ctyun:oos::10rc2arpn6306:trailbucket",
           "arn:ctyun:oos::10rc2arpn6306:trailbucket/*"
           ]
       }
   ]
```



#### }

Storage object group policy

```
{
   "Version": "2012-10-17",
   "Statement": [
       {
       "Effect": "Allow",
       "Action": [
            "oos:ListAllMyBucket"
           ],
            "Resource": "*"
       },
       {
       "Sid": "AllowGroupToGetObject",
       "Effect": "Allow",
       "Action": "oos:GetObject",
       "Resource": "arn:ctyun:oos::10rc2arpn6306:appbucket/*"
       }
   ]
}
```

Upload object group policy

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowGroupToPutObject",
            "Effect": "Allow",
            "Action": "oos:PutObject",
            "Resource": "arn:ctyun:oos::10rc2arpn6306:appbucket/*"
        }
    ]
}
```



## 8 Resource Package

You can order OOS resource packs according to your usage requirements. For ordering instructions, please refer to https://www.ctyun.cn/h5/orderconsole/oos/buy.

On the **Resource Package** page, you can view the ordered resource packs, purchase new resource packs, renew existing resource packs, or unsubscribe existing resource packs.

Object-Oriented Storage	Reso	Resource Package							
Statistics Overview 🔻		Purchase Resource Package C							
Buckets		Region	Туре	Specifications	Remaining Amount (?)	Effective Time	Expired Time	Actions	
Cloudtrail •		China Mainland	Standard Storage-Storage Package	2.000GiB	2.000GiB	2023-04-11 17:19:13 UTC+0800	2023-04-13 09:58:32 UTC+0800	Renew Unsubscribe	
Resource Package									total 1 10 ~ < 1 >



# 9 Appendix

## 9.1 Endpoints

The endpoints of Object Storage Network, Object Storage Network 2, and Hongkong node are different.

## 9.1.1 Object Storage Network Endpoint

Different Endpoints are used for OOS API, statistics, operation tracking, and IAM API in the object storage network. The list of object storage network endpoints is as follows:

- OOS API Endpoint: oos-cn.ctyunapi.cn, support HTTP and HTTPS.
- Statistics API Endpoint: oos-cn-mg.ctyunapi.cn, support HTTP and HTTPS.
- CloudTrail API Endpoint: oos-cn-cloudtrail.ctyunapi.cn, support HTTPS.
- IAM API Endpoint: oos-cn-iam.ctyunapi.cn, support HTTPS.

**Note**: For the OOS API in the object storage network, if your data is stored in a certain region, it is recommended that you can directly use the region endpoint. The Endpoint list is as follows (the Endpoint list is only a description of the access information of the region Endpoint, and is not related to the region status):

Region	OOS API Endpoint
ZhengZhou	oos-hazz.ctyunapi.cn
ShenYang	oos-lnsy.ctyunapi.cn
ChengDu	oos-sccd.ctyunapi.cn
WuLuMuQi	oos-xjwlmq.ctyunapi.cn
LanZhou	oos-gslz.ctyunapi.cn
QingDao	oos-sdqd.ctyunapi.cn
GuiYang	oos-gzgy.ctyunapi.cn
WuHan	oos-hbwh.ctyunapi.cn
LaSa	oos-xzls.ctyunapi.cn
WuHu	oos-ahwh.ctyunapi.cn
ShenZhen	oos-gdsz.ctyunapi.cn
SuZhou	oos-jssz.ctyunapi.cn
SH2	oos-sh2.ctyunapi.cn

## 9.1.2 Object Storage Network 2 Endpoint

Different Endpoints are used for OOS API, statistics, operation tracking, and IAM API in the object storage network 2. The list of object storage network 2 endpoints is as follows:

• OOS API Endpoint: oos-cn2.ctyunapi.cn, support HTTP and HTTPS.



- Statistics API Endpoint: oos-cn2-mg.ctyunapi.cn, support HTTPS.
- CloudTrail API Endpoint: oos-cn2-cloudtrail.ctyunapi.cn, support HTTPS.
- IAM API Endpoint: oos-cn2-iam.ctyunapi.cn, support HTTPS.

