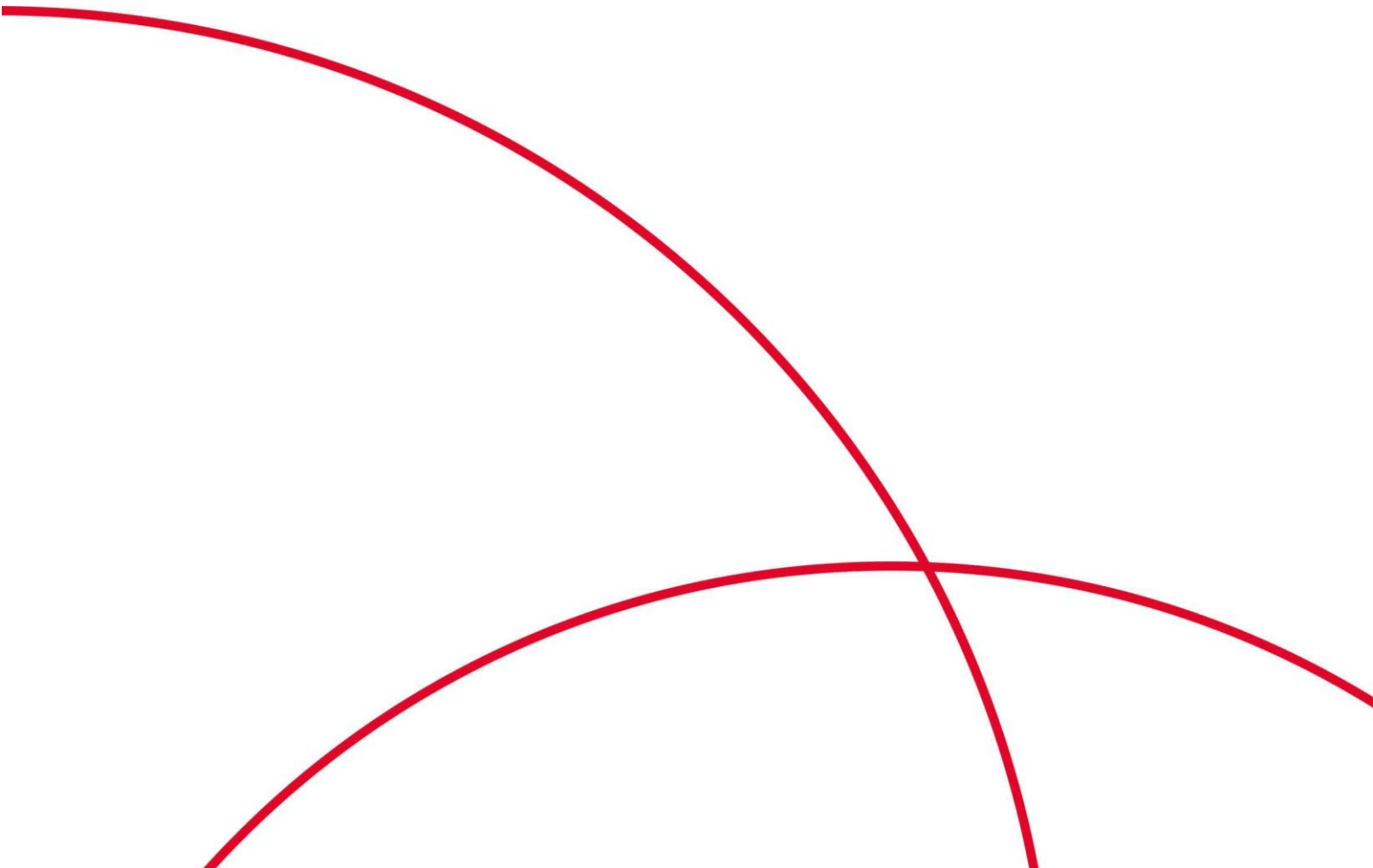
China Telecom Cloud

Object-Oriented Storage User Manual

V6

China Telecom Cloud Technology Co.,Ltd



China Telecom Cloud

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 28
5.1.8 Logging 31

5.1.9 Lifecycle 32
5.1.10 Cross-Origin Resource Sharing (CORS) 35
5.1.11 Compliance Retention (Object Lock Function) 36
5.1.12 Inventory Configuration 40
5.2 Object Management 47
5.2.1 Viewing Object Details 48
5.2.2 Uploading Objects 49
5.2.3 Downloading Objects 53
5.2.4 Managing Object Metadata 54
5.2.5 Previewing an Object 58
5.2.6 Sharing Objects 59
5.2.7 Creating a Folder 62
5.2.8 Deleting Objects or Folders 63
5.2.9 Copying Objects 64
5.2.10 Moving Objects 65
5.2.11 Modifying Storage Classes 66
5.2.12 Searching for a File or Folder 67
5.2.13 Copy the Object Name 68
6 Cloudtrail 69
6.1 Management Events Record 69
6.1.1 View Event Details 70
6.1.2 Event List 72
6.2 Trails List 75
6.2.1 Create Trail 75
6.2.2 Modify the Trail 77
7 IAM 78
7.1 Getting Started 79
7.2 IAM Users 82
7.2.1 Create an IAM User 83
7.2.2 View and Modify the IAM User 87
7.2.3 Delete the IAM User 94
7.2.4 IAM User Login 94
7.3 IAM User Groups 94
7.3.1 Create an IAM User Group 94
7.3.2 View and Modify the IAM User Group 96
7.3.3 Delete the User Group 99
7.4 Policy Management 99
7.4.1 System Policy 99
7.4.2 Custom Policy 100
7.4.3 View the Policy Basic Informaion 112
7.4.4 Attach Policy 113
7.5 Security Setting 114
7.5.1 Password Policy 114
7.5.2 Login Security Policy 116

7.6 Security Credential 117
7.6.1 Accesskeys 117
7.6.2 Password 118
7.6.3 MFA 119
7.7 Best Practices 121
7.7.1 Recommendations for Using IAM 121
7.7.2 Assigning Permissions to IAM users 122
8 Resource Package 125
9 Appendix 126
9.1 Endpoints 126
9.1.1 Object Storage Network Endpoint 126
9.1.2 Hongkong Endpoint 126
9.2 Action List and Corresponding API 127
9.3 Statement 130
9.3.1 Version 130
9.3.2 Statement 131
9.3.3 Sid 131
9.3.4 Effect 132
9.3.5 Action 132
9.3.6 NotAction 132
9.3.7 Resource 133
9.3.8 NotResource 134
9.3.9 Condition 134
9.3.10 IAM Policy Variables 140

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.

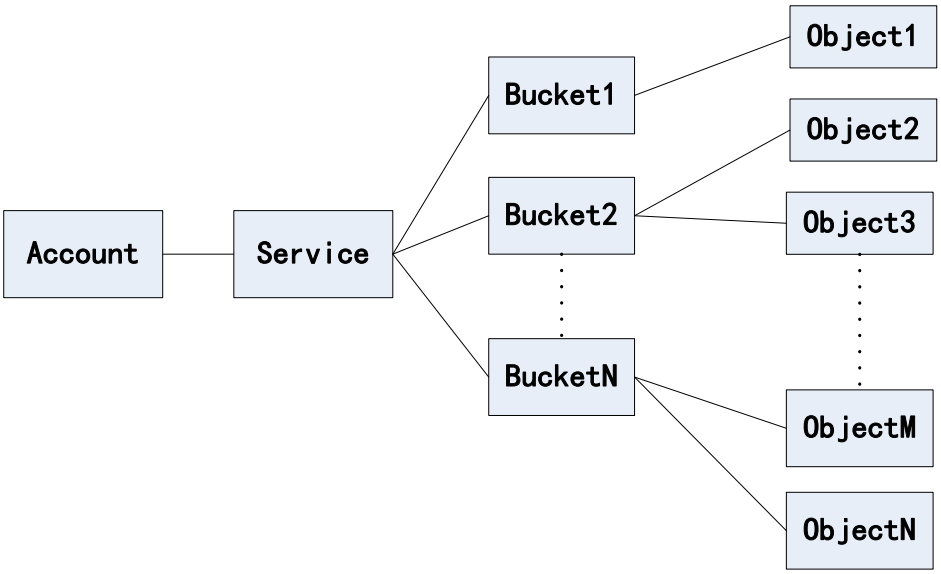
2 Basic Concept

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	99.99999999999%	99.99999999999%
Service Availability	99.99%	99.9%
Minimum chargeable size of the object	Calculated according to the actual size of the object	64KiB
Minimum storage time	No minimum storage time requirement	30 days
Data restoration	No data restoration fee	Charged according to the actual amount of data restoration, in GiB
Data access	Real-time access	Real-time access
Image processing	Supported	Supported
HTTPS encrypted transmission	Supported	Supported
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 ompliance 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 OOS Document on China Telecom Cloud website, click on **管理控制台** to enter **Object-Oriented Storage** console.

3.3 Retrieve Password

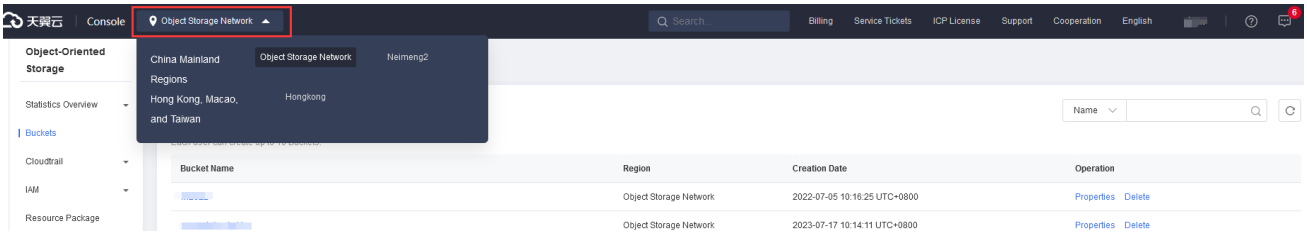
When a registered user forgets the password, he can click **忘记密码** on the login web to retrieve the password. When retrieving the password, the user needs to follow the prompts and enter the relevant information step by step to retrieve the password.

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.



You can select the **Object Storage Network**, **Other Regions**, **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.
- **Other Regions**: Bucket, Object, and AccessKeyId/SecretAccessKey information are not interoperable.
- **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.

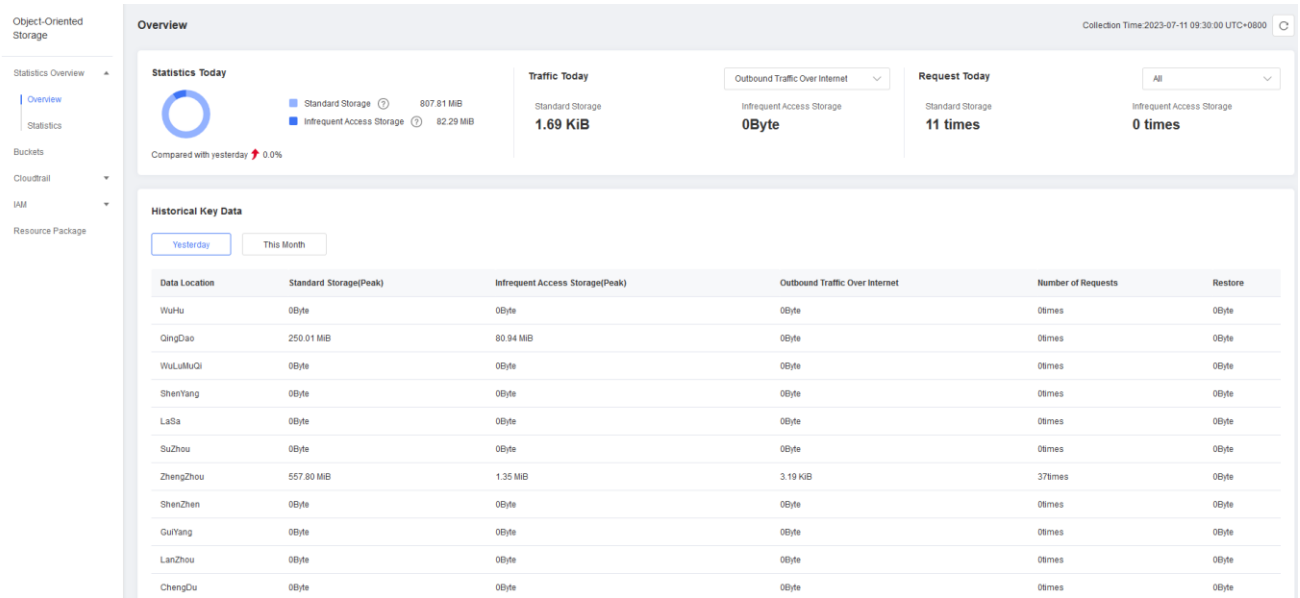
Note: For IAM users, they can view statistics-related information only if they have the corresponding permissions. The permission required is as follows.

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 I**nbound 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**.



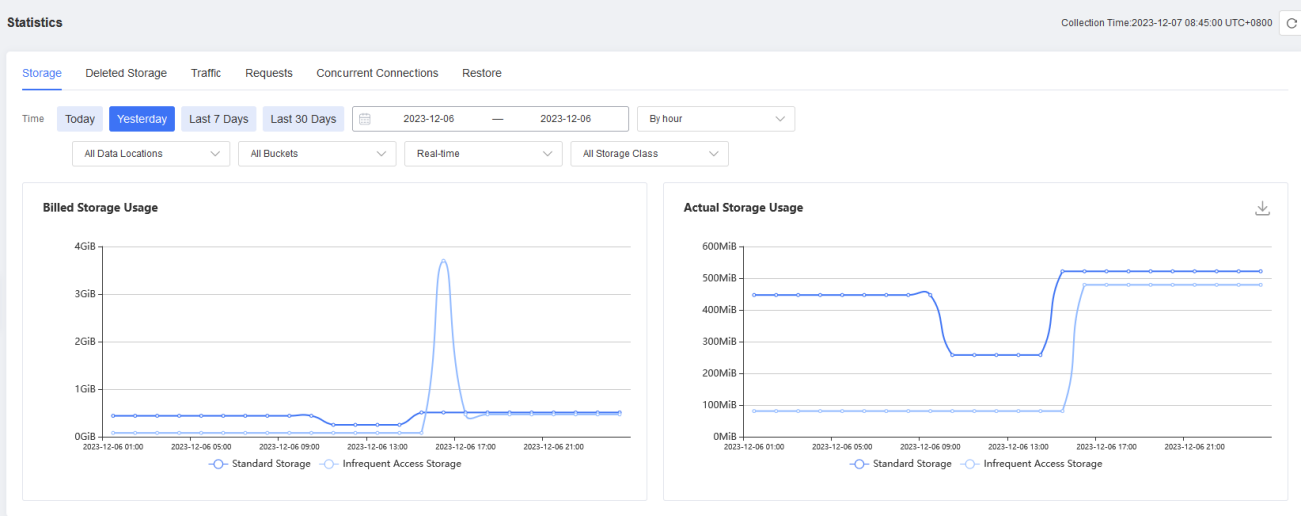
Click **Yesterday** or **This month**, you can view yesterday's statistics or this month's statistics. For yesterday, the statistical time range is the data from 00:00-24:00 the day before the current time in Beijing time. For this month, the statistical time range is from 00:00 on the 1st of the current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

Item	Description
Time	The 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: ● **By 5 minutes**: 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 30 Days** or select any 90 days of data according to the calendar.
Data Location	Data location:

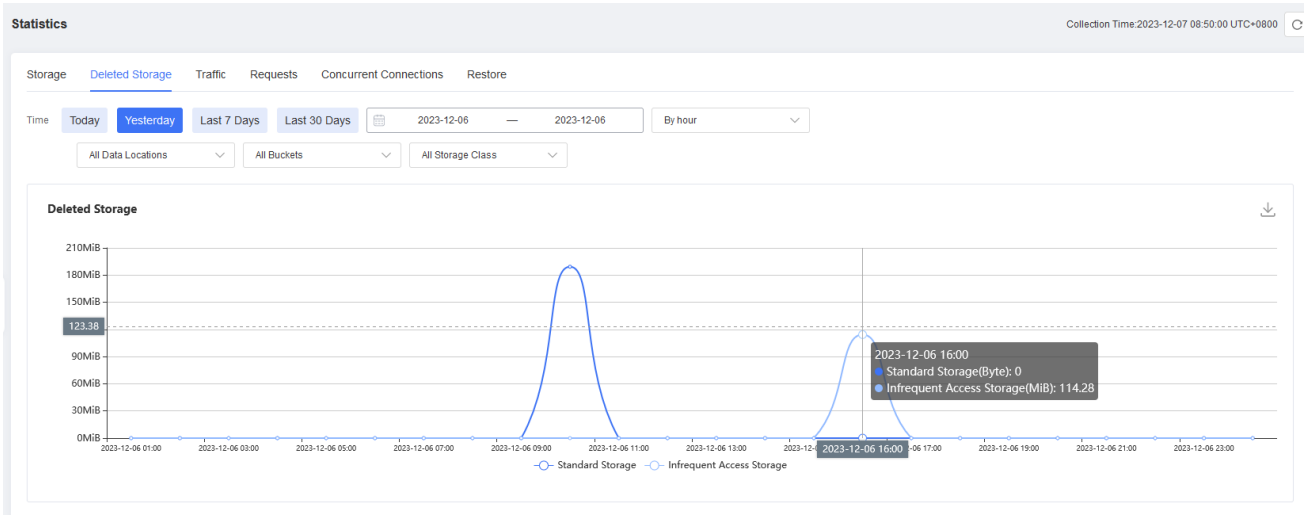
	● **All Data Locations**: Show the sum of the storage capacity for all data locations. ● Specific data location: Choose according to the displayed data location and view the storage for the selected data location.
Bucket	Bucket for storage capacity query: ● **All Buckets**: Show the total storage for 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. ● **Real-time**: 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. ● **Peak**: 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. ● STANDARD_IA: Infrequent Access Storage.
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.



Statistics description of deleted storage

Item	Description
Time	The time period for deleted storage capacity query: ● **Today** ● **Yesterday** ● **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: ● **By 5 minutes**: 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 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.

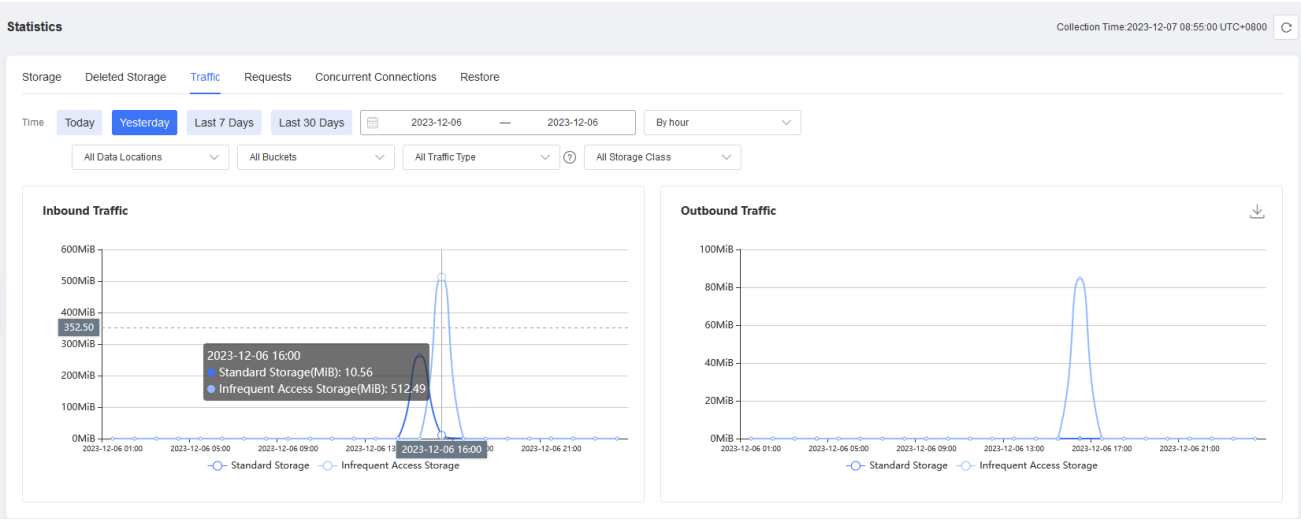
	● Specific data location: Choose according to the displayed data location and view the deleted storage for the selected data location.
Bucket	Bucket for deleted storage capacity query: ● **All Buckets**: Show the total storage for all buckets. ● Specific bucket: Choose according to the displayed bucket 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. ● STANDARD_IA: Infrequent Access storage.
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 description of traffic

Item	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: ● **By 5 minutes**: 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 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 internal scheduling of OOS.
Network Type	Network type for traffic (only supported byHongkong node):

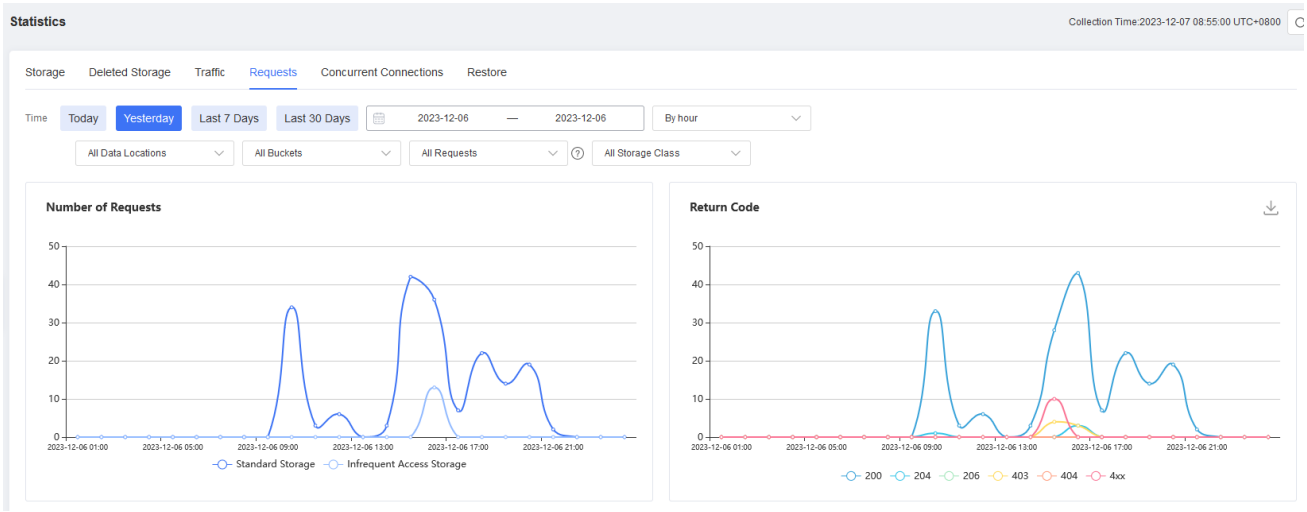
	• **All Network Quality Type**: The sum of the traffic of the High Quality network and the normal network. • **High Quality**: The traffic of the High Qualit network. • **Normal**: The traffic of the normal network.