**Note**: For the OOS API in the object storage network 2, if your data is stored in a certain region, it is recommended that you can directly use the region endpoint. The Endpoint list is as follows (the Endpoint list is only a description of the access information of the region Endpoint, and is not related to the region status):

Region	OOS API Endpoint
NeiMeng1	oos-nm1.ctyunapi.cn
HangZhou1	oos-hz1.ctyunapi.cn

## 9.1.3 Hongkong Endpoint

Hongkong nodes has two modes: highquality network and normal network. The endpoints of the OOS API of highquality network and normal network are different, but their Statistics API, CloudTrail API, IAM API are same.

- Hongkong highquality network OOS API Endpoint: oos-cnhk-hqnet.ctyunapi.cn, support HTTP and HTTPS. Hongkong normal network OOS API Endpoint: oos-cnhk-nqnet.ctyunapi.cn, support HTTP and HTTPS
- Statistics API Endpoint: oos-cnhk-mg.ctyunapi.cn, support HTTP and HTTPS.
- CloudTrail API Endpoint: oos-cnhk-cloudtrail.ctyunapi.cn, support HTTPS.
- IAM API Endpoint: oos-cnhk-iam.ctyunapi.cn, support HTTPS.



## 9.2 Action List and Corresponding API

**Note**: The **Resource** in the following tables shows the resources corresponding to the **Action**, and the effective examples are in parentheses. When the resource is \*, it means that all resources are assigned to the Action in the policy. We suggest that you try not to use \* when allocating resources to avoid allocating too many resources.

Action		Resource	API
Bucket List	ListBucket	Bucket ( <i>bucketname</i> or * )	GET Bucket (List
			Objects), HEAD Bucket
	ListAllMyBucket	All (*)	GET Service
	GetRegions	All (*)	GET Regions
Bucket	ListBucketMultipartUploads	Bucket ( <i>bucketname</i> or * )	List Multipart Uploads
Read	GetBucketAcl	Bucket ( <i>bucketname</i> or * )	GET Bucket acl
	GetBucketLocation	Bucket ( <i>bucketname</i> or * )	GET Bucket location
	GetBucketPolicy	Bucket ( <i>bucketname</i> or * )	GET Bucket policy
	GetLifecycleConfiguration	Bucket ( <i>bucketname</i> or * )	GET Bucket lifecycle
	GetBucketWebsite	Bucket ( <i>bucketname</i> or * )	GET Bucket website
	GetBucketCORS	Bucket ( <i>bucketname</i> or * )	GET Bucket cors
	GetBucketLogging	Bucket ( <i>bucketname</i> or * )	GET Bucket logging
	GetBucketObjectLockConfiguration	Bucket ( <i>bucketname</i> or * )	GET Bucket Object Lock
	GetBucketInventoryConfiguration	Bucket ( <i>bucketname</i> or * )	GET Bucket Inventory
			Configuration, List
			Bucket Inventory
			Configuration
Bucket	PutBucket	Bucket ( <i>bucketname</i> or * )	PUT Bucket
Write	DeleteBucket	Bucket ( <i>bucketname</i> or * )	DELETE Bucket
	DeleteMultipleObjects	Bucket ( <i>bucketname</i> or * )	DELETE Multiple Objects
	PutlifecycleConfiguration	Bucket ( <i>bucketname</i> or * )	PUT Bucket lifecycle,
			DELETE Bucket lifecycle
	PutBucketWebsite	Bucket ( <i>bucketname</i> or * )	PUT Bucket website
	DeleteBucketWebsite	Bucket ( <i>bucketname</i> or * )	DELETE Bucket website
	PutBucketCORS	Bucket ( <i>bucketname</i> or * )	PUT Bucket cors, DELETE
			Bucket cors
	PutBucketLogging	Bucket ( <i>bucketname</i> or * )	PUT Bucket logging
	PutBucketObjectLockConfiguration	Bucket ( <i>bucketname</i> or * )	PUT Bucket Object Lock
	DeleteBucketObjectLockConfiguration	Bucket ( <i>bucketname</i> or * )	DELETE Bucket Object Lock
		Bucket ( <i>bucketname</i> or * )	PUT Bucket Inventory
	PutBucketInventoryConfiguration		Configuration, DELETE
			Bucket Inventory
			Configuration
Bucket	PutBucketPolicy	Bucket ( <i>bucketname</i> or * )	PUT Bucket policy