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. • STANDARD_IA: Infrequent Access storage.
NetType	Network type for traffic (only supported byHongkong node): • highqualitynet：The traffic of the High Qualit network.； • normalqualitynet：The traffic of the normal network。
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: ● **By 5 minutes**: 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**.

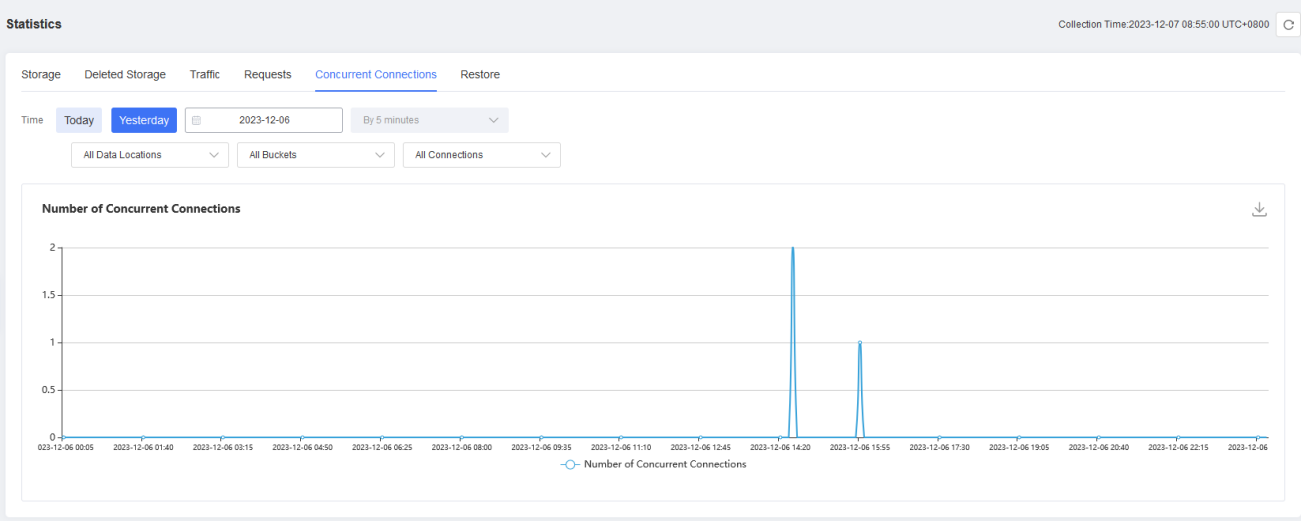
Storage Class	Storage class: ● **All Storage Class**: Show the number of requests and the number of return codes for **Standard Storage** and **Infrequent Access Storage** respectively. ● **Standard Storage**. ● **Infrequent Access Storage**.

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

Item	Description
Date	Time of statistics
StorageClass	Storage class: ● STANDARD: Standard storage. ● STANDARD_IA: Infrequent Access storage.
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 description of concurrent connections

Item	Description

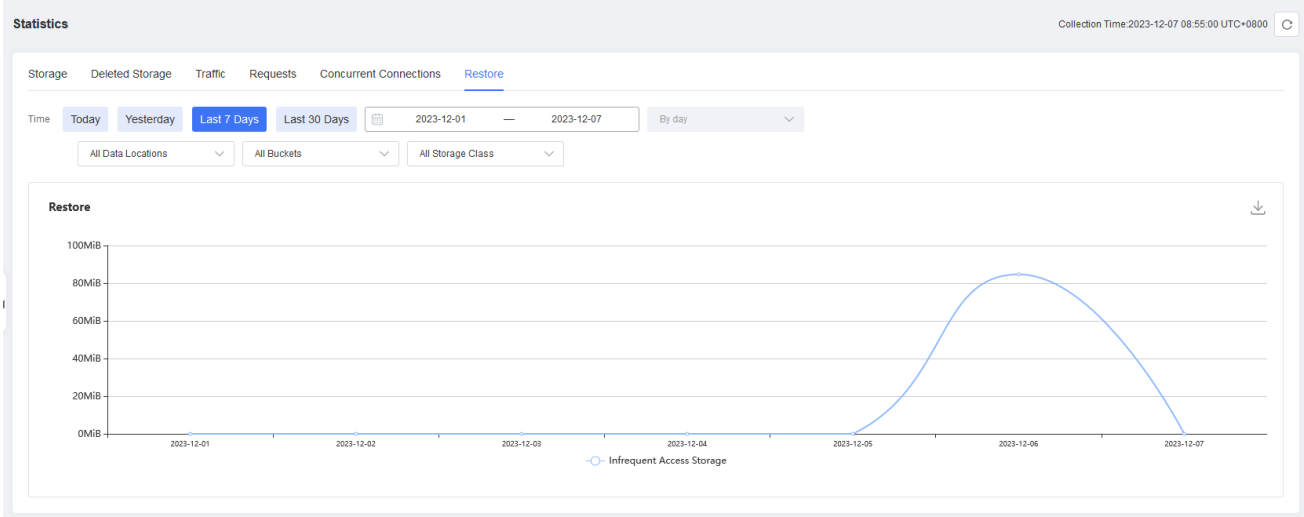
Time	The time period for concurrent connections query: ● **Today** ● **Yesterday** ● According to the calendar button, select and query the concurrent connections in any day
Data Location	Data location: ● **All Data Locations**: Show the total number of concurrent connections for all data locations. ● 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**. ● **Non-Internet Connections**.

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 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

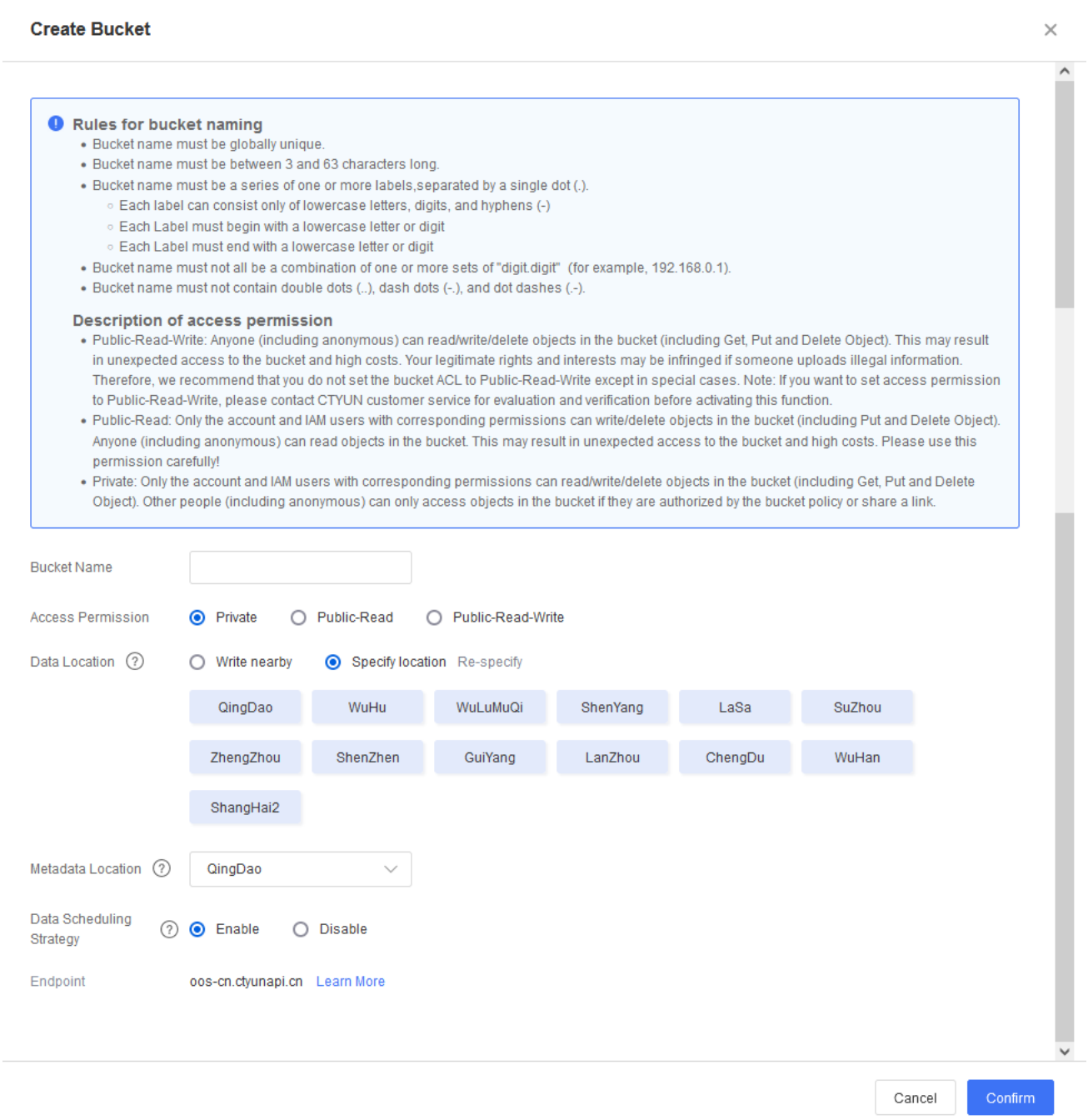
For IAM users, they can operate buckets only if they have the corresponding permissions. The permissions required are as follows.

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 Sharing (CORS)	oos:ListAllMyBucket, oos:GetBucketCORS, oos:PutBucketCORS
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.



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

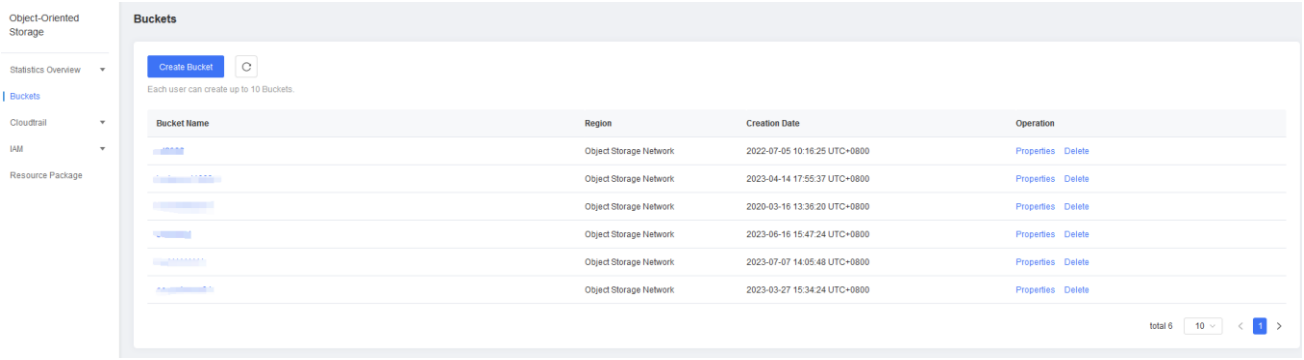
You can also set OOS data scheduling strategy to allow OOS to flexibly handle data location storage:

- 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.

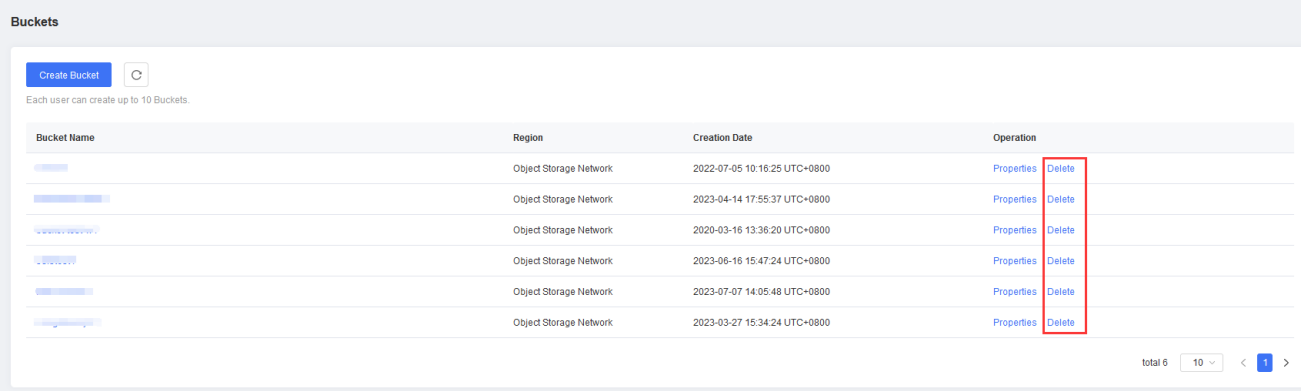
You can enter the name of the Bucket to be queried in the search box in the upper right corner, supporting fuzzy matching queries.



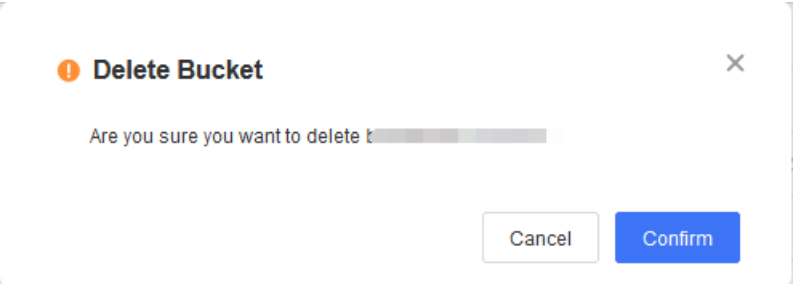
Item	Description
Bucket Name	Bucket name.
Region	The bucket region, including Object Storage Network, Other Regions, Hongkong. Please refer to **Region Switch** for details.
Creation Date	The time when the bucket was created.
Operation	You can view and modify the properties of the bucket and delete it. 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.

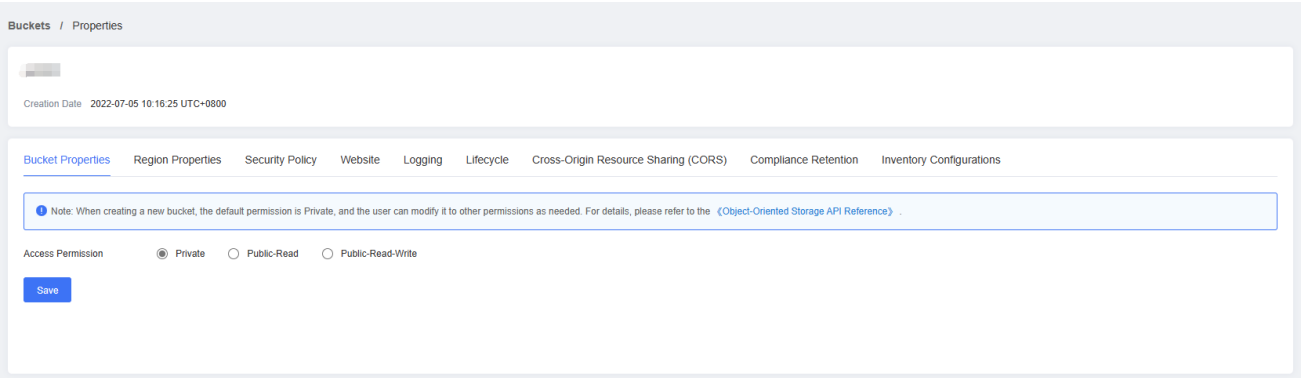


When the user clicks **`Delete`**, the deletion can be performed after a second confirmation in the pop-up window.



5.1.4 Bucket Properties

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



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

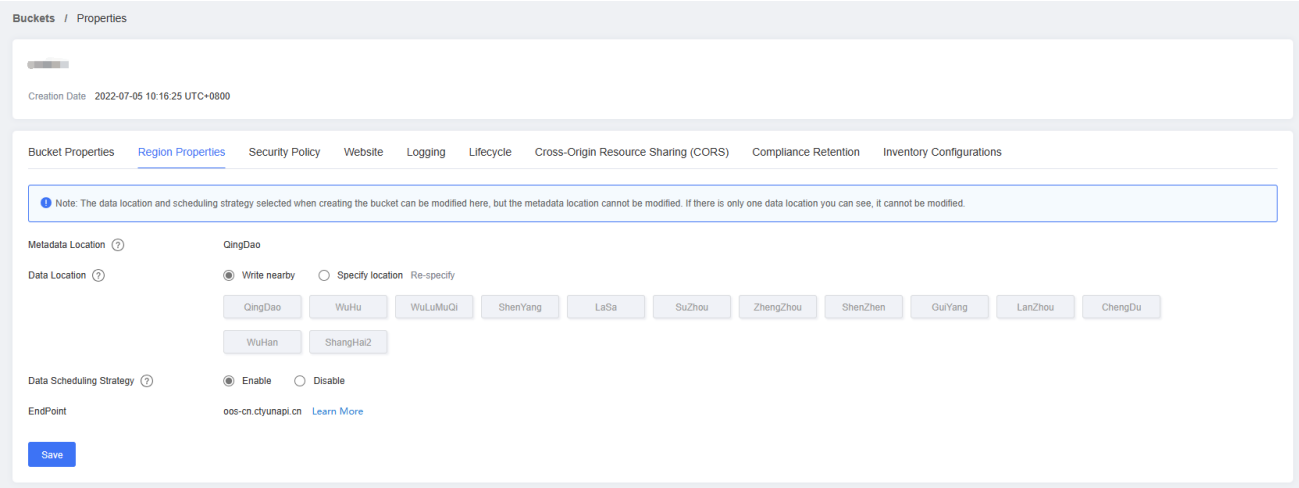
- **Private**: Only the account and IAM users with corresponding permissions can read/write/delete objects in the bucket (including Get, Put and Delete Object). Other people (including anonymous) can only access objects in the bucket if they are authorized by the bucket policy or share a link.
- **Public-Read**: 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

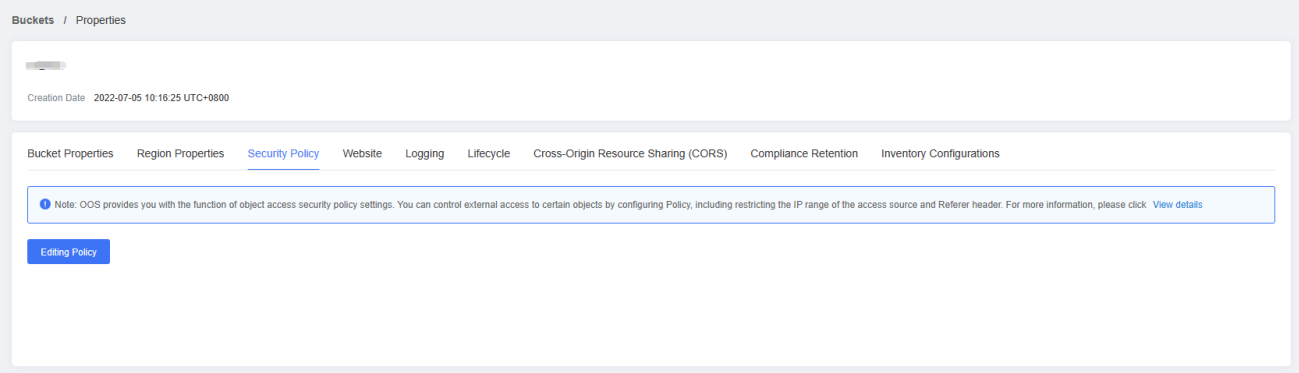
Click **Bucket** > **Properties** > **Region Properties**, enter **Region Properties** page. You can modify the data location and data scheduling strategy, but you can not modify the metadata location.
Note: The Hongkong node only displays **EndPoint**.



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.



Examples of Bucket Policy are as follows:

1) Referer setting

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

As shown above, for example, configure the bucket policy of the bucket named `example-bucket`, and only allow the Referer header to start with `http://www.mysite.com/` or `http://mysite.com/`. If http requests to access this Bucket, then the above configuration method can be used. If requests with an empty Referer header are also allowed to access the Bucket, then an empty string can be added to `ctyun:Referer`.

2) IP Setting

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

```
          "Id": "PolicyId1",
          "Statement": [
            {
                "Sid": "IPAllow",
                "Effect": "Allow",
                "Principal": {
                "CTYUN": "*"
             },

             "Action": "oos:*",
             "Resource": "arn:ctyun:oos::: example-bucket/*",
             "Condition" : {
                 "IpAddress" : {
                     "ctyun:SourceIp": "192.168.143.0/24"
                 },
                 "NotIpAddress" : {
                     "ctyun:SourceIp": "192.168.143.188/32"
                 }
             }
          }
      ]
  }
```

As shown above, if you want to only allow IP addresses within the range of `192.168.143.0/24` to access this bucket, and not allow IP addresses within the range of `192.168.143.188/32` to access this bucket, then the above configuration method can be used.

5.1.7 Website

Click **`Bucket`** > **`Properties`** > **`Website`**, enter **`Website`** page, you can configure website hosting function for bucket and access the static website through the bucket website URL.

Note:

- The hosted domain name of the OOS website does not support HTTPS access, and the user-defined domain name supports HTTPS access.
- If you configure website hosting function, when anonymous users directly access the URL of the bucket, the static website files will be downloaded as an attachment. If you need to preview website content instead of downloading static website files when accessing a static website, you need to bind a custom URL that has passed the record for the bucket. Please contact our staff to apply for binding a custom URL. When applying to bind a custom URL, it is necessary to attach the website certificate together. The certificate supports formats such as crt+key or PEM. Please ensure that the provided certificate is within its validity period.

- Avoid using periods (.). in the target bucket name. Otherwise, failures in client authentication certificate may occur when users use HTTPS for access.

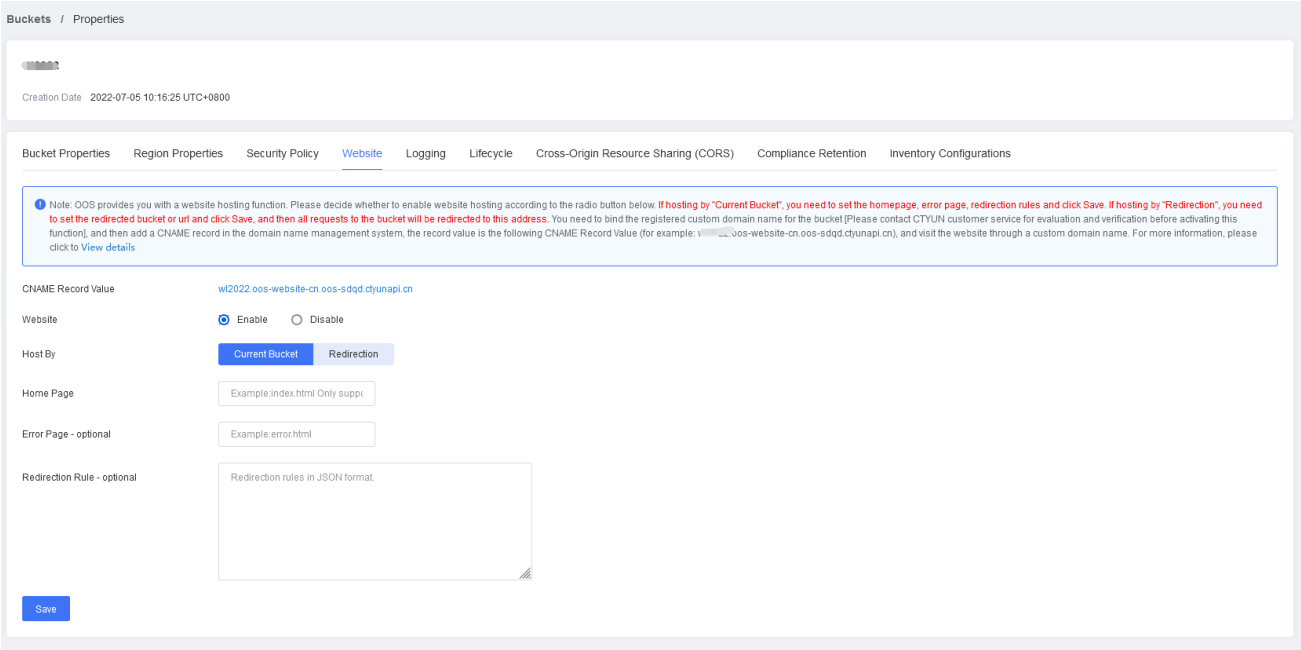
Website hosting configuration steps:

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*.oos-website-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 back-to-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-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-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`**.



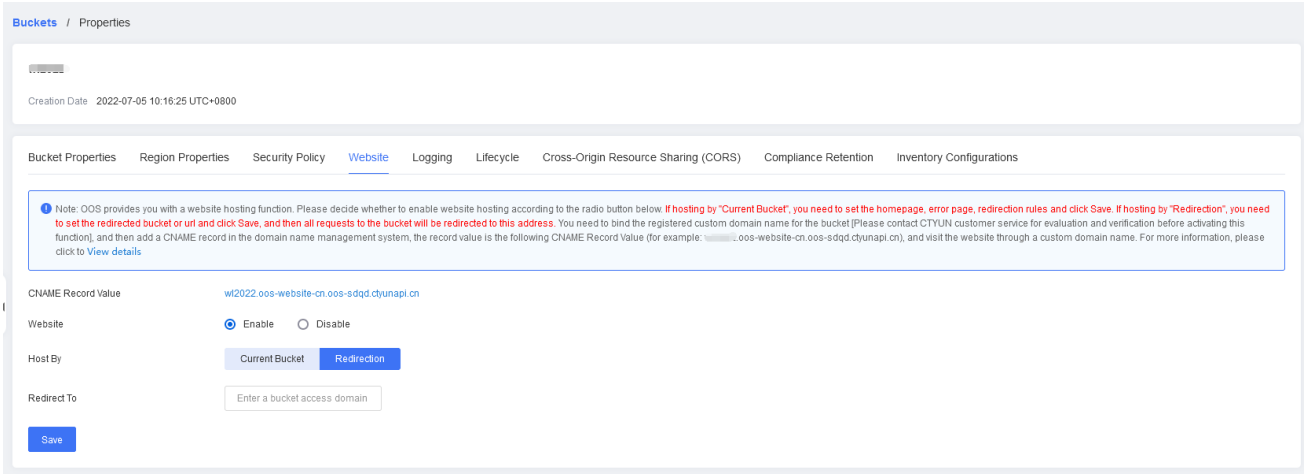
- **Host By Current Bucket**
  - **Home Page**: The home page is the page you jump to when you visit the website. For example, if the **Home Page** is set to `index.html`, when the website is accessed, the `http://yourdomain.com/index.html` page will be opened by default.
  - **Error Page** (optional): 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:

```
[
   {
     "Condition": {
          "HttpErrorCodeReturnedEquals": "string",
          "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 object name to use when redirecting 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. ● If Condition is not configured, it is equivalent to match all rules.
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.

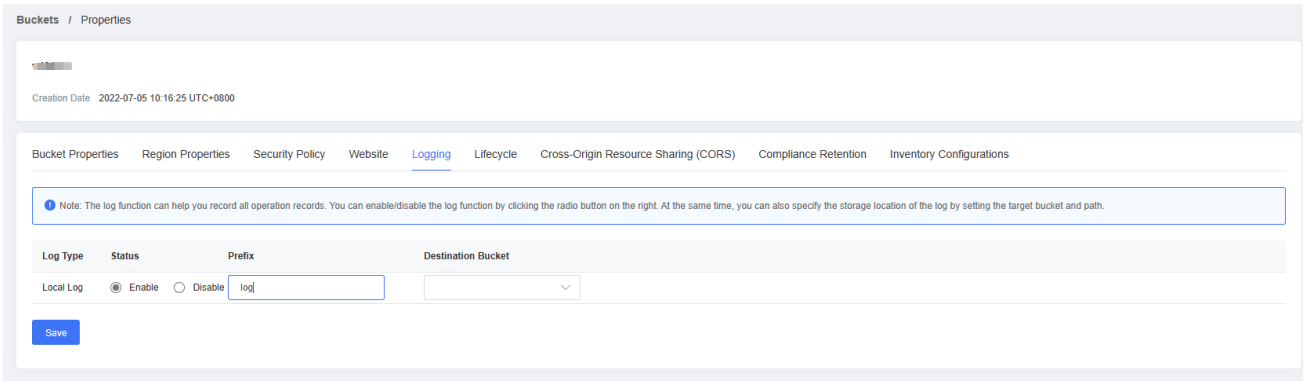
- **Host By Redirection:** You need to set the redirected Bucket access domain name or URL, and all requests to the Bucket will be redirected to this address. For example, if you configure the redirect page to www.example.com, all requests to your domain name (eg http://*yourdomain*.com) will be redirected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



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

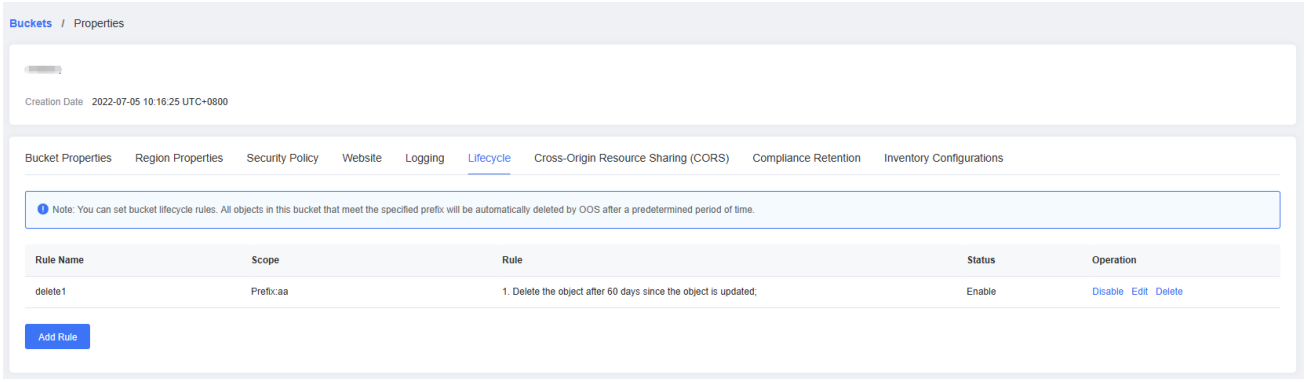
by setting the target bucket and path.



5.1.9 Lifecycle

You can set bucket life cycle rules on this page.

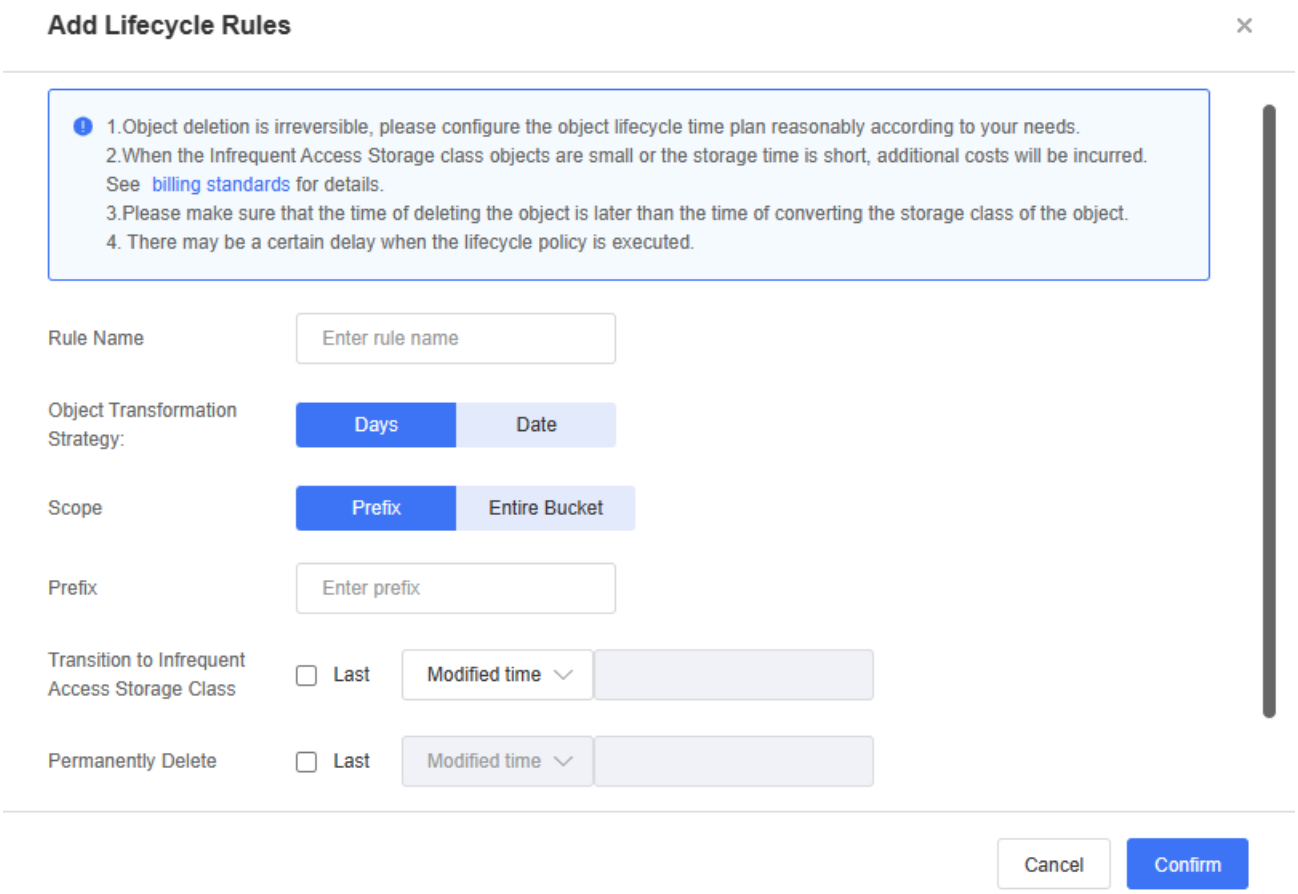
- By setting the bucket lifecycle rules, you can delete objects in the bucket that match the lifecycle rules. When the lifecycle of objects expires, OOS deletes them asynchronously. There may be a delay between the expiration time configured in the lifecycle rule and the actual deletion time. But after 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**.



Name	Description
Rule Name	Lifecycle name.
Scope	The scope of application of the lifecycle rule.
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.



Lifecycle Rules Description

Item	Description
`Rule Name`	Lifecycle rule name.
`Object Transformation Strategy`	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:

	● **Prefix**: 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 Access Storage Class	Objects that match the lifecycle rule are converted into Infrequent Access storage objects after expiration. ● If **Object Transformation Strategy** is **Days**, 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 accessed, according to lifecycle rule, the object is converted to infrequent access storage class. ● If **Object Transformation Strategy** is **Date**, according 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 **Object Transformation Strategy** is **Days**, 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 lifecycle rule, the object modified before this date will be deleted.

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.

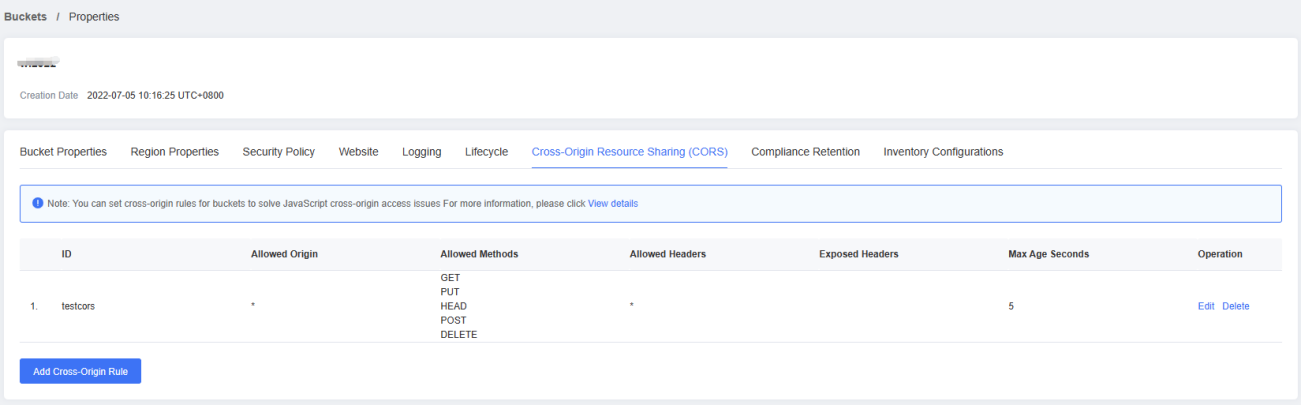
OOS calculates the expiration time by adding the last modified time or last access time of the object to the lifecycle time, and approximates the time to zero GMT on the next day. For example, if an object is created at 10:30 on January 15, 2016 GMT, with a lifecycle of 3 days, then the expiration time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

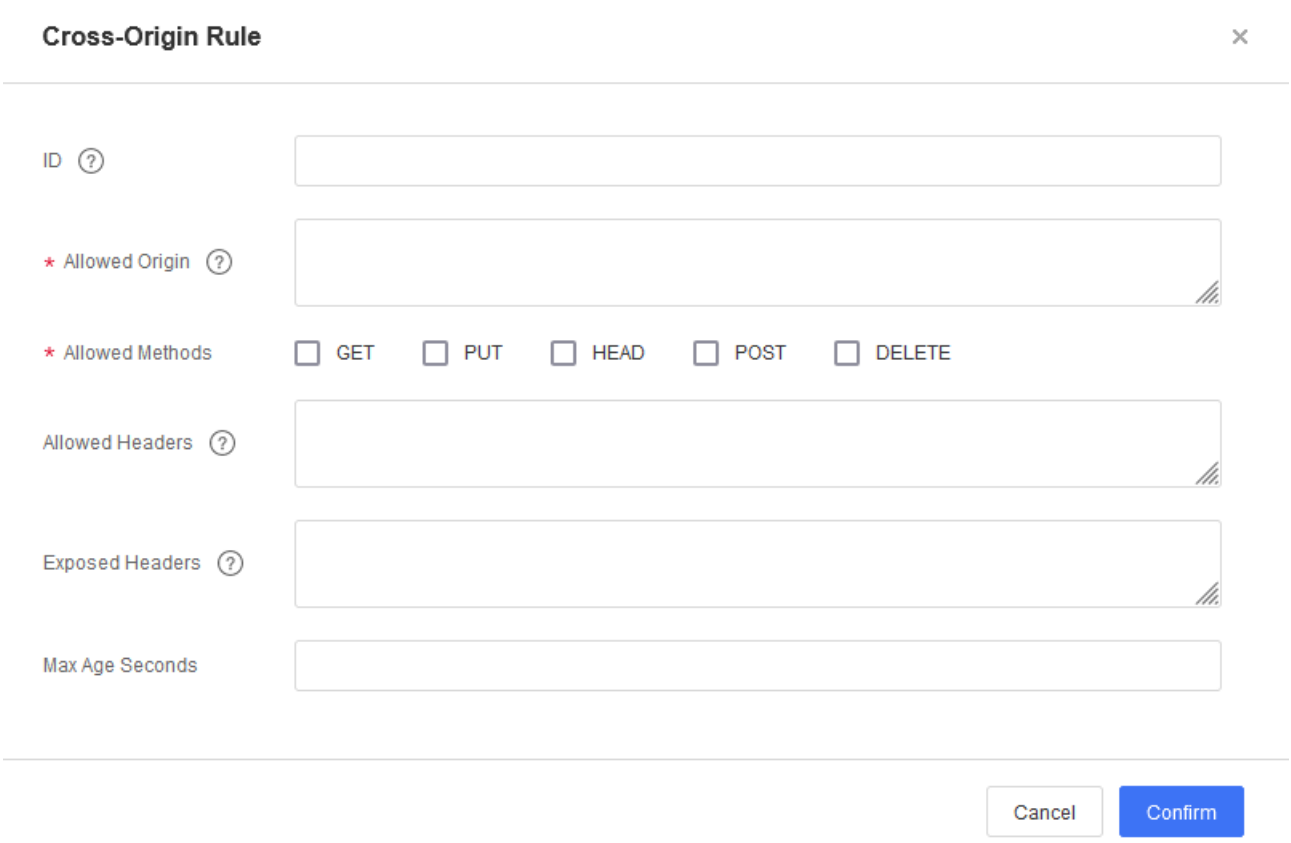
5.1.10 Cross-Origin Resource Sharing (CORS)

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`.



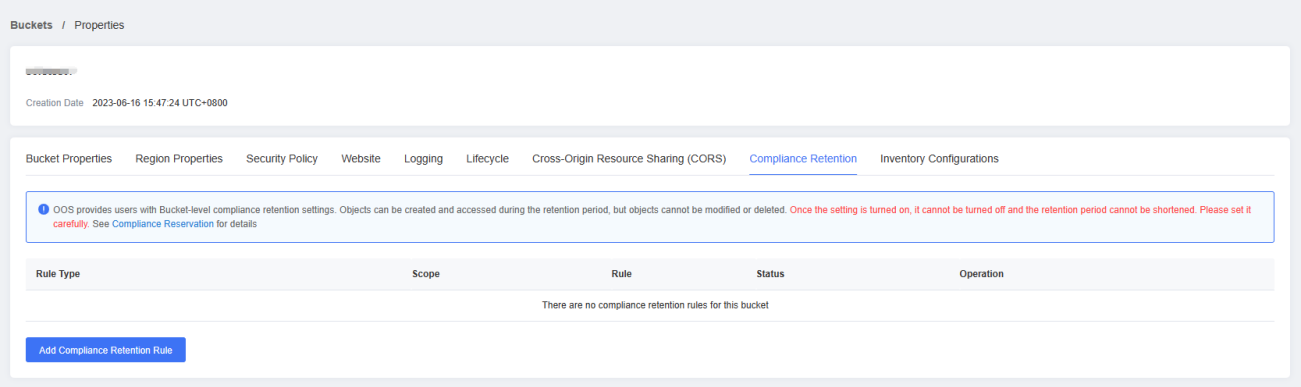
Click Add **`Cross-Origin Rule`** to add a new cross-origin rule:



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.



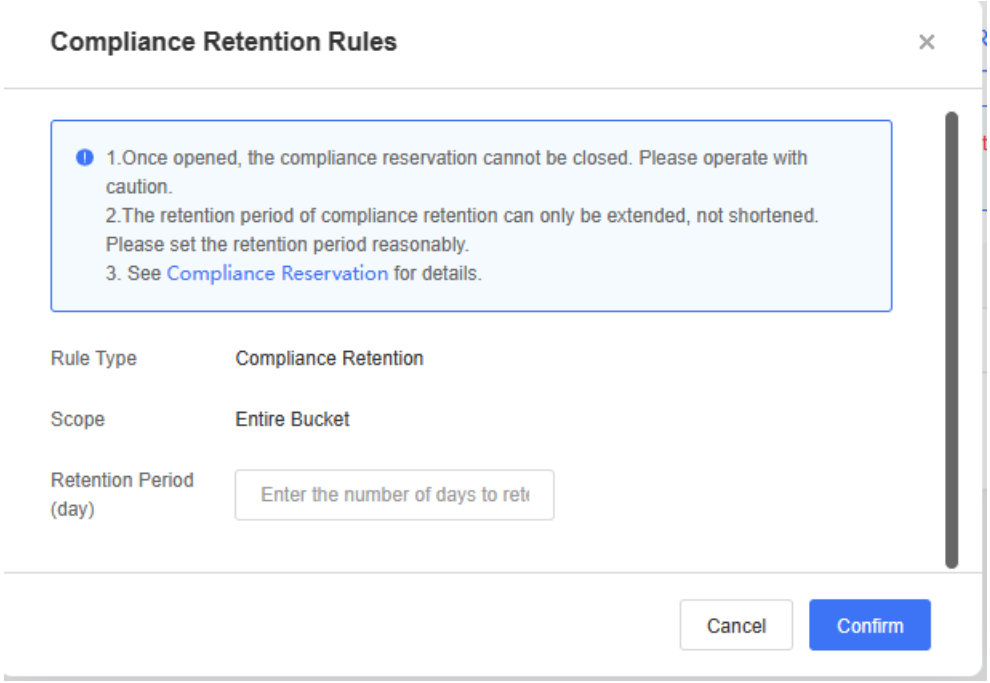
Item	Description
Rule Type	The rule type is Compliance Retention.
Scope	Scope of application of compliance retention rule. Currently, it is the entire bucket.
Rule	Compliance retention period.
Status	Status of compliance retention rule: ● Enable ● Disable
Operation	You can operation the compliance retention 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.

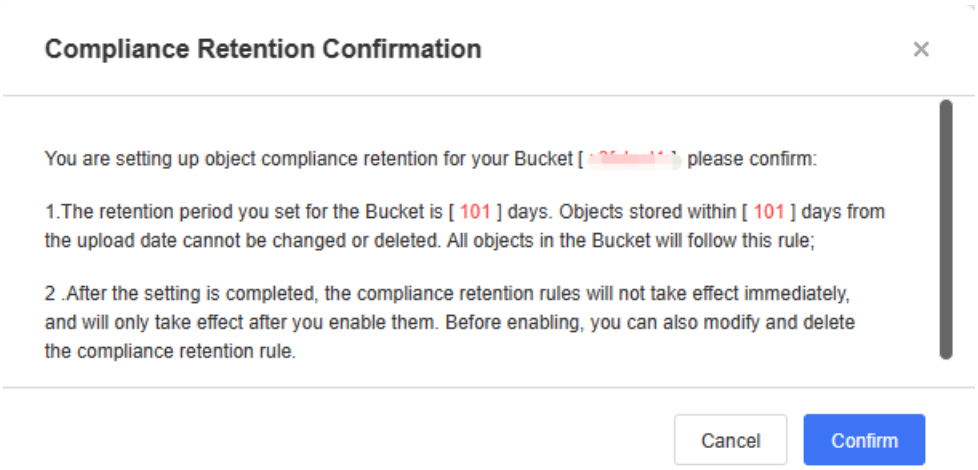
You can enable a compliance retention rule as following:

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

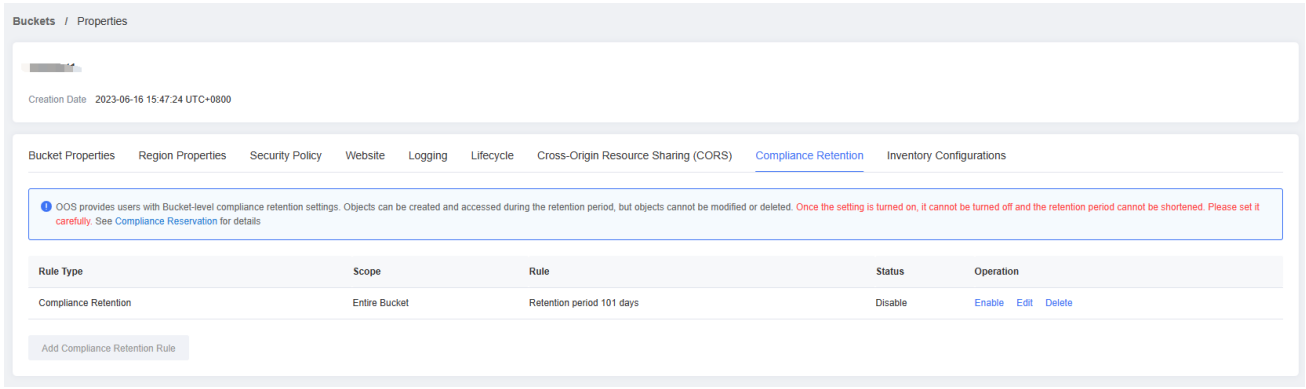
   If compliance retention has been added and has not been enabled, you can click **Edit** in the **Operation** column to make modifications. If not modified, skip to step 3 to enable compliance retention.



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.



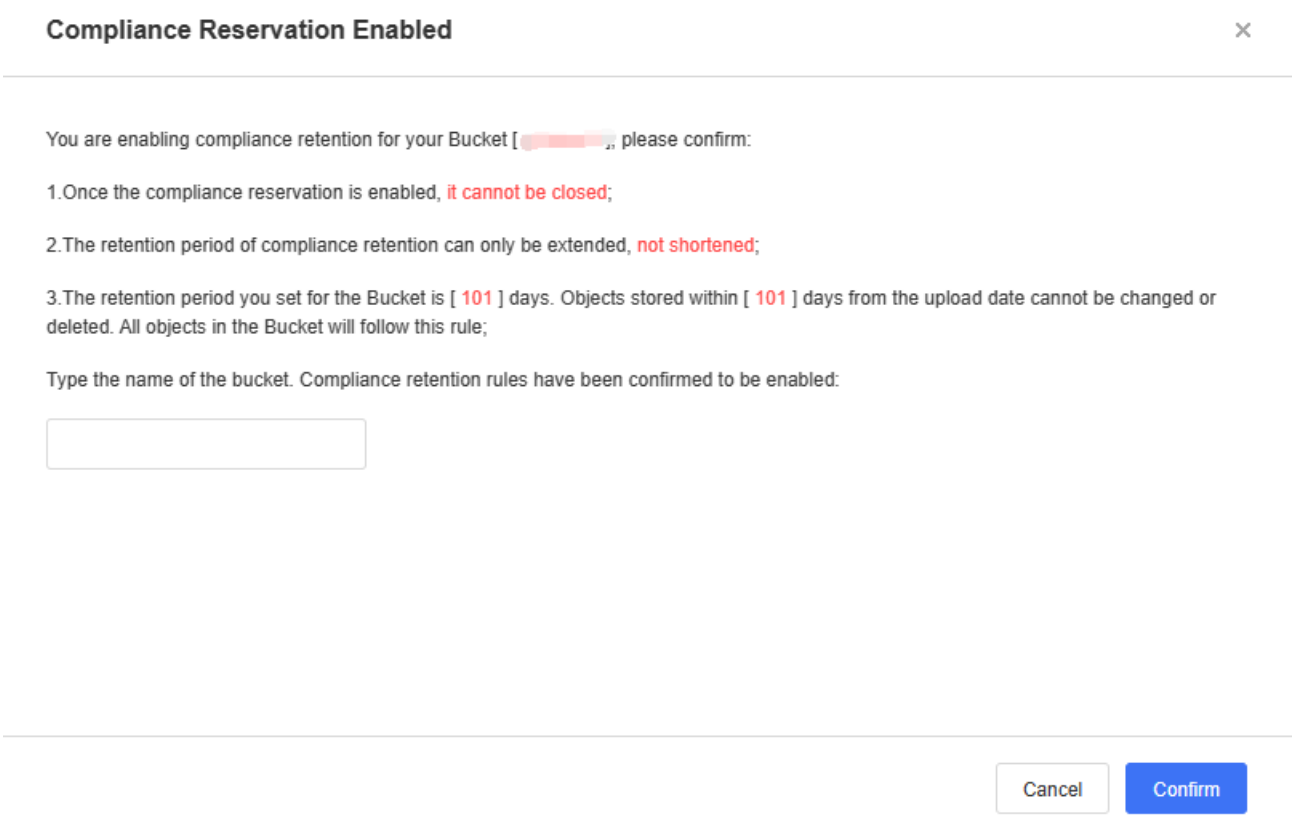
3. After clicking **Confirm**, a compliance retention is created.



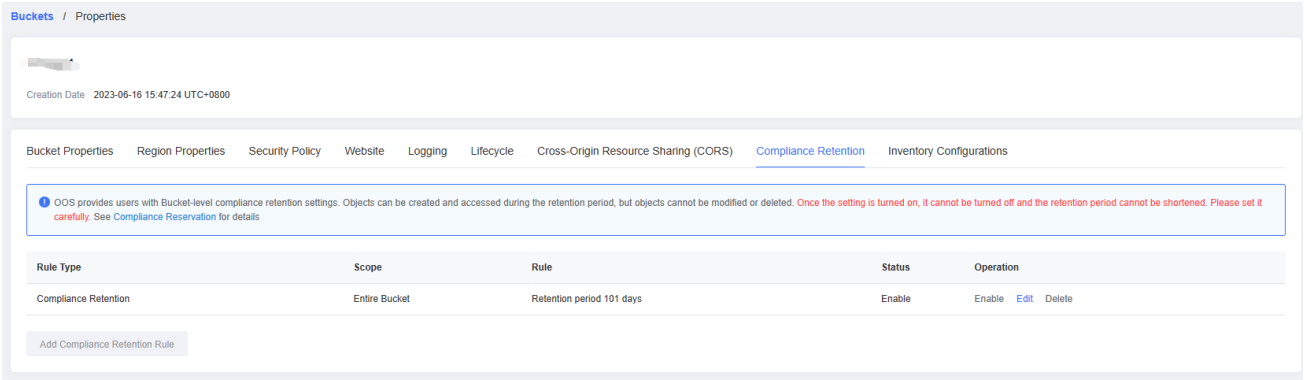
After the compliance retention is created, it is disabled by default, and it needs to be enabled by the

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.



5. After clicking **Confirm**, the compliance retention is enabled.



Note:

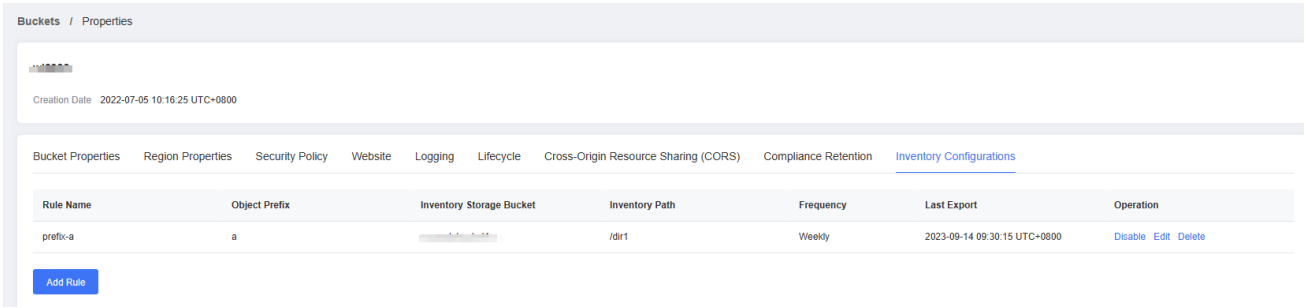
- Once the compliance retention function is enabled, it cannot be disabled, and the compliance retention period cannot be shortened, but the compliance retention period can be extended.
- The compliance retention time is accurate to the second. For example, set the compliance retention time for Bucket 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

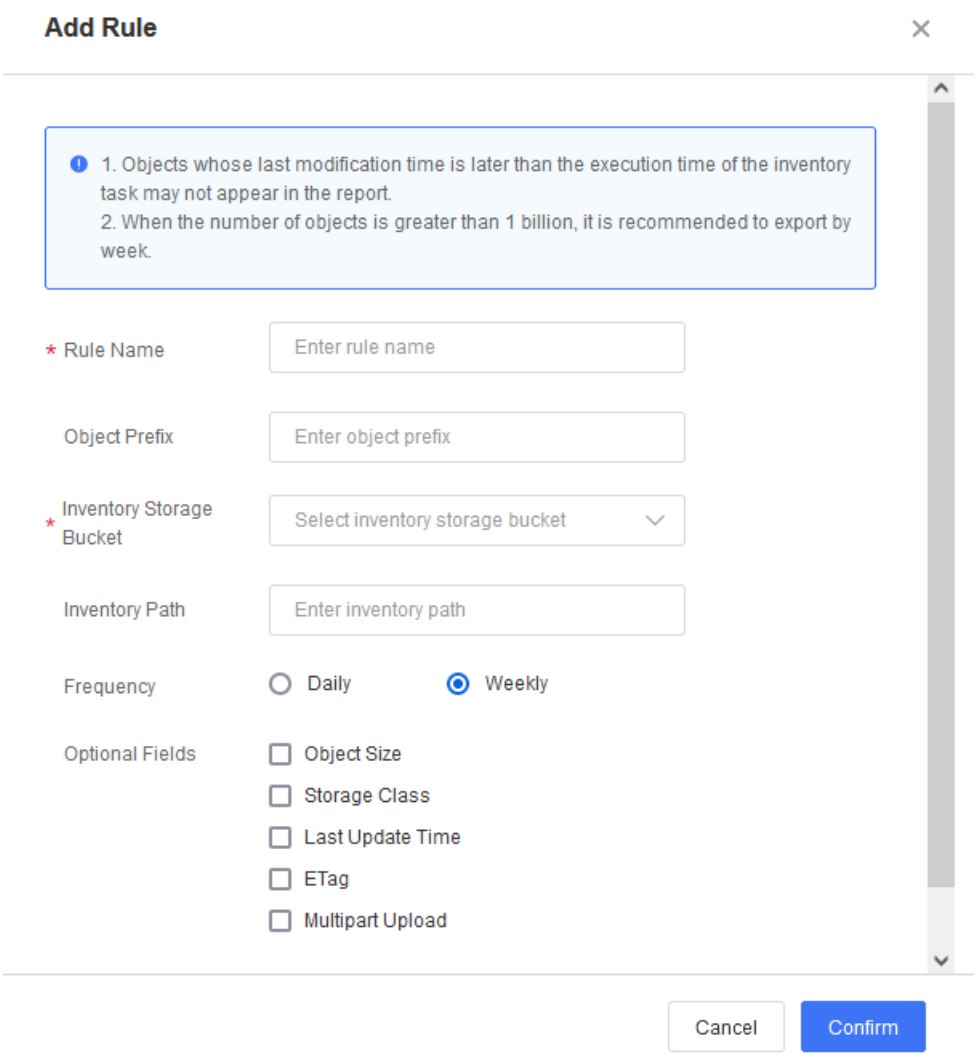
You can use an inventory to obtain information about specific objects in the bucket, such as sizes, storage classes. Compared to the GET Bucket (List Objects) API, the inventory list file can output relevant information of specified objects in CSV format by day or week, without affecting the bucket's 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.



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.



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.

	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. ● 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. **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	Items included in the inventory file, and multiple items can be specified. ● Object Size: The size of the object. ● Storage Class: The storage class of the object. ● Last Update Time: The last modified time of the object. ● 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:

```
dest_bucket
      └──destination-prefix
                  └──src_bucket
                              └──inventory_id
                                        ├──YYYY-MM-DDTHH-MMZ
                                        │                  ├──manifest.json
                                        │                  └──manifest.checksum
                                        └──data
```

```
└──UUID.csv.gz
```

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-MMZ	This directory is the time when scanning the source bucket started, with a 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, OOS will 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.

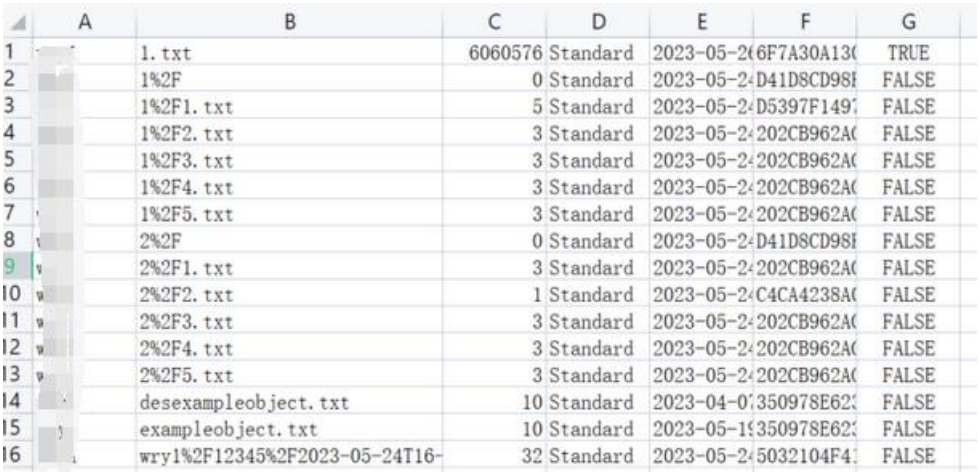
```
{
    "destinationBucket": "testbucket1",
    "fileSchema": "Bucket, Key, Size, StorageClass, LastModifiedDate, ETag, IsMultipartUploaded",
    "creationTimestamp": "1692856559088",
    "files": [
        {
            "MD5checksum": "3970e82605c7d109bb348fc94e9eecc0",
            "size": 20,
            "key": "abc/testbucket2/bucketempty/data/8b87dce0-26a5-4377-ab63-70e484764ba5.csv.gz"
        }
    ],
    "sourceBucket": "testbucket2",
    "version": "2023-08-30",
    "fileFormat": "CSV"
}
```


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. ● 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: 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 *destination-prefix*/*src_bucket*/*inventory_id*/data/*filename*. The d*estination-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”.



	A	B	C	D	E	F	G
1		1.txt	6060576	Standard	2023-05-2(	6F7A30A13(	TRUE
2		1%2F	0	Standard	2023-05-2	D41D8CD98I	FALSE
3		1%2F1.txt	5	Standard	2023-05-2	D5397F149	FALSE
4		1%2F2.txt	3	Standard	2023-05-2	202CB962A(	FALSE
5		1%2F3.txt	3	Standard	2023-05-2	202CB962A(	FALSE
6		1%2F4.txt	3	Standard	2023-05-2	202CB962A(	FALSE
7		1%2F5.txt	3	Standard	2023-05-2	202CB962A(	FALSE
8		2%2F	0	Standard	2023-05-2	D41D8CD98I	FALSE
9		2%2F1.txt	3	Standard	2023-05-2	202CB962A(	FALSE
10		2%2F2.txt	1	Standard	2023-05-2	C4CA4238A(	FALSE
11		2%2F3.txt	3	Standard	2023-05-2	202CB962A(	FALSE
12		2%2F4.txt	3	Standard	2023-05-2	202CB962A(	FALSE
13		2%2F5.txt	3	Standard	2023-05-2	202CB962A(	FALSE
14		desexampleobject.txt	10	Standard	2023-04-0	350978E62	FALSE
15		exampleobject.txt	10	Standard	2023-05-1	350978E62	FALSE
16		wry1%2F12345%2F2023-05-24T16-	32	Standard	2023-05-2	5032104F4	FALSE

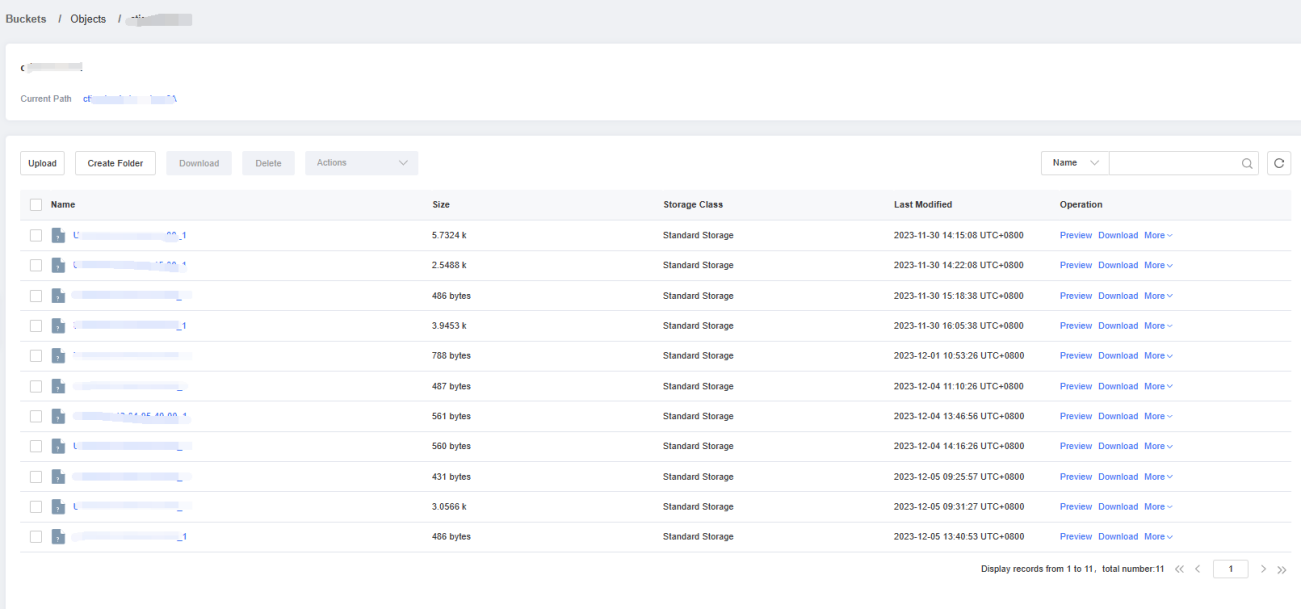
The fields in the inventory list file left to right are described as follows.

Field Name	Description
Bucket	The bucket where the object is located.
Key	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.

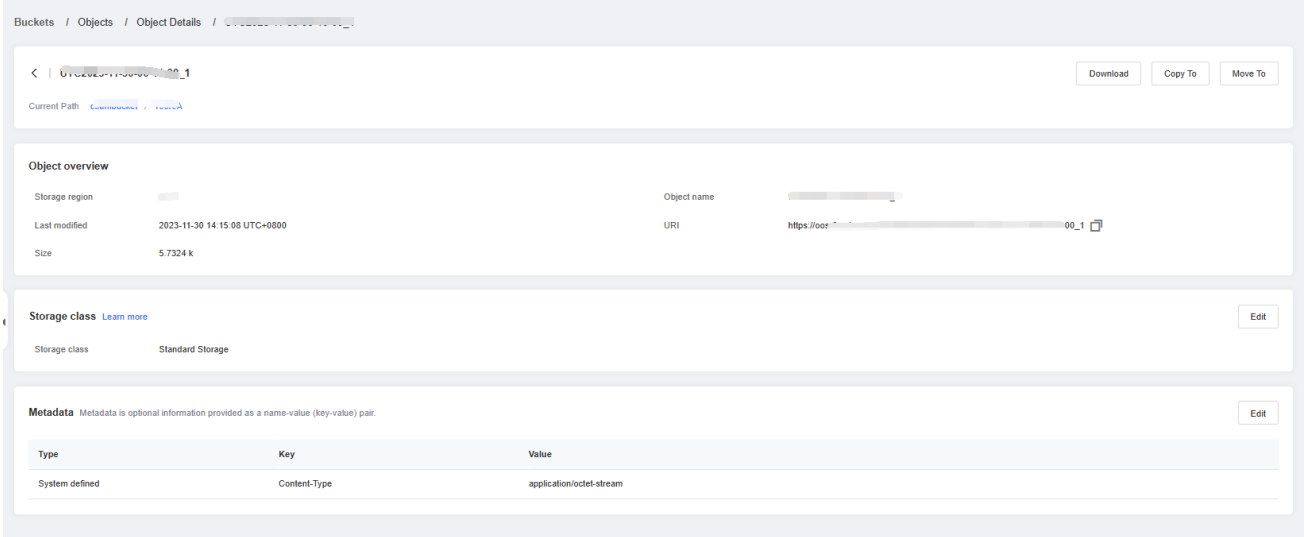


For IAM users, they can operate objects only if they have the corresponding permissions. The permissions required are as follows.

Operation	Permission
Upload File	oos:ListAllMyBucket, oos:ListBucket, oos:PutObject
DownLoad Object	oos:ListAllMyBucket, oos:ListBucket, oos:GetObject
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
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.



Item	Description
Object overview	You can view the following information: ● Storage region The data location where object is stored ● Object name. ● Last modified: The last modification time of the object. ● 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**.

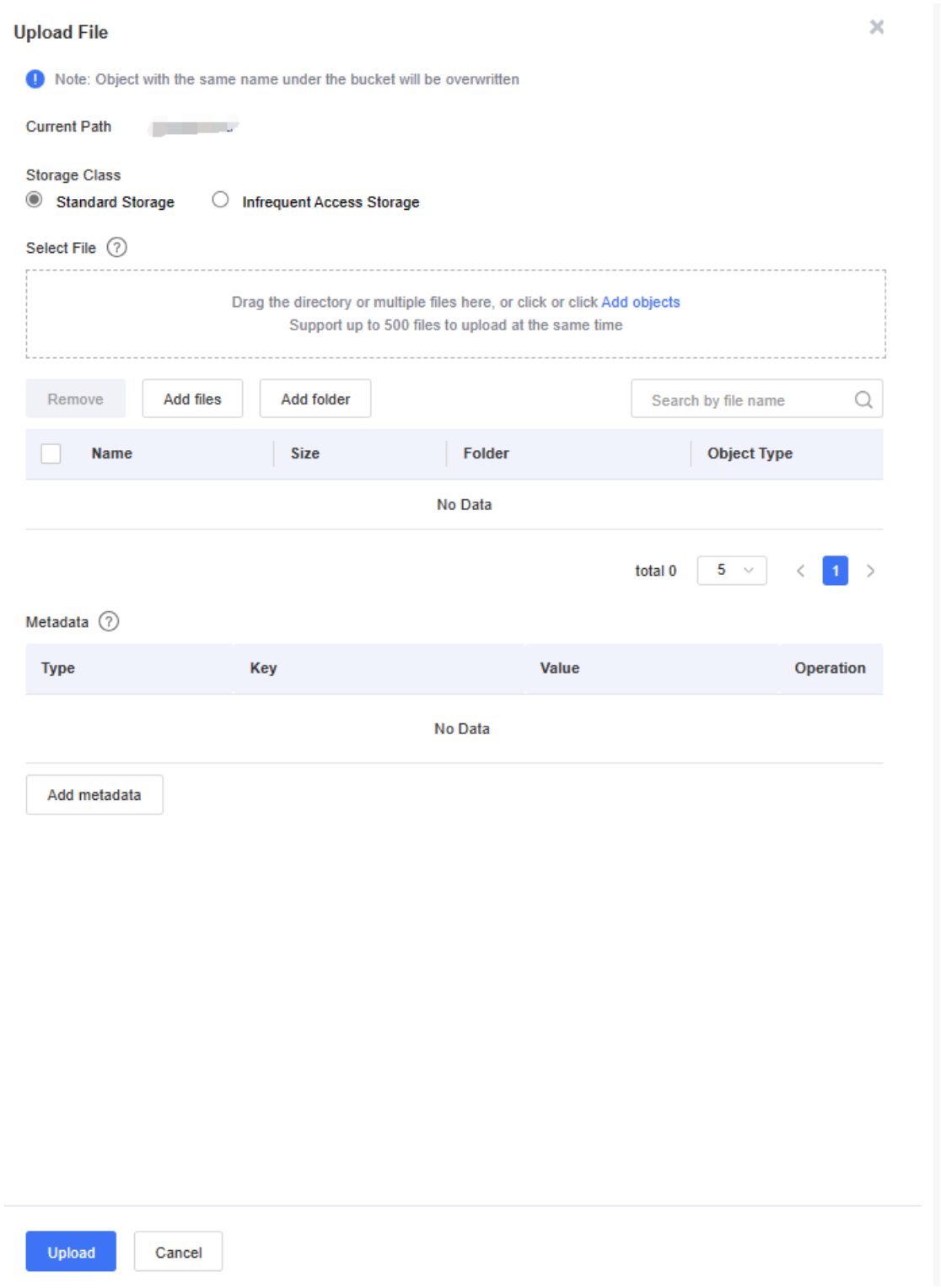
5.2.2 Uploading Objects

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.



Item	Description
Current Path	The location of the files upload.
Storage Class	The storage class of files: ● **`Standard Storage`**: 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 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.
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 **Remove** 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
  ```