Table1	OOS action	list and	correst	ondina	API
				· · · · · · · · · · · · · · · · · · ·	



Permissions	DeleteBucketPolicy	Bucket (bucketname or * )	DELETE Bucket policy
Object Read	ListMultipartUploadParts	Object	List Parts
		(bucketname/objectname	
		, <i>bucketname</i> /*, or *)	
	GetObject	Object	GET Object、HEAD Object
		(bucketname/objectname	
		, <i>bucketname</i> /*, or *)	
Object Write	PutObject	Object	PUT Object, PUT Object-
		(bucketname/objectname , bucketname/*, or *)	Copy, POST Object, Initiate
			Mulitipart Upload,Upload
			Part, Compelete Multipart
			Upload,Upload Part -Copy
	DeleteObject	Object	DELETE Object
		(bucketname/objectname	
		, <i>bucketname</i> /*, or *)	
	AbortMultipartUpload	Object	Abort Multipart Upload
		(bucketname/objectname	
		, <i>bucketname</i> /*, or *)	

### Table2 Statistics action list and corresponding API

Action	Resource	API
GetAccountStatistcsSummary	All (*)	GET Capacity, GET DeleteCapacity, GET Traffics,
		GET AvailableBandwidth, GET Requests, GET
		RetarnCode, GET ConcurrentConnection, GET Usage,
		GET AvailBW, GET Bandwidth, Get Connection

#### Table3 Cloudtrail action list and corresponding API

Action		Resource	API
List	DescribeTrails	trail (trail/* or *)	DescribeTrails
	LookupEvents	trail (trail/* or *)	LookupEvents
Read	GetEventSelectors	trail (trail/ <i>trailname</i> , trail/*, or *)	GetEventSelectors
	GetTrailStatus	trail (trail/ <i>trailname</i> , trail/*, or *)	GetTrailStatus
Write	PutEventSelectors	trail (trail/ <i>trailname</i> , trail/*, or *)	PutEventSelectors
	StopLogging	trail (trail/ <i>trailname</i> , trail/*, or *)	StopLogging
	CreateTrail	trail (trail/ <i>trailname</i> , trail/*, or *)	CreateTrail
	UpdateTrail	trail (trail/ <i>trailname</i> , trail/*, or *)	UpdateTrail
	DeleteTrail	trail (trail/ <i>trailname</i> , trail/*, or *)	DeleteTrail
	StartLogging	trail (trail/ <i>trailname</i> , trail/*, or *)	StartLogging



### Table4 IAM action list and corresponding API

Action		Resource	API
List	GetAccountSummary	All (*)	GetAccountSummary
	GetLoginProfile	user (user/ <i>username</i> , user/*, or *)	GetLoginProfile
	ListAccessKeys	user (user/ <i>username</i> , user/*, or *)	ListAccessKeys
	ListUsers	user (user/* or * )	ListUsers
	ListUserTags	user (user/ <i>username</i> , user/*, or *)	ListUserTags
	ListGroups	group (group/* or *)	ListGroups
	ListGroupsForUser	user (user/ <i>username</i> , user/*, or *)	ListGroupsForUser
	ListPolicies	policy (policy/* or *)	ListPolicies
	ListAttachedGroupPolicies	group (group/ <i>groupname</i> , <i>group/*</i> or *)	ListAttachedGroupPolicies
	ListAttachedUserPolicies	user (user/ <i>username</i> , user/*, or *)	ListAttachedUserPolicies
	ListEntitiesForPolicy	policy (policy/ <i>policyname</i> , policy/*, or *)	ListEntitiesForPolicy
	ListMFADevices	user (user/username, user/*, or *)	ListMFADevices
	ListVirtualMFADevices	mfa (mfa/* or *)	ListVirtualMFADevices
Read	GetUser	user (user/ <i>username</i> , user/*, or *)	GetUser
	GetAccessKeyLastUsed	user (user/ <i>username</i> , user/*, or *)	GetAccessKeyLastUsed
	GetGroup	group (group/ <i>groupname</i> , <i>group/</i> * or *)	GetGroup
	GetPolicy	policy (policy/ <i>policyname</i> , policy/*, or *)	GetPolicy
	GetAccountPasswordPolicy	All (*)	GetAccountPasswordPolicy
	GetAccountLoginSecurityPol icy	All (*)	GetAccountLoginSecurityPolic y
Write	CreateAccessKey	user (user/ <i>username</i> , user/*, or *)	CreateAccessKey
	DeleteAccessKey	user (user/ <i>username</i> , user/*, or *)	DeleteAccessKey
	UpdateAccessKey	user (user/ <i>username</i> , user/*, or *)	UpdateAccessKey
	CreateUser	user (user/ <i>username</i> , user/*, or *)	CreateUser
	DeleteUser	user (user/ <i>username</i> , user/*, or *)	DeleteUser
	TagUser	user (user/ <i>username</i> , user/*, or *)	TagUser
	UntagUser	user (user/ <i>username</i> , user/*, or *)	UntagUser
	CreateGroup	group (group/ <i>groupname</i> , <i>group/</i> * or *)	CreateGroup
	DeleteGroup	group (group/ <i>groupname</i> , <i>group/</i> * or *)	DeleteGroup
	AddUserToGroup	group (group/ <i>groupname</i> , <i>group/</i> * or *)	AddUserToGroup
	RemoveUserFromGroup	group (group/ <i>groupname</i> , <i>group/*</i> or *)	RemoveUserFromGroup
	ChangePassword	user (user/username, user/*, or *)	ChangePassword
	UpdateAccountPasswordPolic	All (*)	UpdateAccountPasswordPolicy



Appendix

	у		
	DeleteAccountPasswordPolic	All (*)	DeleteAccountPasswordPolicy
	у		
	UpdateAccountLoginSecurity	All (*)	UpdateAccountLoginSecurityPo
	Policy		licy
	DeleteAccountLoginSecurity	All (*)	DeleteAccountLoginSecurityPo
	Policy		licy
	CreateVirtualMFADevice	mfa (mfa/mfaname, mfa/*, or *)	CreateVirtualMFADevice
	DeactivateMFADevice	user (user/ <i>username</i> , user/*, or *)	DeactivateMFADevice
	DeleteVirtualMFADevice	mfa (mfa/mfaname, mfa/*, or *)	DeleteVirtualMFADevice
	EnableMFADevice	user (user/ <i>username</i> , user/*, or *)	EnableMFADevice
	CreateLoginProfile	user (user/ <i>username</i> , user/*, or *)	CreateLoginProfile
	DeleteLoginProfile	user (user/ <i>username</i> , user/*, or *)	DeleteLoginProfile
	UpdateLoginProfile	user (user/ <i>username</i> , user/*, or *)	UpdateLoginProfile
Policy	CreatePolicy	policy (policy/policyname, policy/*, or	CreatePolicy
		*)	
	DeletePolicy	policy (policy/policyname, policy/*, or	DeletePolicy
		*)	
	AttachUserPolicy	user (user/ <i>username</i> , user/*, or *)	AttachUserPolicy
	DetachUserPolicy	user (user/ <i>username</i> , user/*, or *)	DetachUserPolicy
	AttachGroupPolicy	group (group/groupname, group/* or	AttachGroupPolicy
		*)	
	DetachGroupPolicy	group (group/groupname, group/* or	DetachGroupPolicy
		*)	

## 9.3 Statement

## 9.3.1 Version

The Version of the IAM policy element is used in a policy to define the version of the policy language and is included before the Statement element in all policies.

The current Version of the policy used by OOS IAM is 2012-10-17, compatible with the latest AWS policy Version.

If the Version element is not included in the policy, it is 2012-10-17 by default.

## 9.3.2 Statement

The Statement element is the main element for an IAM policy, and it is required. The Statement element can contain a single JSON statement of a JSON statement block composed of multiple statements. Each individual statement block must be enclosed in braces {}. Each JSON statement block includes the following elements: Sid (optional), Effect (required), Action or NotAction (choose one), Resource or NotResource (choose one), and Condition (optional).



The structure of the Statement is as follows.

"Statement": [ {...}, {...}, {...}, ...]