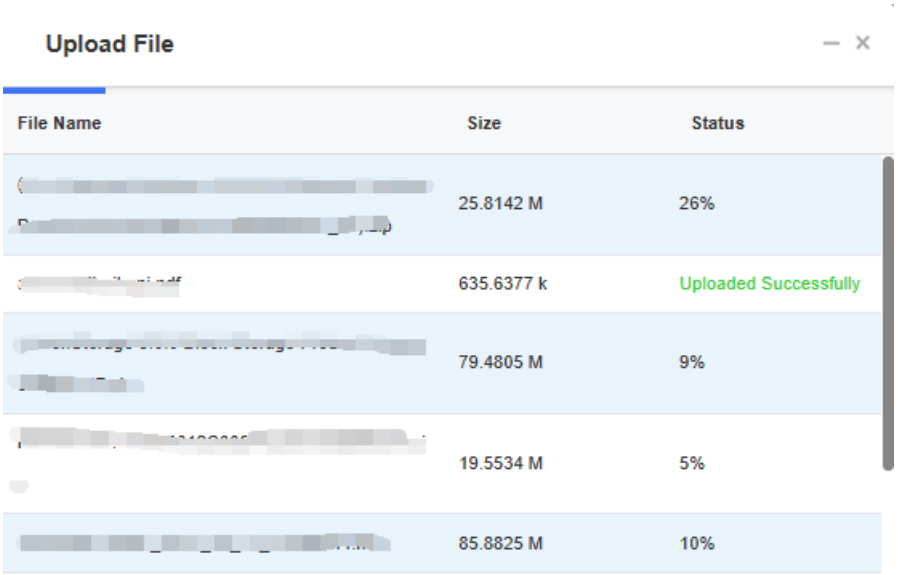
- Click **`Add files`**, and a dialog box for uploading files will pop up. You can select one or more objects

to upload.

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

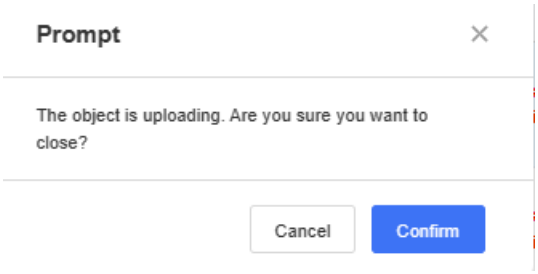
During files upload process, you can view the upload status of each file:

- 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`**.



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

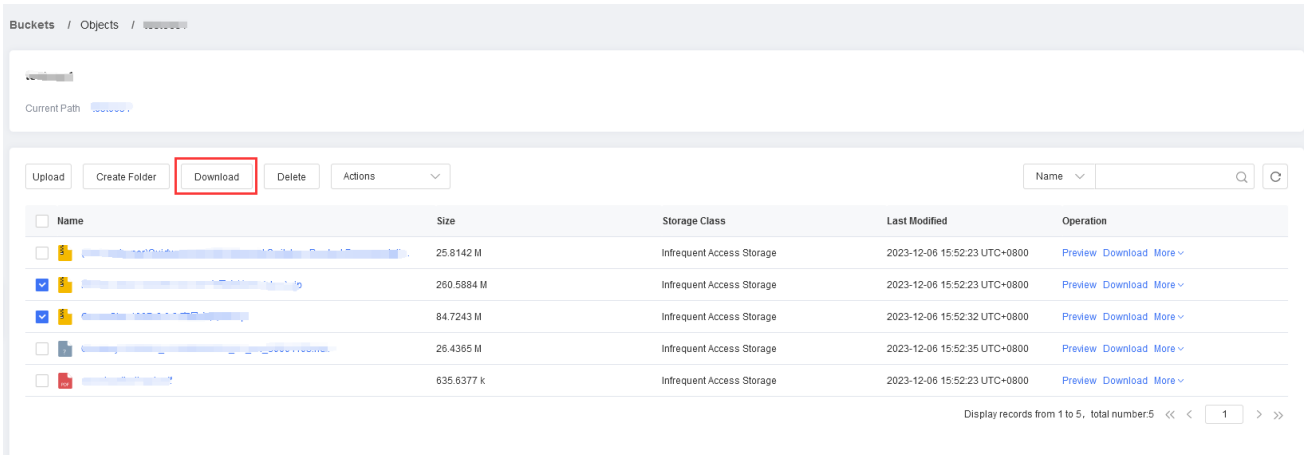
- **`Confirm`:** Terminate uploading files.
- **`Cancel`:** Continue uploading files.



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.



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. ● no-store: The file will not be cached. ● 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. ● max-age=<seconds>: The relative expiration time of cache files, 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. ● Content-Disposition:attachment: The file is downloaded to the 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: ● If the file name contains special characters such as asterisks (*) and forward slashes (/), special character escape may occur. For example, when downloading **test *. jpg** locally, it may be escaped as **test. jpg**. ● 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**.txt**" from OOS to the local location, it is necessary to keep the file name as "中文**.txt**" 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: ● identity: The file has not been compressed or encoded. ● 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. ● br: The file is encoded using the Brotli algorithm. The default value is identity. For more information about Content Encoding, please refer to RFC2616.
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.
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

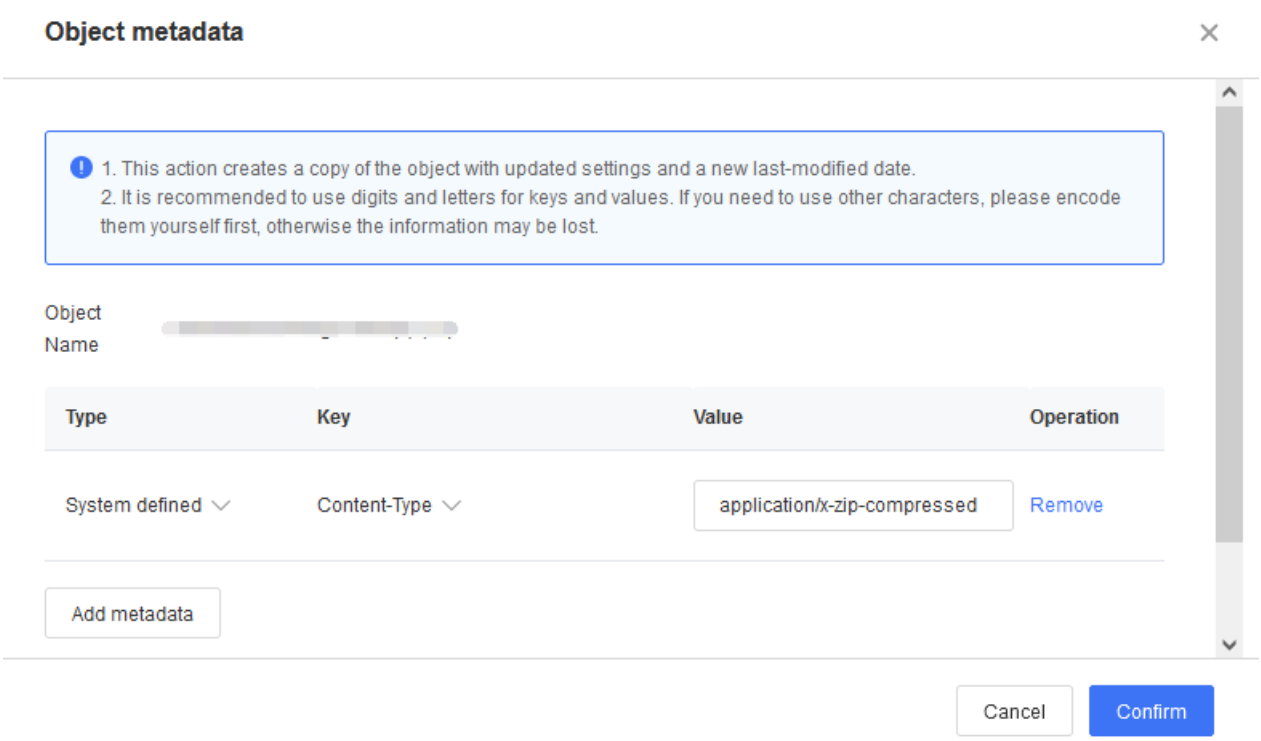
Field	Description
x-amz-meta-*	User metadata. The key must be a partial value of printable characters in ASCII. Unsupported characters can be found in the table below. The value is a character within ISO 8859-1, excluding (space).

Values that cannot be taken from 95 ASCII printable characters.

ASCII Decimal	Graphical	ASCII Decimal	Graphical
32	（space）	61	=
34	"	62	>
40	(	63	?
41	)	64	@
44	,	91	[
47	/	92	\
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.



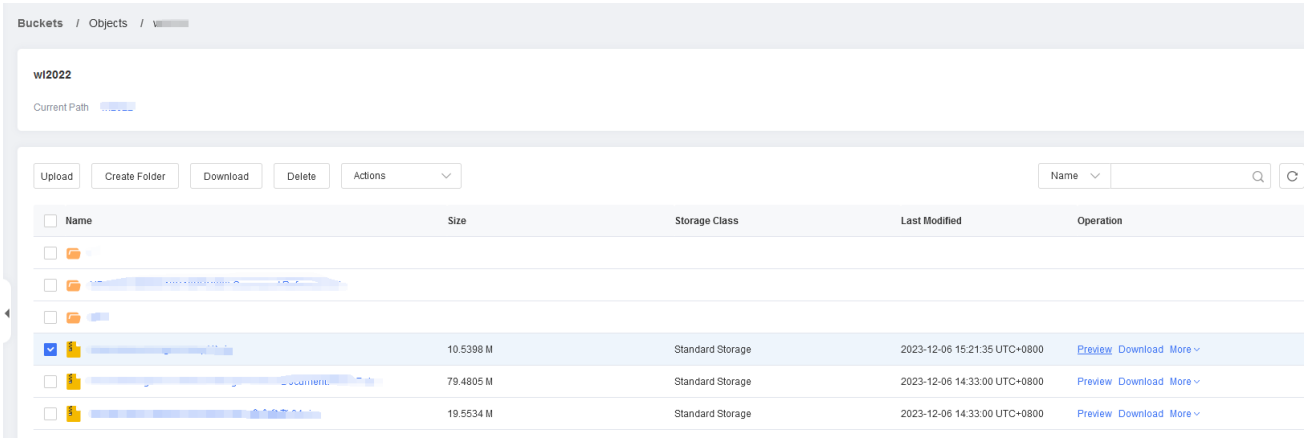
Click **Add metadata**, you can modify the system metadata or user metadata.

Items	Description
Type	The type of the object metadata: ● System defined: system metadata. ● User defined: user metadata.
Key	The specific metadata: If the type is **System defined**, values: ● Cache-Control ● Content-Disposition ● Content-Encoding ● Content-Type ● Content-Language ● Expires ● x-amz-website-redirect-location If the type is **User defined**, the value is x-amz-meta-*.
Value	The value of the specific metadata.
Operation	Click **Remove**, 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.



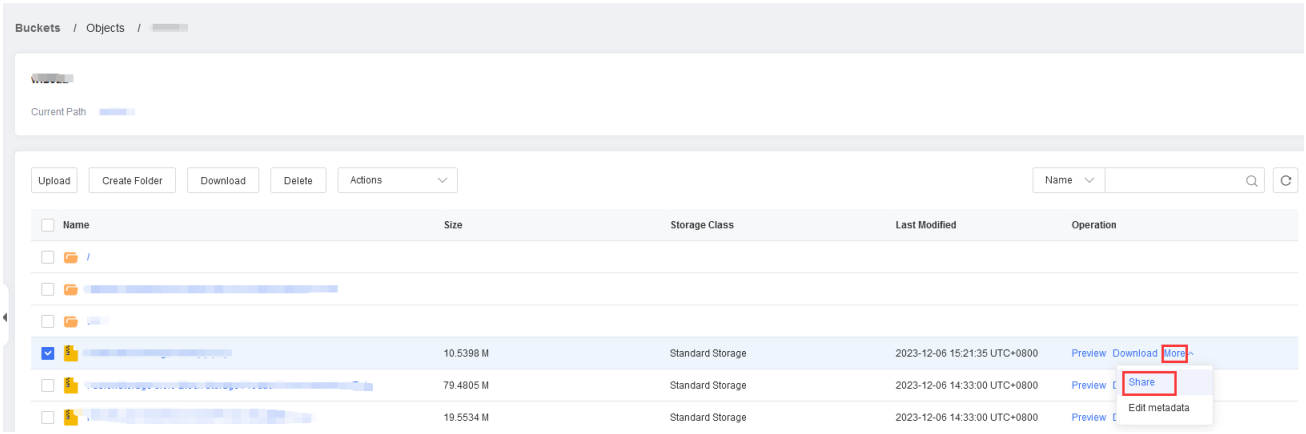
5.2.6 Sharing Objects

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

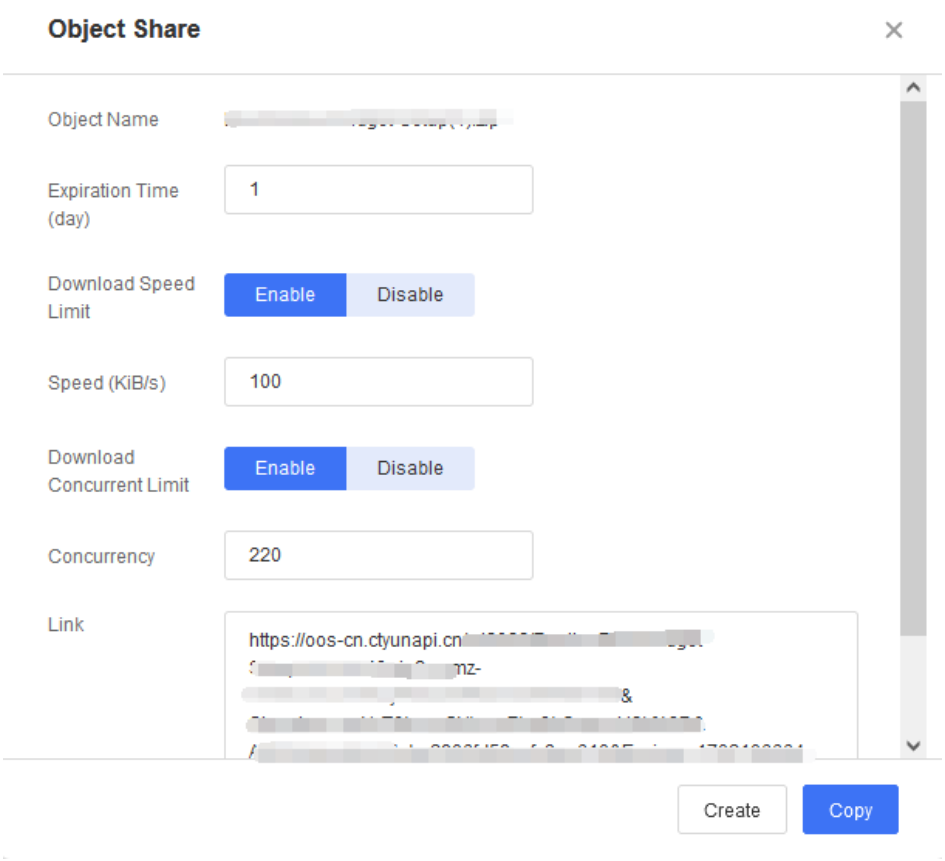
Note: When sharing pictures or webpages, visitors will download them locally for viewing.

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.



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

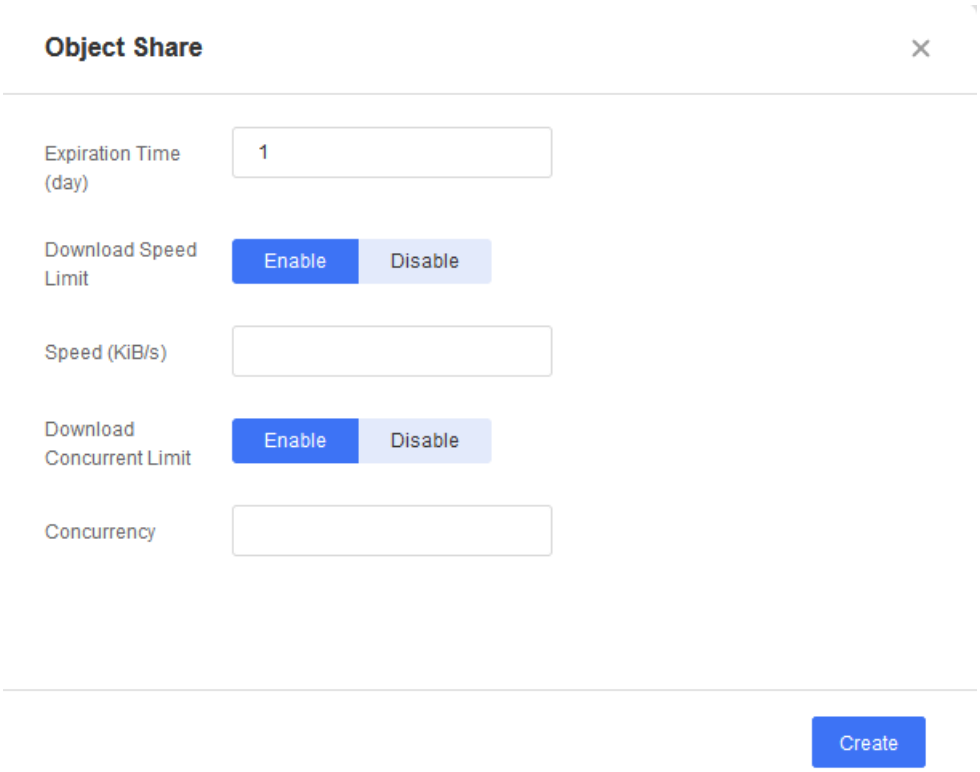


Name	Description
Object Name	The name of the object to be shared.
Expiration Time (day)	Set expiration time. The value range is [1, 9999999], and the unit is days. **Note:** If left blank, the sharing link will expire in 15 minutes by default.
Download Speed Limit	Whether to enable the download speed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



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 Limit	Whether to enable the download speed limit: ● Enable ● Disable
Speed (KiB/s)	Set download speed limit. The value range is [1, 2147483647], and the unit is KiB/s.
Download Concurrent Limit	Whether to enable the download concurrent limit: ● Enable ● Disable
Concurrency	Set download concurrent limit: The value range is [1, 2147483647].

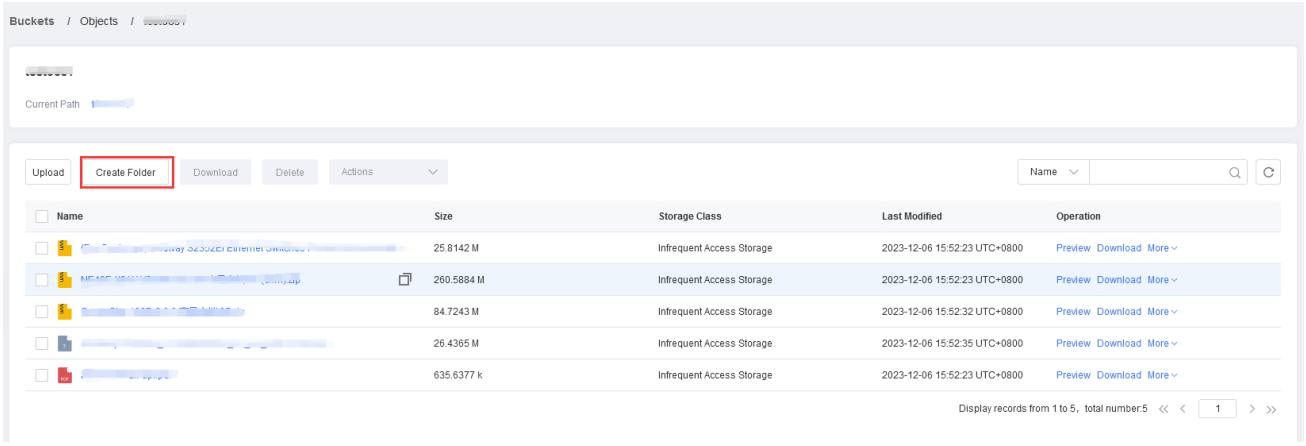
Clicking the **Create** button will generate a CSV file, in which users can view the specific sharing links for each file.