For example, the following example is an example composed of multiple JSON statement blocks.

```
{
   "Version": "2012-10-17",
   "Statement": [
       {
           "Sid": " AllowGroupToManageTrail",
           "Effect": "Allow",
           "Action": "cloudtrail:*",
           "Resource": "*"
       },
       {
           "Sid": " AllowGroupToSeeBucket",
           "Effect": "Allow",
           "Action": [
               "oos:GetObject",
               "oos:ListBucket"
           1,
           "Resource": [
               "arn:ctyun:oos::10rc2arpn6306:trailbucket",
               "arn:ctyun:oos::10rc2arpn6306:trailbucket/*"
           ]
       }
   ]
}
```

### 9.3.3 Sid

Sid is an optional identifier provided for the policy statement. The user can specify a Sid value for each statement in the statement array, and the Sid value is a sub-ID of the policy file ID. In IAM, the Sid value must be unique in the JSON policy.

## 9.3.4 Effect

The Effect element is a required element that specifies whether the result of the declaration is allow or deny. The valid value of Effect is Allow or Deny. By default, access to resources is denied. To allow access to the resource, the Effect element must be set to Allow.



## 9.3.5 Action

The Action element describes the specified action that will be allowed or denied. Each service has a corresponding task operation, and users can use the corresponding service to perform the described tasks. Services currently available are: oos, cloudtrail, statistics, and iam. See the **Action List** for specific operations included in each service.

The syntax structure of the Action element is: "Action": "Service: *specific operation*". The specific actions can also use wildcards (\*) to indicate certain types of operations.

• Example1: OOS:GetObject.

"Action": "oos:GetObject"

Example2: iam:CreateUser.

"Action": "iam:CreateUser"

• Example3: Use wildcard (\*) which indicates perform all OOS services.

```
"Action": "oos:*"
```

 Example4: Use wildcard (\*) which indicates perform an operation that includes an AccessKey in an IAM service.

"Action": "iam:\*AccessKey\*"

## 9.3.6 NotAction

NotAction is a policy element that explicitly matches everything except the specified action list. Use NotAction to list only those actions that should not match. When using NotAction:

- If the Allow effect is used, all applicable actions or services not listed are allowed.
- If the Deny effect is used, all applicable actions or services not listed are denied. If you want to allow a listed action or service, you must explicitly allow the action or the service.
- Example1: Allow users to perform all other actions of OOS except DeleteBucket.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "NotAction": "oos:DeleteBucket",
        "Resource": "arn:ctyun:oos::10rc2arpn6306:*",
        } ]
```

• Example2: Allow users to perform all actions except IAM service.

{



```
"Version": "2012-10-17",
"Statement": [{
    "Effect": "Allow",
    "NotAction": "iam:*",
    "Resource": "*",
    } ]
```

• Example3: Deny services other than oos, cloudtrail and statistics. However, it does not mean that the actions of the oos, cloudtrail, and statistics services are allowed. If you allow certain actions in oos, cloudtrail, and statistics, you need to write a new policy to explicitly allow them.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Deny",
        "NotAction": [
            "oos:*",
            "cloudtrail:*",
            "statistics:*",
        ],
        "Resource": "*",
    } ]
```

## 9.3.7 Resource

The Resource element specifies the resources for the execution policy, and can specify one or more objects.

The format is as follows :

- "Resource": "arn:ctyun:service::accountid:resource"
- "Resource": "arn:ctyun:service::accountid:resourcetype/resource"

Note:

- service is service name.
- *accounted* is account ID.
- resource is the specified resource. You can use wildcards when specifying resources, where \* represents any combination of characters, ? Represents any single character.
- *resourcetype* is resource type.

**Note**: Add the IAM policy variable "\$ {ctyun: username}" at the last part of the resource to specify the placeholder. When the policy is executed, the IAM policy variable will be replaced with the username of the request itself.



**For example**: Attach a policy with the IAM policy variable to multiple users. When User A initiates a request, *username* will be replaced with A's username. when User B initiates a request, *username* will be replaced with B's username

## 9.3.8 NotResource

The NotResource element is a policy element that explicitly matches every resource except the specified resource list. When using NotResource, only some resources that should not match are listed, instead of including a list of resources that will match. When using NotResource, it should be noted that the resource specified in this element is a restricted resource, that is,

- If Allow is used, all resources not listed, including resources in all other services, will be allowed
- If Deny is used, all resources not listed will be denied.