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:

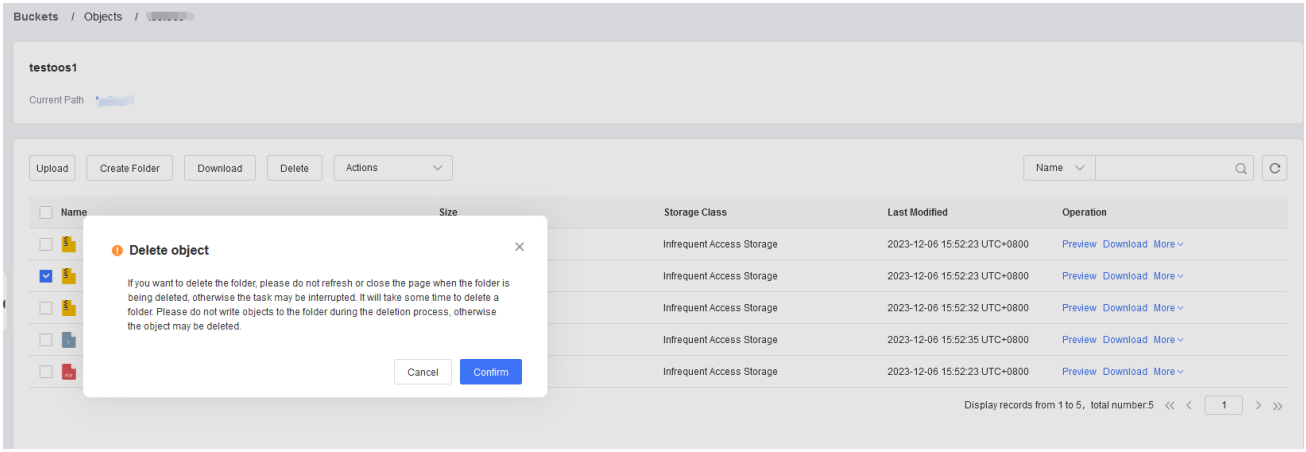
- The name is not empty;
- The name cannot contain the following special characters: ? " : / ' \ ;
- The name cannot start or end with a vertical bar (|);
- The name cannot be: dots (.) Or plus (+).



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.

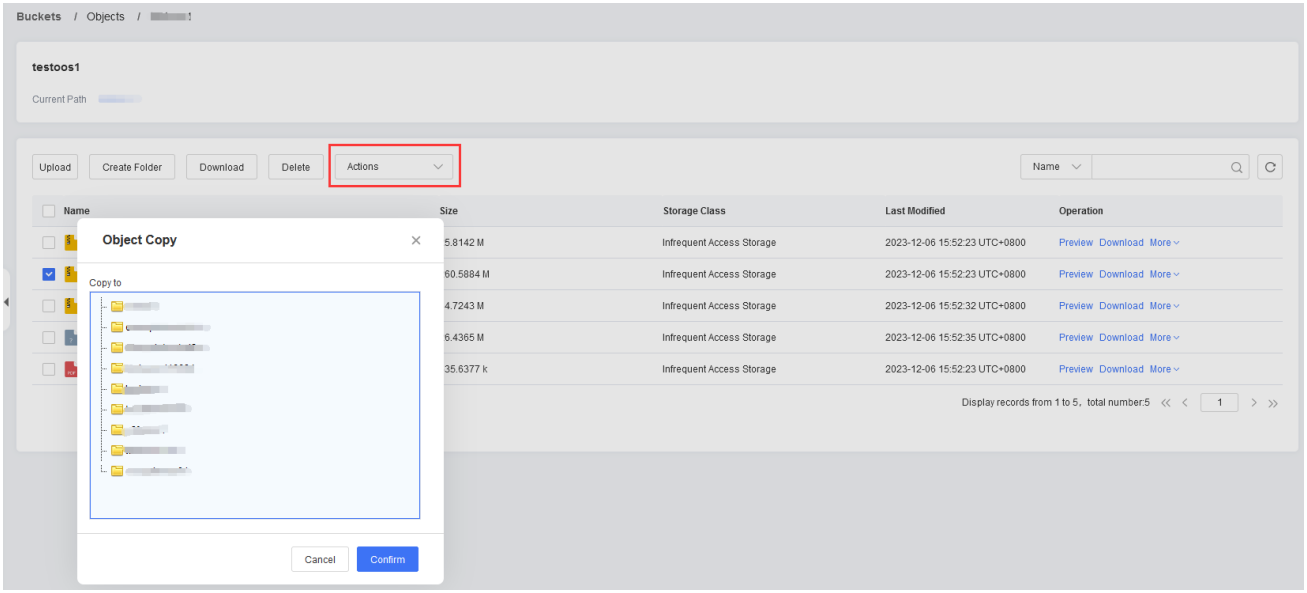


- Delete objects or folders by configuring lifecycle rules, as detailed in **Lifecycle** chapter.

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.

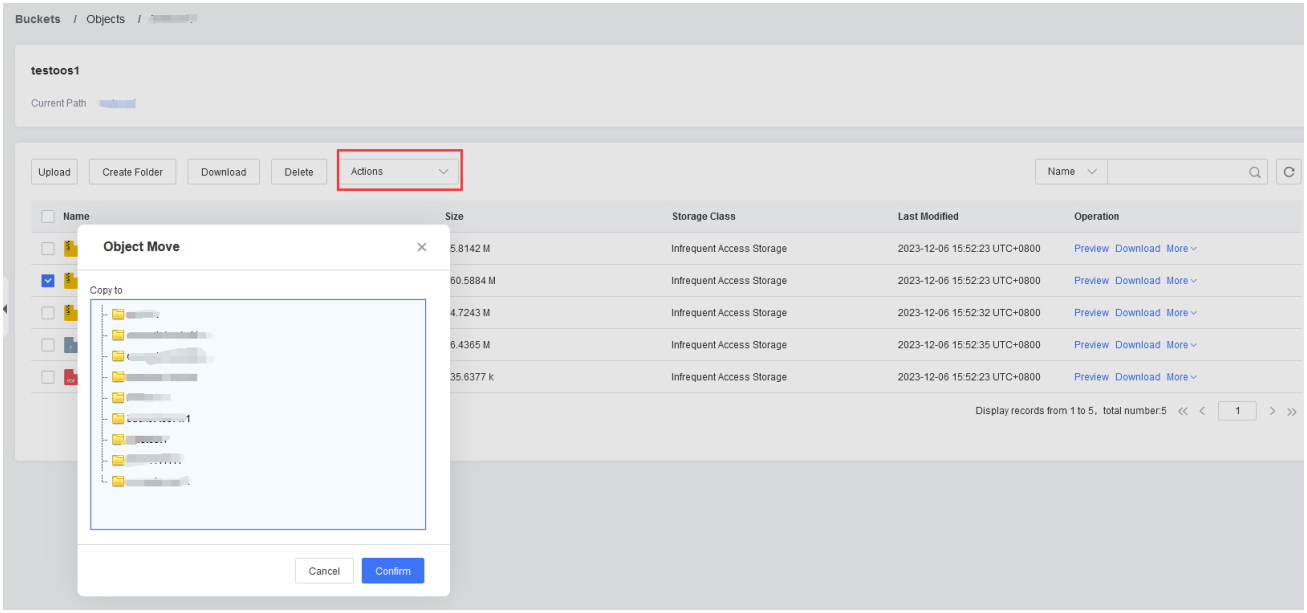
Note: Using the console operation, the single object copied is no larger than 5 GiB. If it exceeds 5 GiB, please call the API interface **PUT Object -Copy** or **Copy Part** to operate.



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.

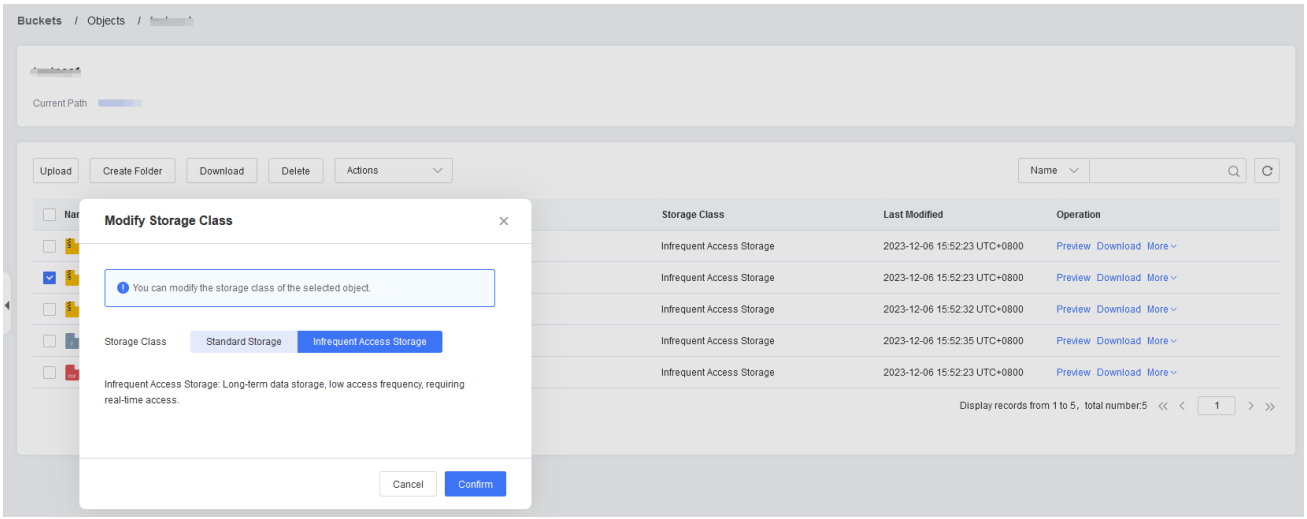
Note: Using the console operation, the single object moved is no larger than 5GiB. If it exceeds 5GiB, please call the API interface **PUT Object -Copy** or **Copy Part**, DELETE Object to operate.



5.2.11 Modifying Storage Classes

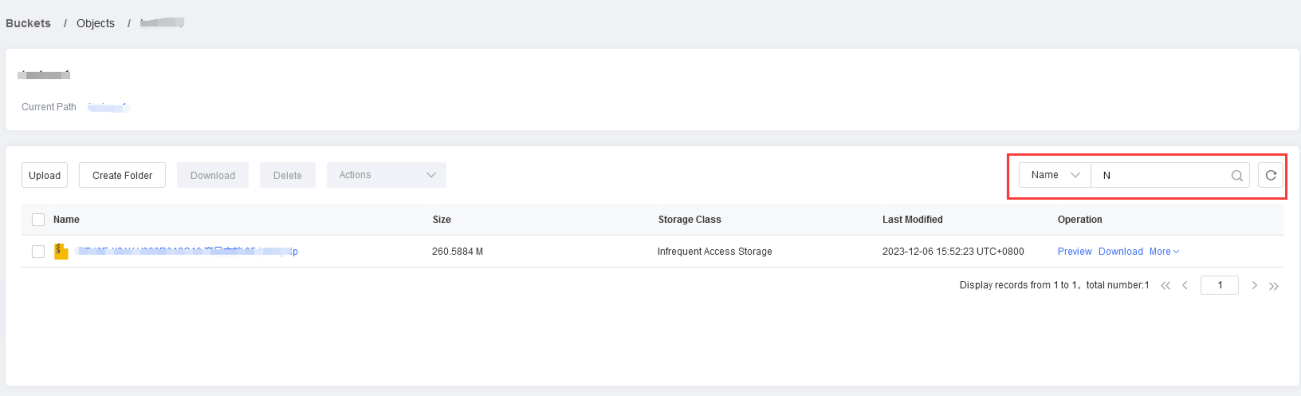
On the **Buckets** page, click on the corresponding bucket to enter the **Objects** page. Select objects that need to modify their storage type, click **Actions**> **Modify Storage Class** in the navigation bar, **Modify Storage Class** window will pop up, and you can modify storage classes for selected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

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



5.2.12 Searching for a File or Folder

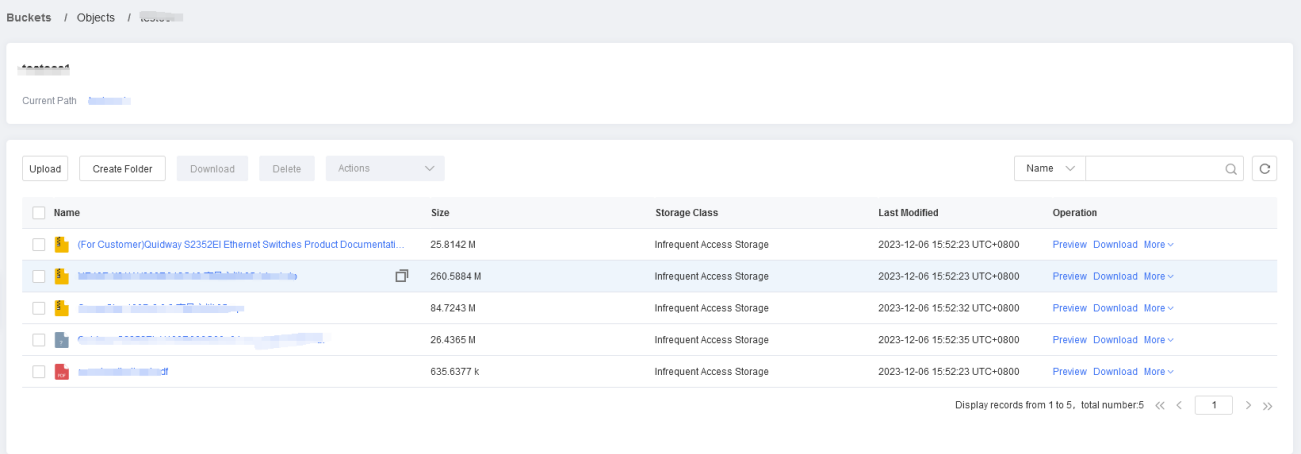
On the **Buckets** page, click on the corresponding bucket to enter the **Objects** page.
When there are many stored objects, you can search for the eligible files and folders by searching for the object prefix.



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



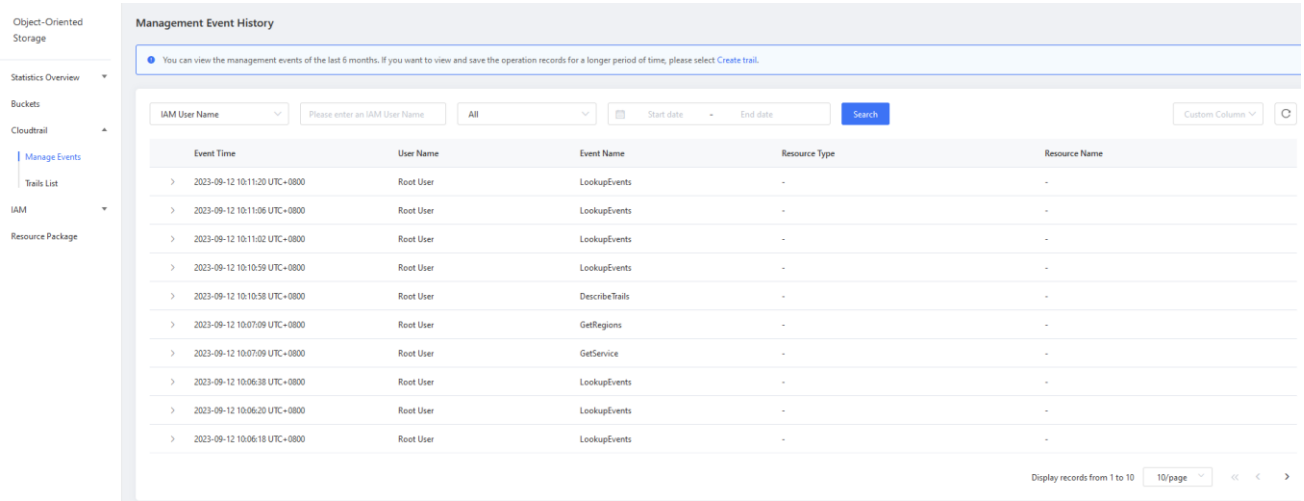
6 Cloudtrail

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.



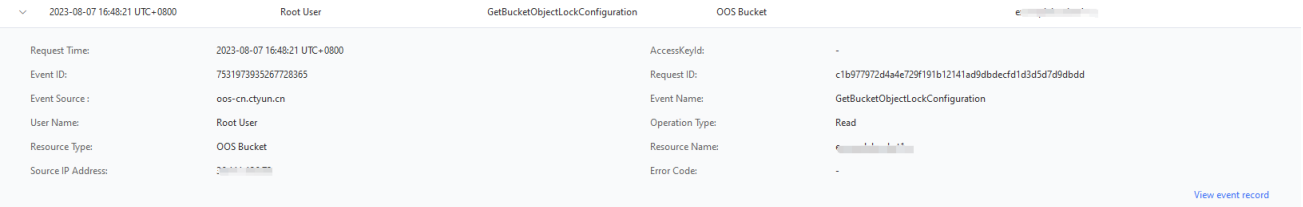
You can select the **IAM User Name**, **AccessKeyId**, **Event ID**, **Event Name**, **Event Source**, **Resource Name**, and **Resource Type** to query according to your needs, and you can also select the operation type (including: all types, read operations, and write operations), start and end time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



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: ■ OOS: oos-cnhk-hqnet.ctyunapi.cn (Hongkong Highquality Network), or oos-cnhk-nqnet.ctyunapi.cn (Hongkong Normal Network) ■ Cloudtrail: oos-cnhk-cloudtrail.ctyunapi.cn ■ IAM: oos-cnhk-iam.ctyunapi.cn ■ 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\":\"OOS
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.
sourceIp	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

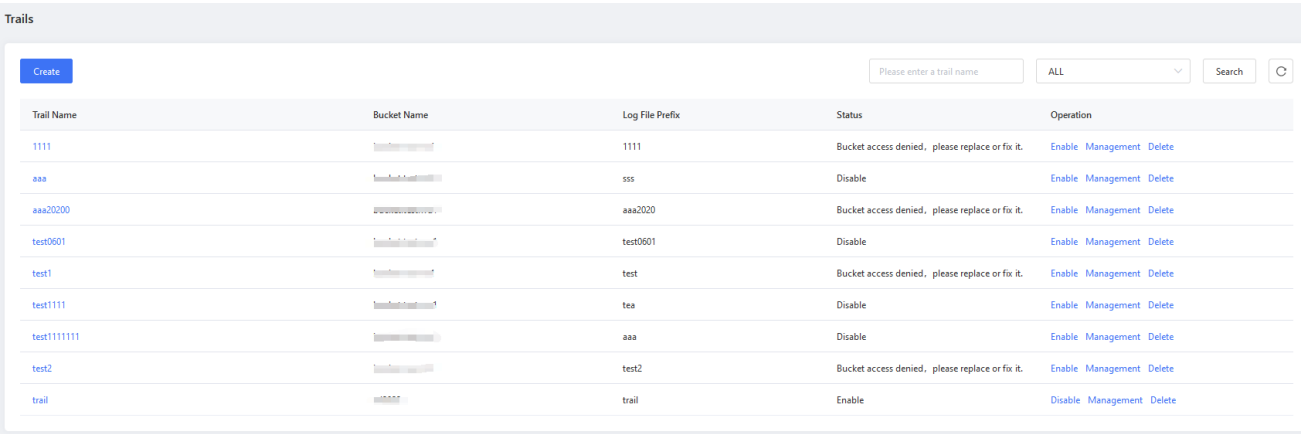
	GetBucketLocation
	CreateBucket
	PutBucketLifecycle
	PutBucketLogging
	GetBucketAcl
	PutBucketAcl
	GetBucketPolicy
	PutBucketPolicy
	DeleteBucketPolicy
	GetBucketWebsite
	PutBucketWebsite
	DeleteBucketWebsite
	ListMultipartUploads
	GetBucketLogging
	GetBucketCors
	PutBucketCors
	DeleteBucketCors
	PutBucketObjectLockConfiguration
	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

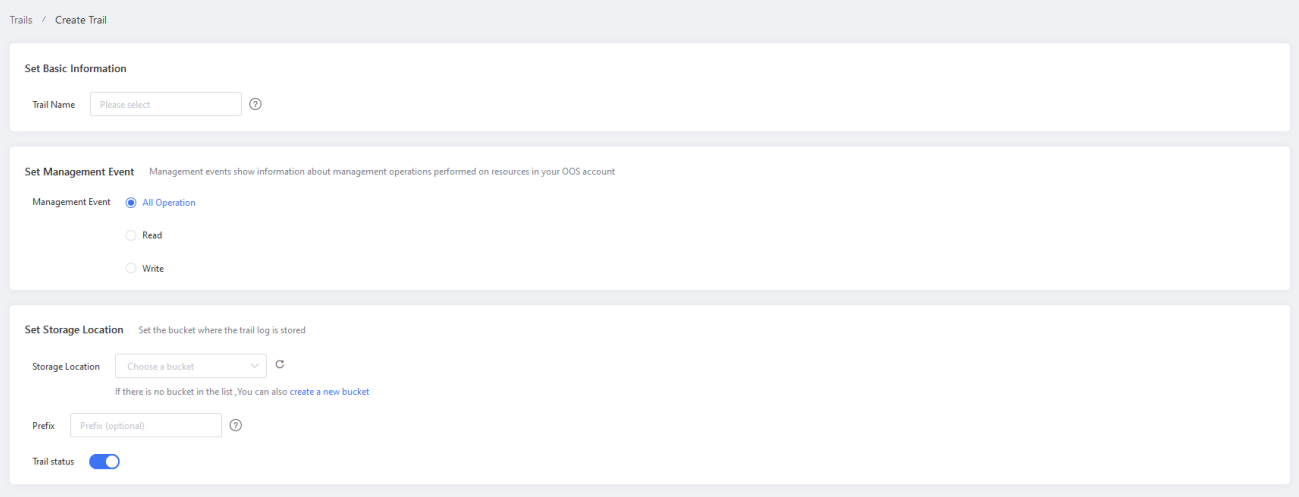
Enter **Trails List**, you can view all trails information under the current account, including: **Trail Name**, **Bucket Name**, **Log File Prefix**, **Status**, and **Operation**.



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.