## 9.3.9 Condition

The Condition element describes the conditions that allow the user to specify the policy to take effect. In Condition element, users can build expression in which users use condition operators to match the conditions in the policy with the requested values.

The Condition element can consist of multiple conditions. Conditions include: condition operators, condition keys, and condition values. A condition key can correspond to multiple condition values. Condition syntax structure is as follows:

```
"Condition": {"Condition Operator A": {"Condition Key A":["Condition Value A1",
"Condition Value A2",...]}, "Condition Operator B": {"Condition Key B":["Condition Value
B1", "Condition Value B2",...] } }
```

**Note**: condition keys are not case sensitive. If the condition value is time, the time to be set is converted to the time in the UTC+0 time zone.

#### Appendix



Condition Blo	ock
	Condition 1: Key1: Value1A OR Value1B OR Value1C AND Key2: Value2A OR Value2B
	Condition 2:
	Key3: Value3A

If there are multiple conditions, the constraints between each condition are as follows:

- If there are multiple conditional operators, and these conditions are evaluated using a logical AND.
- If a condition key corresponds to multiple condition values, use logical OR to evaluate these condition values.
- All condition operators must be met to allow or explicitly deny. If any of the conditions are not met, the result is a rejection.

•• • • • •				
About condition key	vs condition a	operators and	condition values	see the table
/ loour oonanion no	yo, oonanaon (	oporatoro, ana	oonanon valaoo,	

Condition Keys	Condition Operators	Condition Values
ctyun:CurrentTime	• DateEquals: Match the specified date.	The format is yyyy-MM-
	• DateNotEquals: Not equal to the specified	dd'T'HH:mm:ss'Z'. Such as
	date.	2019-12-18T09:00:00Z.
	Date essThan: Before the specified date	DateEquals and
		DateNotEquals are accurate to
	• DateLessInanEquals: Before or equal to	days, others are accurate to
	the specified date.	seconds.
	• DateGreaterThan: Later the specified date.	Note: Convert the time to be set
	• DateGreaterThanEquals: Later or equal to	to the time in UTC+0 time zone.
	the specified date.	
ctyun:Sourcelp	• IpAddress: Match the specified IP address	IPv4: The value is in dotted
	or IP range.	decimal notation.
	<ul> <li>NotTnAddress: Match all IP addresses</li> </ul>	IPv6: The address is a 32-digit
	except the specified IP address or IP range.	
		If an address range is specified,
		a mask is added after the IP
		address, such as


		192.163.1.5/3.
ctyun:userid	• StringEquals: Matches exactly the	The value is a string of 1 to 32
	specified value and is case sensitive.	lowercase letters and numbers.
	<ul> <li>StringNotEquals: Does not match the</li> </ul>	The operators for StringLike
	specified value and is case sensitive.	and StringNotLike can
	<ul> <li>StringEqualsIgnoreCase: Matches exactly</li> </ul>	include wildcard characters.
	the specified value and is not case sensitive.	
	<ul> <li>StringNotEqualsIgnoreCase: Does not</li> </ul>	
	match the specified value and is not case	
	sensitive.	
	• StringLike: Matches exactly the specified	
	value, or is similar to the specified value by	
	padding wildcards, wildcards can be multi-	
	character matching wildcards (*) or single-	
	character matching wildcards (?).	
	• StringNotLike: Does not match the	
	specified value and is case sensitive, or does	
	not match the specified value by padding	
	wildcards.	
ctyun:username	• StringEquals: Matches exactly the	The value is a string of 1 to 64
	specified value and is case sensitive.	insensitive letters, numbers, or
	<ul> <li>StringNotEquals: Does not match the</li> </ul>	special characters. The special
	specified value and is case sensitive.	characters only include
	• StringEqualsIgnoreCase: Matches exactly	comma () period () plus sign
	the specified value and is not case sensitive.	(+), equal sign (=), and at sign
	<ul> <li>StringNotEqualsIgnoreCase: Does not</li> </ul>	(@).
	match the specified value and is not case	Note: The condition operators
	sensitive.	for StringLike and
	• StringLike: Matches exactly the specified	StringNotLike can include
	value, or is similar to the specified value by	wildcard characters.
	padding wildcards, wildcards can be multi-	
	character matching wildcards (*) or single-	
	character matching wildcards (?).	
	• StringNotLike: Does not match the	
	specified value and is case sensitive, or does	
	not match the specified value by padding	
	wildcards.	
ctyun:UserAgent	• StringEquals: Matches exactly the	A string that can contain special
		ah aya ataya



	specified value and is case sensitive.	
	• StringNotEquals: Does not match the	
	specified value and is case sensitive.	
	<ul> <li>StringEqualsIgnoreCase: Matches exactly</li> </ul>	
	the specified value and is not case sensitive.	
	<ul> <li>StringNotEqualsIgnoreCase: Does not</li> </ul>	
	match the specified value and is not case	
	sensitive.	
	• StringLike: Matches exactly the specified	
	value, or is similar to the specified value by	
	padding wildcards, wildcards can be multi-	
	character matching wildcards (*) or single-	
	character matching wildcards (?).	
	<ul> <li>StringNotLike: Does not match the</li> </ul>	
	specified value and is case sensitive, or does	
	not match the specified value by padding	
	wildcards.	
ctyun:Referer	<ul> <li>StringEquals: Matches exactly the</li> </ul>	A string that can contain special
	specified value and is case sensitive.	characters.
	<ul> <li>StringNotEquals: Does not match the</li> </ul>	
	specified value and is case sensitive.	
	<ul> <li>StringEqualsIgnoreCase: Matches exactly</li> </ul>	
	the specified value and is not case sensitive.	
	<ul> <li>StringNotEqualsIgnoreCase: Does not</li> </ul>	
	match the specified value and is not case	
	sensitive.	
	• StringLike: Matches exactly the specified	
	value, or is similar to the specified value by	
	padding wildcards, wildcards can be multi-	
	character matching wildcards (*) or single-	
	character matching wildcards (?).	
	• StringNotLike: Does not match the	
	specified value and is case sensitive, or does	
	not match the specified value by padding	
	wildcards.	
ctyun:SecureTransport	Bool: Boolean match.	● true
		• false
ctyun:MultiFactorAuthP	Bool: Boolean match.	● true
resent	Note: Only IAM service supports this condition	



	operator.	• false		
ctyun:MultiFactorAuthA	• NumericEquals: Match the specified value.	An integer.		
ge	• NumericNotEquals: Negatively match the			
	specified value.			
	• NumericLessThan: Less than the specified			
	value.			
	• NumericLessThanEquals: Less than or			
	equal to the specified value.			
	• NumericGreaterThan: Greater than the			
	specified value.			
	• NumericGreaterThanEquals: Greater than			
	or equal to the specified value.			
	Note: Only IAM service supports this condition			
	operator.			
oos:prefix	• StringEquals: Matches exactly the	The value is a string.		
	specified value and is case sensitive.	Note: The condition key is only		
	• StringNotEquals: Does not match the	of oos: listBucket		
	specified value and is case sensitive.			
	• StringEqualsIgnoreCase: Matches exactly			
	the specified value and is not case sensitive.			
	<ul> <li>StringNotEqualsIgnoreCase: Does not</li> </ul>			
	match the specified value and is not case			
	sensitive.			
	• StringLike: Matches exactly the specified			
	value, or is similar to the specified value by			
	padding wildcards, wildcards can be multi-			
	character matching wildcards (*) or single-			
	character matching wildcards (?).			
	• StringNotLike: Does not match the			
	specified value and is case sensitive, or does			
	not match the specified value by padding			
	wildcards, wildcards can be multi-character			
	matching wildcards (*) or single-character			
	matching wildcards (?).			
oos:x-amz-acl	• StringEquals: Matches exactly the	The value is a string.		
	specified value and is case sensitive.	The value:		
	• StringNotEquals: Does not match the	• private: only the owner		
	specified value and is case sensitive.	• nublic-read: all can		
	• StringEqualsIgnoreCase: Matches exactly			



	the specified value and is not case sensitive.	read the bucket.
•	StringNotEqualsIgnoreCase: Does not	• public-read-write: all
•	StringNotEqualsIgnoreCase: Does not match the specified value and is not case sensitive. StringLike: Matches exactly the specified value, or is similar to the specified value by padding wildcards, wildcards can be multi- character matching wildcards (*) or single- character matching wildcards (?). StringNotLike: Does not match the specified value and is case sensitive, or does not match the specified value by padding wildcards, wildcards can be multi-character matching wildcards (*) or single-character	<ul> <li>public-read-write: all can operate the bucket, including read and write operations.</li> <li>Note: When create a bucket, you can use this condition key to control the type of bucket ACL. The condition key is only valid for the operation authority of oos:PutBucket.</li> </ul>
	matching wildcards (?).	