- **`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>/OOSLogs/<AccountID>/CloudTrail/<year>/<month>/<day>/<log data file>`

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

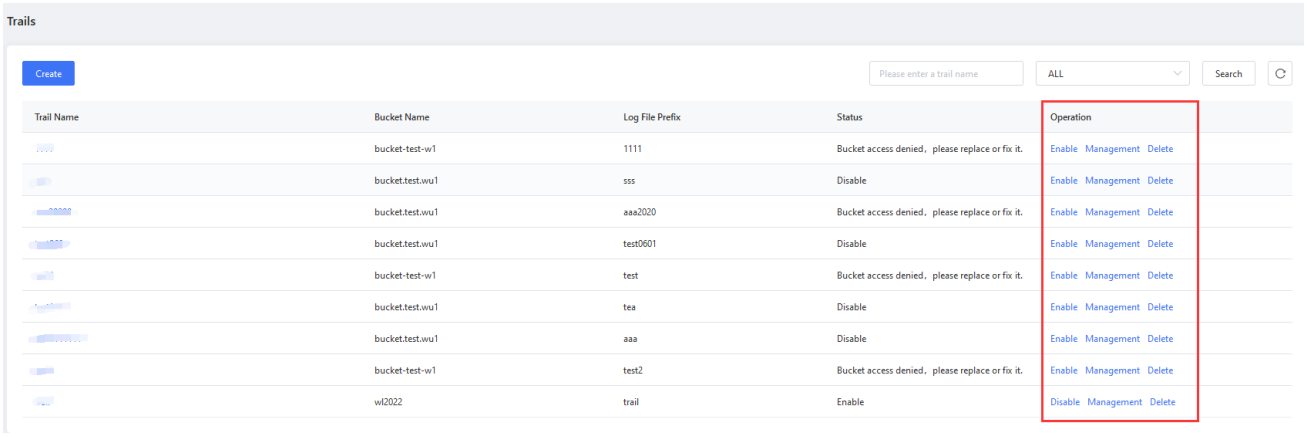
  oos://<*bucket*>/OOSLogs/<*AccountID*>/CloudTrail/<*year*>/<*month*>/<*day*>/<*log data file*>

➢ **Trail status**:

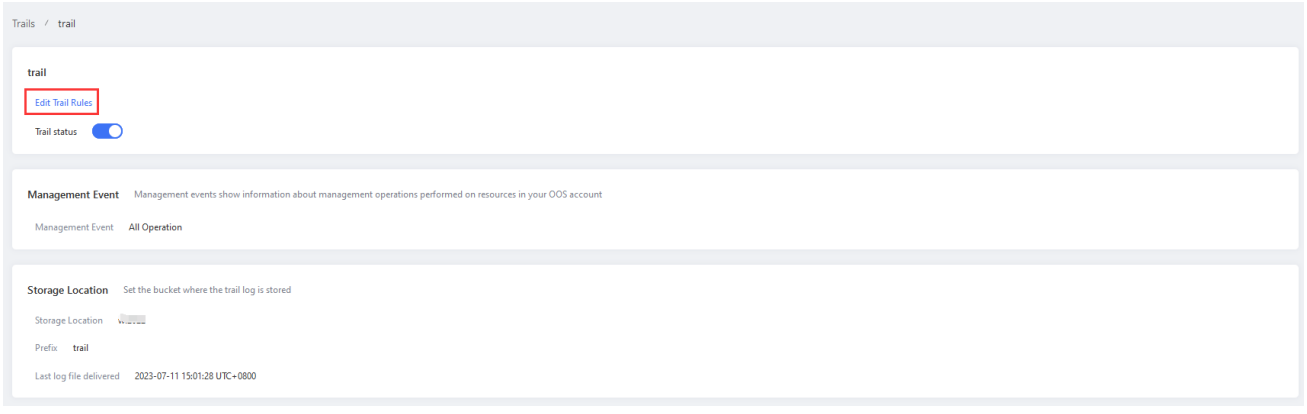
- **ON**: The trail is turned on;
- **OFF**: The trail is turned off.

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.



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**.



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.

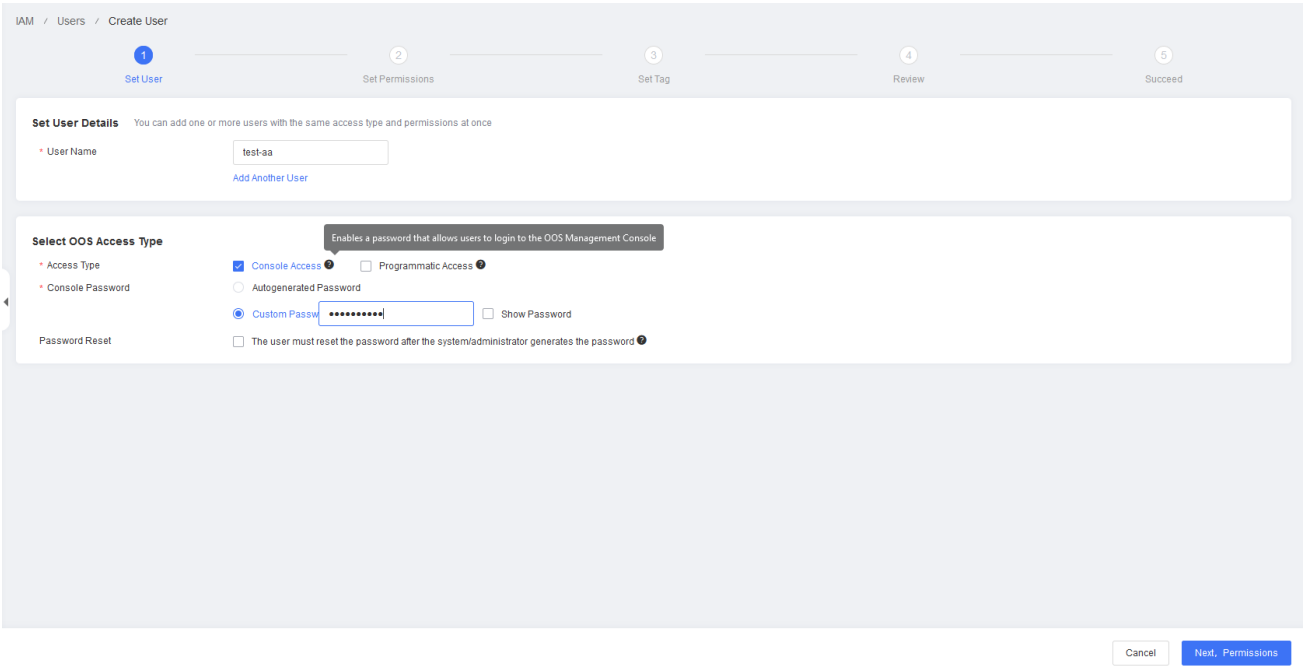
Operation		Permissions required
IAM User	Create IAM users	iam:CreateUser, iam:CreateAccessKey, iam:CreateLoginProfile, iam:GetAccountPasswordPolicy, iam:GetUser Suggested permissions: iam:AddUserToGroup, iam:AttachUserPolicy, iam:ListUsers, iam:ListGroups, iam:ListPolicies
	Delete IAM users	iam:ListUsers, iam:DeleteAccessKey, iam:DeleteUser, iam:RemoveUserFromGroup, iam:DeactivateMFADevice, iam:DeleteLoginProfile, iam:DetachUserPolicy
	View IAM user information	iam:ListAccessKeys, iam:ListUsers, iam:ListUserTags, 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 group	Create User Group	iam:CreateGroup 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 Policy	iam:CreatePolicy, iam:GetPolicy, iam:ListPolicies
	Delete the Custom Policy	iam:ListPolicies, iam:DeletePolicy, iam:DetachUserPolicy, iam:DetachGroupPolicy
	Attach/Deattach Users/Groups	iam:ListUsers, iam:ListGroups, iam:ListPolicies, iam:ListAttachedGroupPolicies, iam:ListAttachedUserPolicies, iam:ListEntitiesForPolicy, iam:AttachUserPolicy, iam:DetachUserPolicy, iam:AttachGroupPolicy, iam:DetachGroupPolicy
Security Setting	Edit Password Policy	iam:GetAccountPasswordPolicy, iam:UpdateAccountPasswordPolicy
	Delete Password Policy	iam:GetAccountPasswordPolicy, iam:DeleteAccountPasswordPolicy
	Edit Login Security Policy	iam:GetAccountLoginSecurityPolicy, iam:UpdateAccountLoginSecurityPolicy
	Delete Login Security Policy	iam:UpdateAccountLoginSecurityPolicy, iam:DeleteAccountLoginSecurityPolicy
Security Credential	AccessKeys	iam:ListAccessKeys, iam:GetUser, iam:CreateAccessKey, am:DeleteAccessKey, iam:UpdateAccessKey
	Password	iam:GetLoginProfile, iam:GetUser, iam:ChangePassword
	MFA	iam:ListMFADevices, iam:GetUser, iam:CreateVirtualMFADevice, iam:DeleteVirtualMFADevice, iam:EnableMFADevice, iam:DeactivateMFADevice

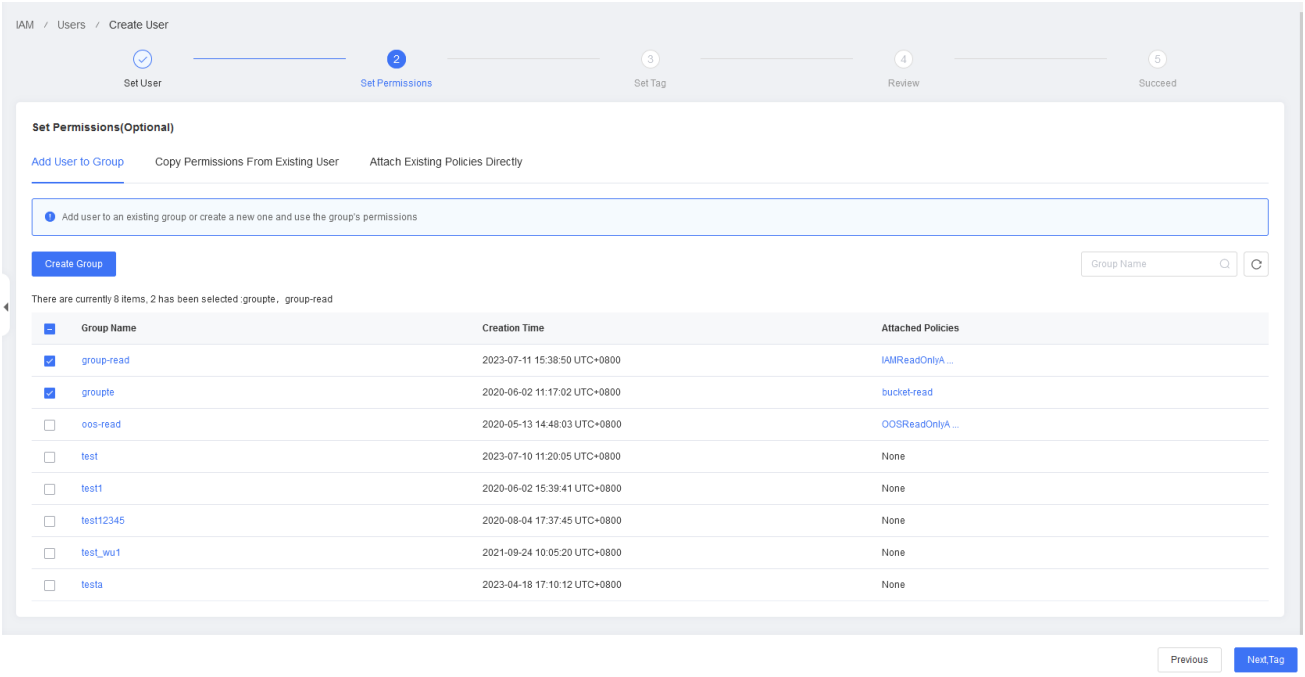
7.1 Getting Started

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

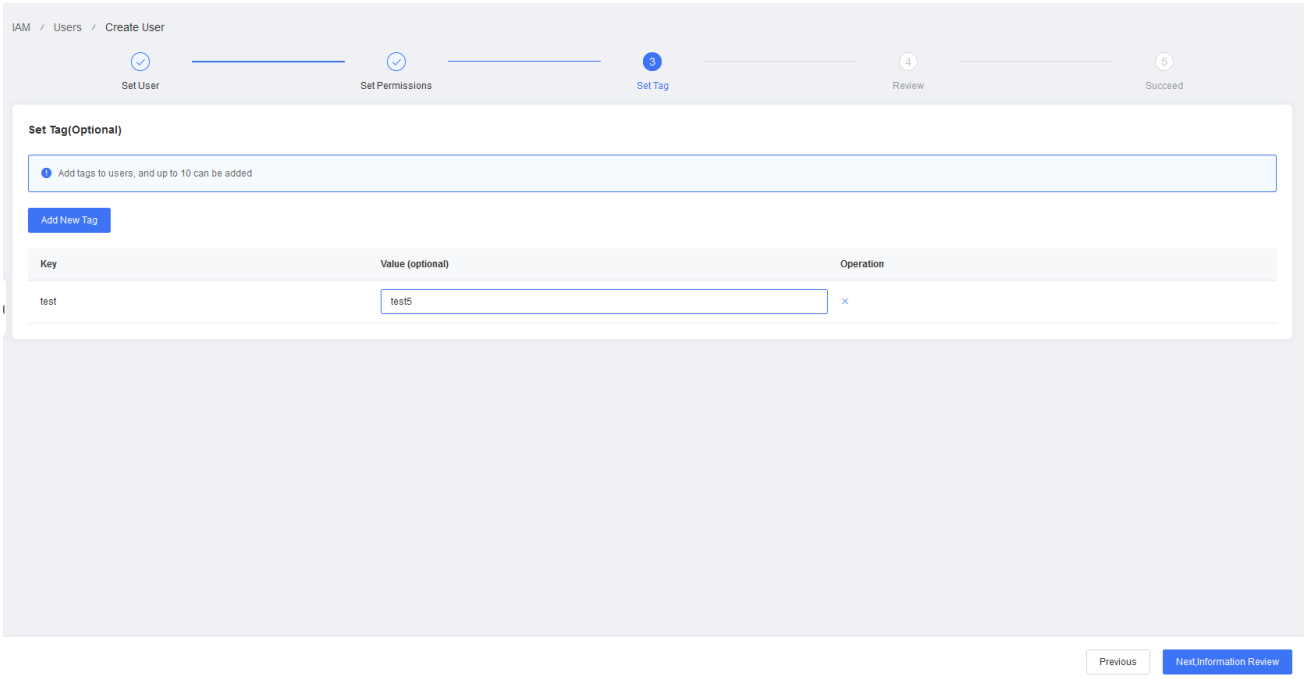
1. **Set User**: You can add one or more IAM users, and **Select OOS Access Type** for IAM users.



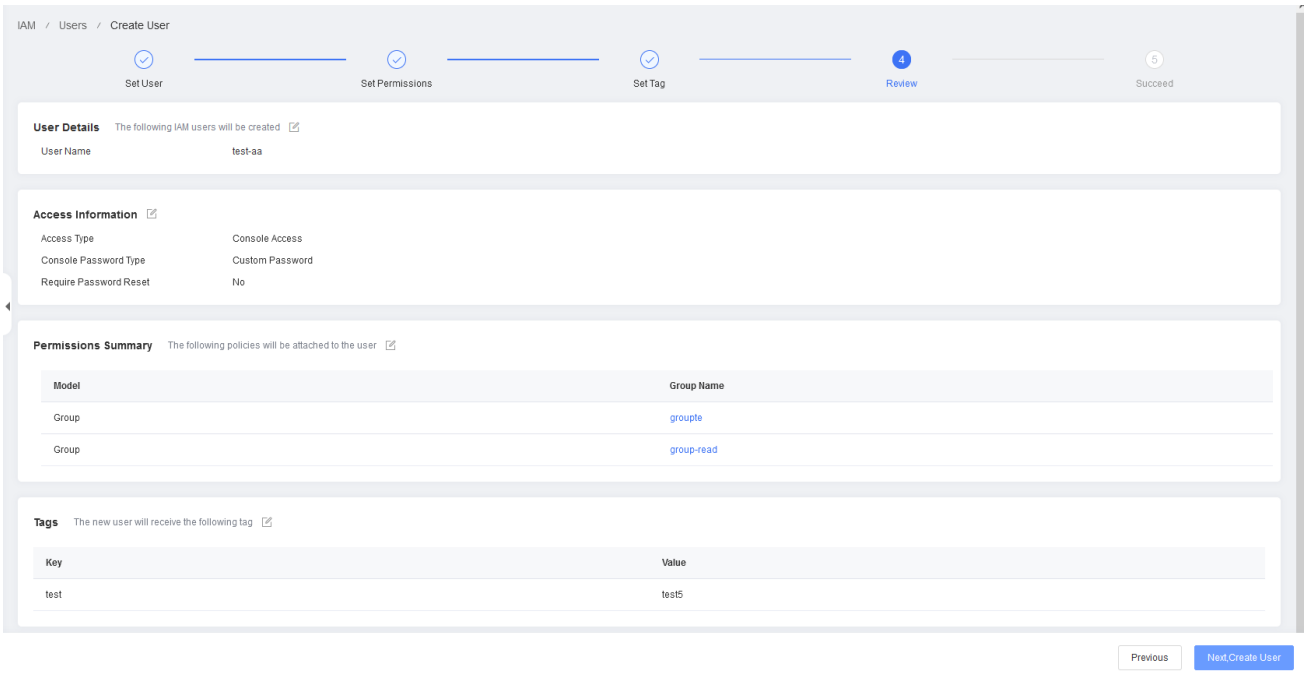
2. **Set Permissions** (Optional): To add permissions for IAM users, there are three ways to add permissions (only one can be selected).
   - **`Add User to Group`** (Prerequisite: There is already a user group): The IAM user will have all the permissions of the user group;
   - **`Copy Permissions From 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`**.



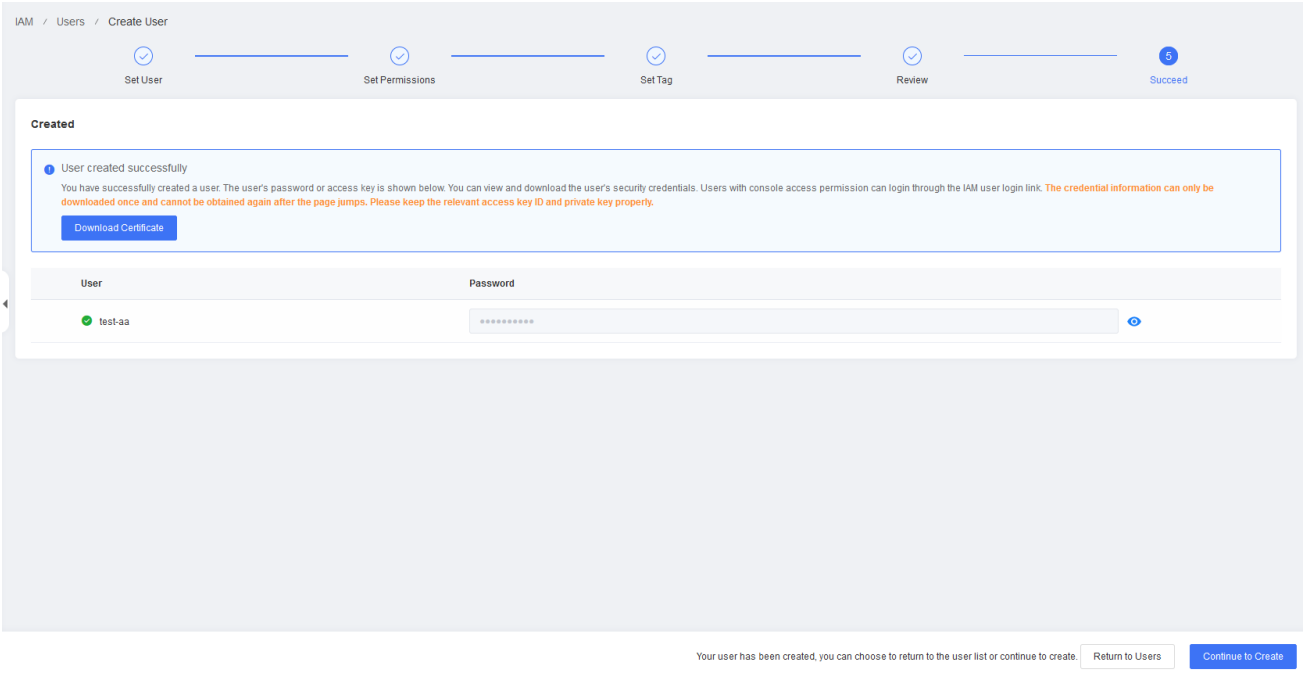
3. **`Set Tag`** (Optional): You can add tag keys and tag values for new IAM users. Each IAM user can add up to 10 tags.



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.



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



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

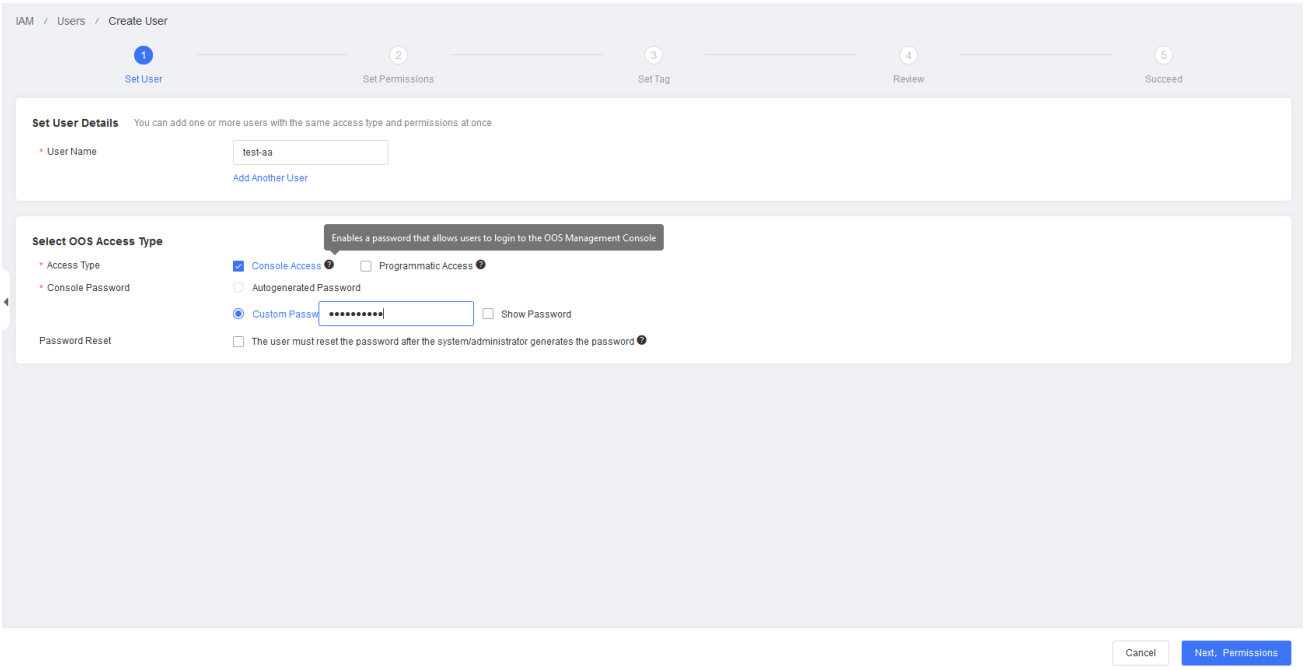
authorization can authorize IAM sub-users. After authorization, IAM users can operate on resources according to their permissions.

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.