**Note**: Add the "\$ {ctyun: username}" to specify the placeholder in the Condition element. When the policy is executed, the IAM policy variable will be replaced with the username of the request itself.

**For example**: Attach a policy containing policy variables to multiple users. When user **A** initiates a request, the condition key oos:prefix will be judged based on user A's username. When user **B** initiates a request, the condition key oos:prefix will be judged based on user B's username.

```
{
   "Version": "2012-10-17",
   "Statement": [
    {
        "Action": ["oos:ListBucket"],
        "Effect": "Allow",
        "Resource": ["arn:ctyun:oos::123456789012:mybucket"],
        "Condition": {"StringLike": {"oos:prefix": ["${ctyun:username}/*"]}}
    }
]
```

## • ...IfExists Condition Operators

IfExists: If keywords exist in the request, the keywords are processed according to the conditions described in the policy. If the keyword does not exist, the condition element will evaluate to true. Currently, Only Bool and numeric operators support the IfExists condition operator. The expression: Operator IfExists, such as BoolIfExists, NumericEqualsIfExists. About the use of ...IfExists, see **Example1** and **Example2**.

## Example1



• Deny console requests that do not use MFA authentication, do not deny the console requests that use MFA authentication, and API requests that use keys. However, if the console requests that use MFA authentication, and API requests are allowed, you need to write explicit allow statements.

```
"Effect" : "Deny",
"Condition" : { "Bool" : { "ctyun:MultiFactorAuthPresent" : false } }
```

 Deny console requests that do not use MFA authentication and API requests that use keys, do not deny the console requests that use MFA authentication. However, if the console requests that use MFA authentication are allowed, you need to write explicit allow statements.

```
"Effect" : "Deny",
"Condition" : { "BoolIfExists" : { "ctyun:MultiFactorAuthPresent" : false } }
```

## Example2

Allows requests using MFA authentication within 1800 seconds and API requests using keys.

```
"Effect" : "Allow",
"Condition" : { " NumericLessThanEqualsIfExists" : { "ctyun:MultiFactorAuthAge " :
1800 } }
```

 Allows requests using MFA authentication within 1800 seconds, but requests using MFA authentication greater than 1800 seconds and not using MFA authentication (including API requests) are not allowed.

```
"Effect" : "Allow",
"Condition" : { " NumericLessThanEquals" : { "ctyun:MultiFactorAuthAge " : 1800 } }
```

## 9.3.10 IAM Policy Variables

When writing an IAM policy, if you cannot determine the exact value in the Resource, NotResource, or Condition element, you can use the IAM policy variable as a placeholder. Currently only the variable "\$ {ctyun: username}" is supported. When the policy is executed, the IAM policy variable will be replaced with the username of the request itself.

**Example 1**: Attach a policy with the IAM policy variable to multiple users. When User A initiates a request, *username* will be replaced with A's username. When User B initiates a request, *username* will be replaced with B's username.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
               "oos:GetObject",
               "oos:PutObject"
        ],
```



}

```
"Effect": "Allow",
    "Resource": ["arn:ctyun:oos::123456789012:mybucket/${ctyun:username}/*"]
}
```

**Example 2**: Attach a policy containing policy variables to multiple users. When user **A** initiates a request, the condition key oos:prefix will be judged based on user A's username. When user **B** initiates a request, the condition key oos:prefix will be judged based on user B's username.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": ["oos:ListBucket"],
            "Effect": "Allow",
            "Resource": ["arn:ctyun:oos::123456789012:mybucket"],
            "Condition": {"StringLike": {"oos:prefix": ["${ctyun:username}/*"]}}
     }
    ]
}
```