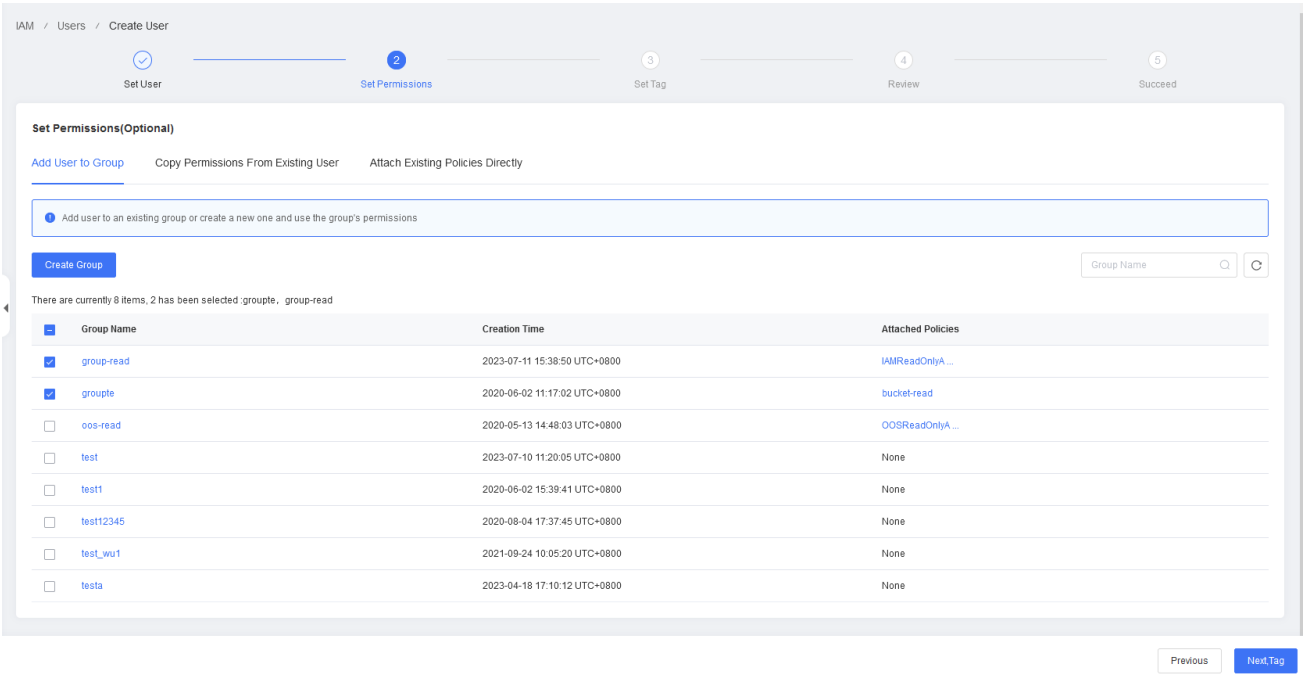
- **User Name**: The user name for logging in to OOS, the administrator (the root user or related IAM users with IAM authorization) can add 1-10 IAM users with the same access type and access permissions at a time. The user name must follow the following principles:
  - The name of the IAM user must 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**:
  - **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.

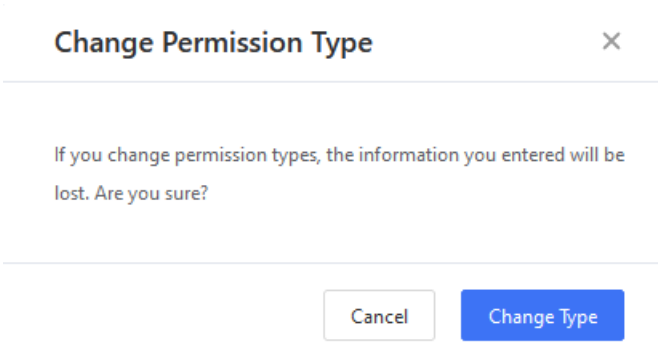
2. **Set Permissions**

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



- **`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.

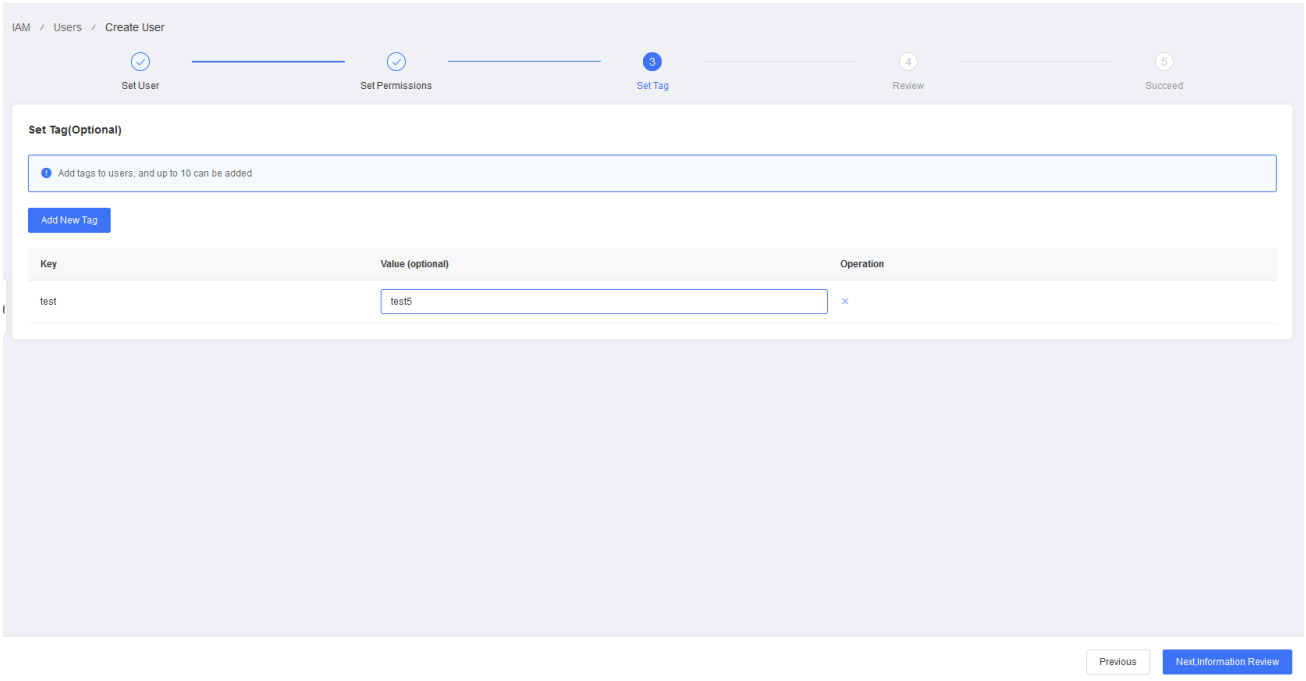


- **Cancel**: No permission type changes;
- **Change Type**: Confirm that the existing permission type is changed, and the existing permission information will not be retained after the change.

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.



A user can have up to 10 tags。

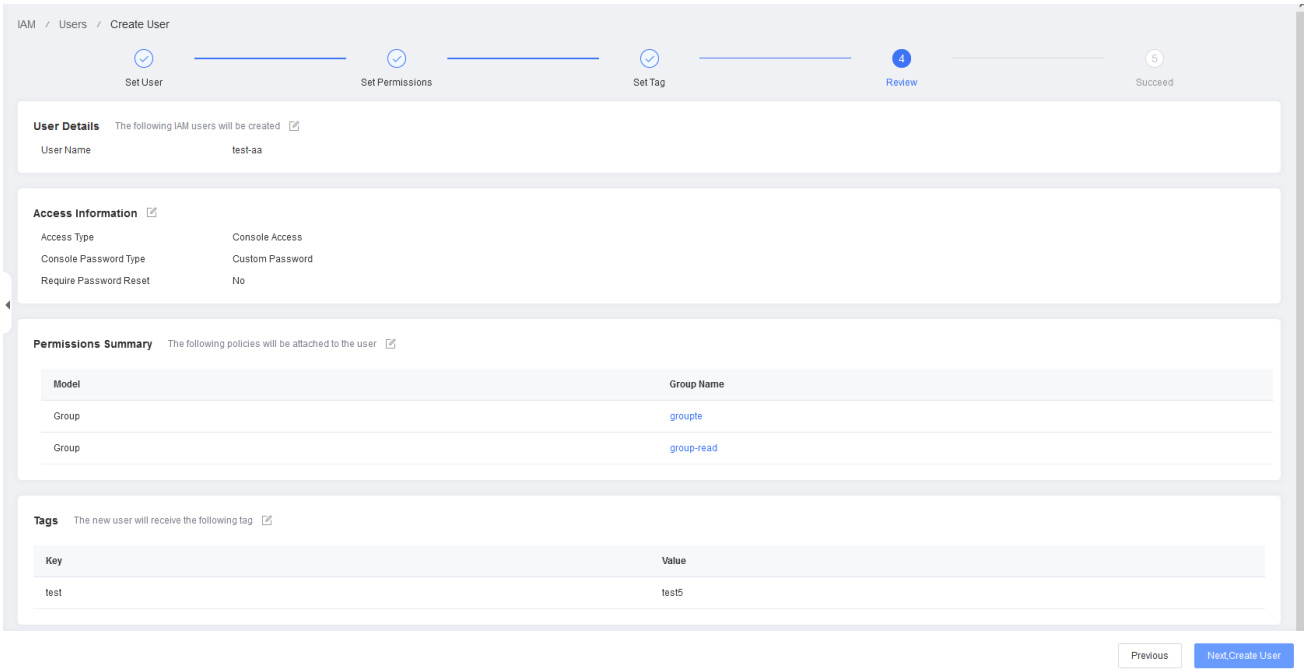
- **Key**: The value can include letters, digits, spaces, plus (+), equals (=), period (.), 'At' symbol (@), underscores (_), hyphens (-), colons (:), forward slash (/).

  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**

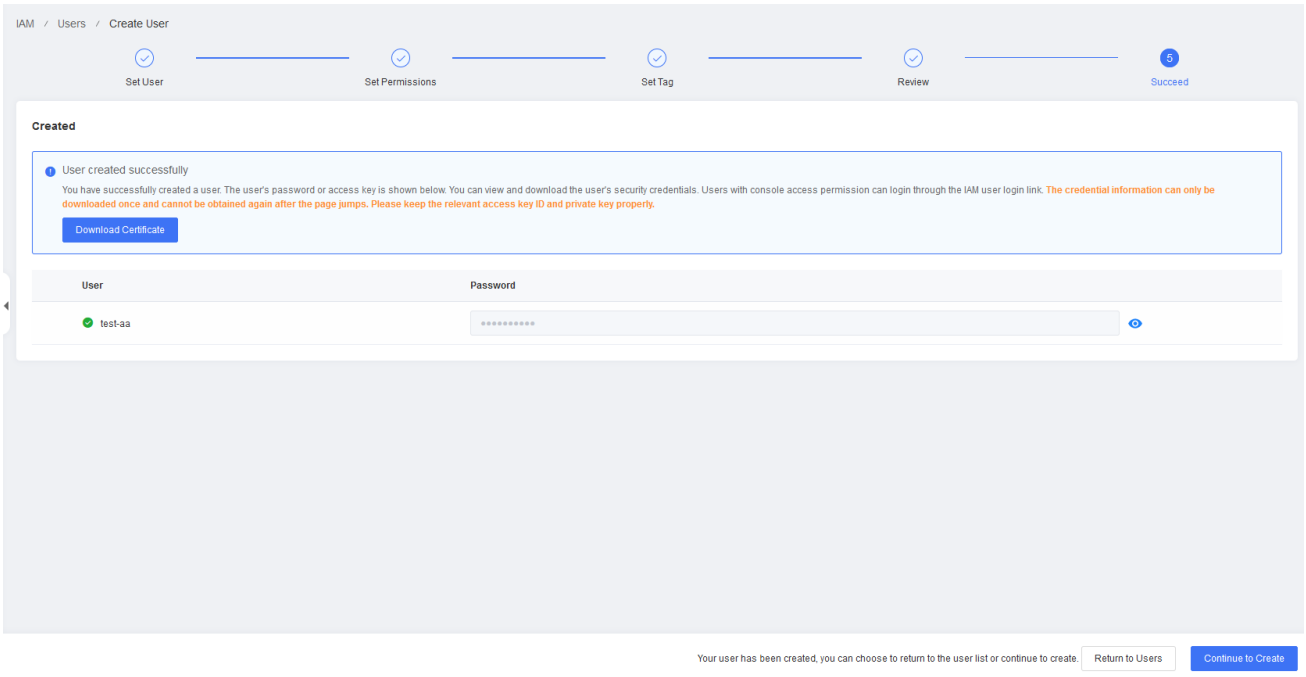
Review the information of the newly created user(s). If you need to change it, you can click the corresponding edit icon on this page, and then go to the corresponding page to make changes.



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.



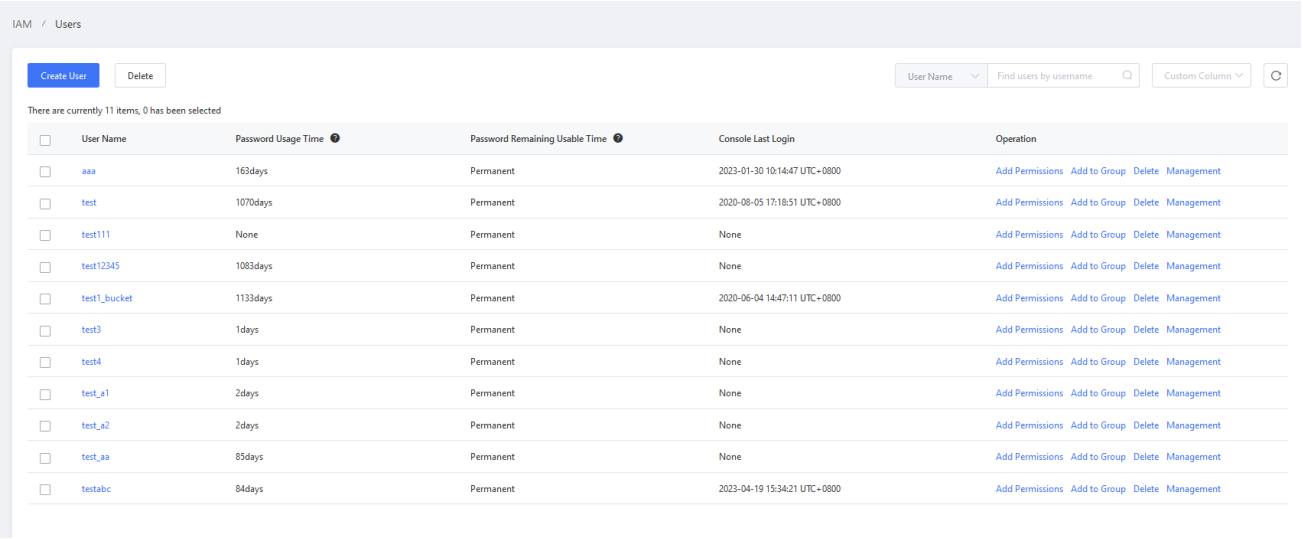
7.2.2 View and Modify the IAM User

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:

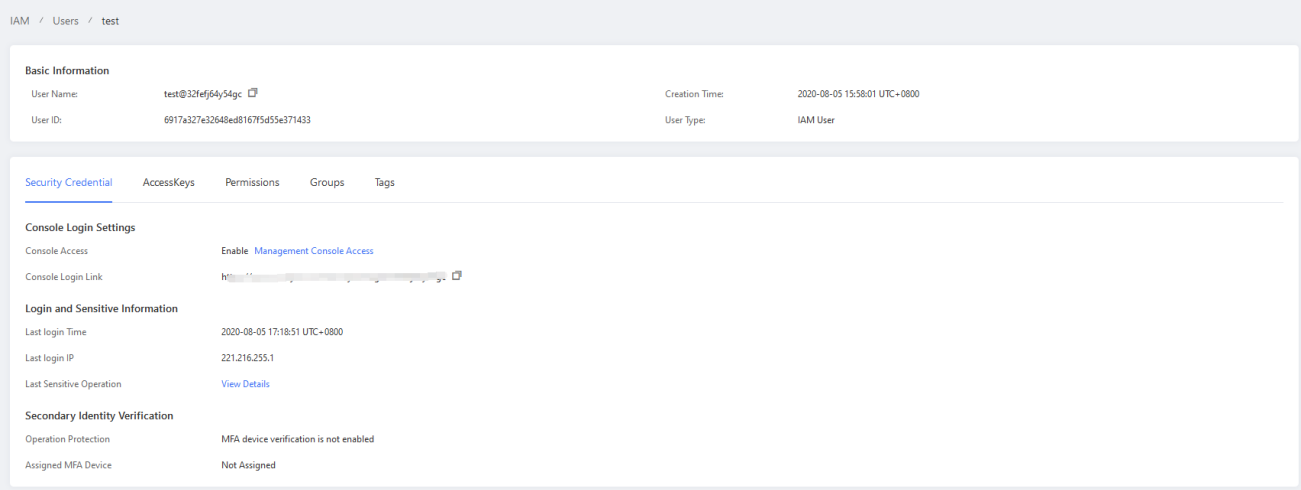
- **User Name**
- **Password Usage Time**
- **Password Remaining Usable Time**
- **Console Last Login**
- **User ID**
- **ARN**
- **MFA**
- **Programmatic Access**
- **Console Access**

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.



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 Time	The number of days since the password was created successfully. If there is no console access permission, **None** is displayed.
Password Remaining Usable Time	Password remaining time: ● If the user's password has no expiration time, it will be displayed as **Permanent**; ● 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 **0 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 Access	Whether to enable programmatic 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.

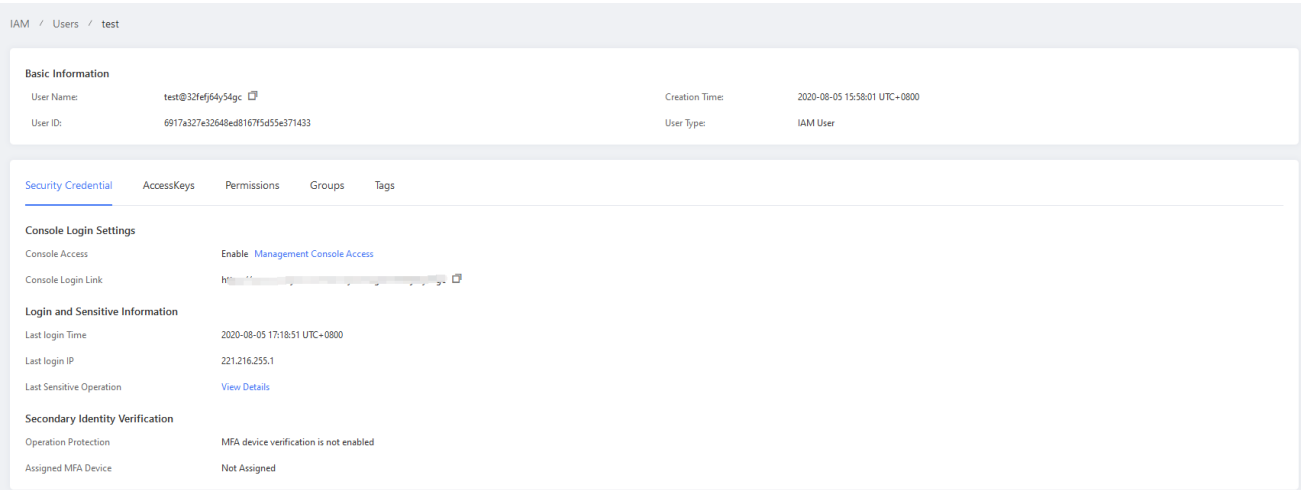


Basic Information Description

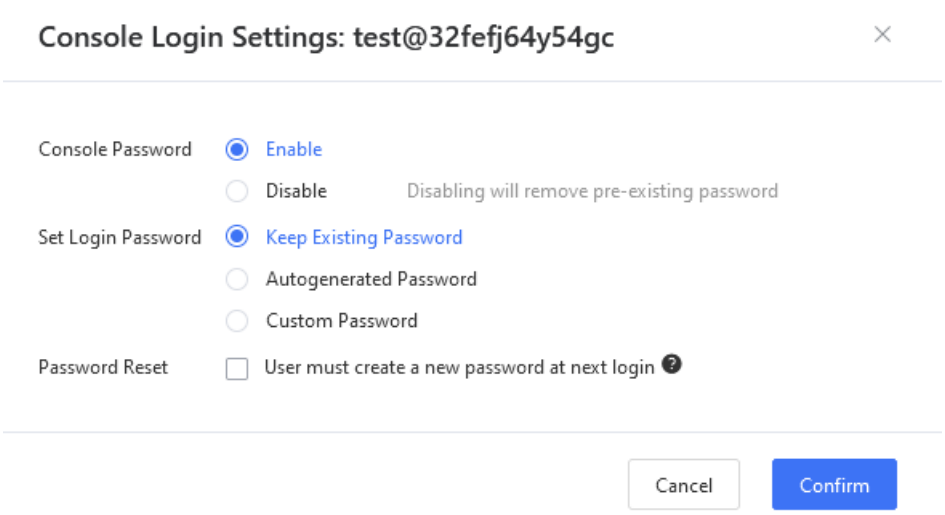
Item	Description
User Name	*<IAM user name>@<account ID>*. When the IAM user logs in, the user name is *<IAM user name>*.
Creation Time	The time when the IAM user was created.
User ID	IAM user ID.
User Type	User type: ● Root User ● IAM User

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`.



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



Console Login Settings description

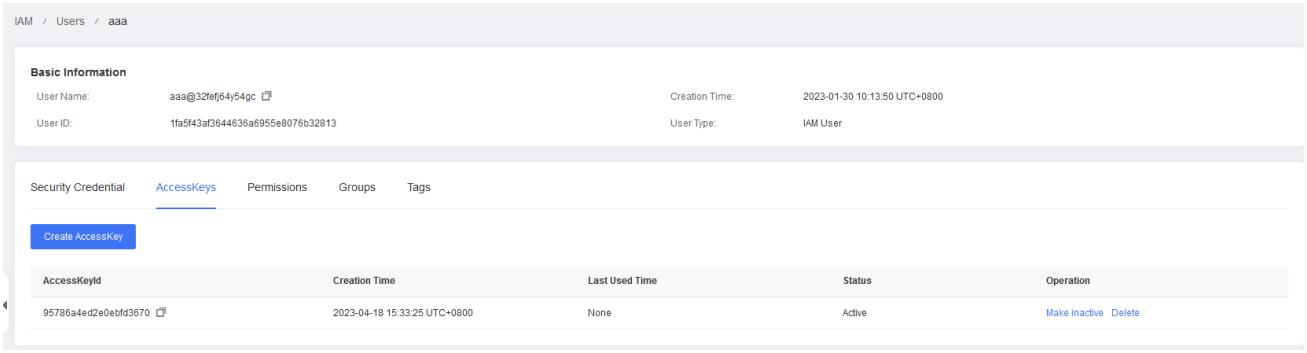
Item	Description
Console Password	Whether the console password login is enabled: ● **Enable**: Enable console password login. When there is no console login password, a new login password will be generated; ● **Disable**: Disable console password login and delete the current password.
Set Login Password	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; ● **Custom Password**: 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.

7.2.2.2 View and Modify AccessKeys

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

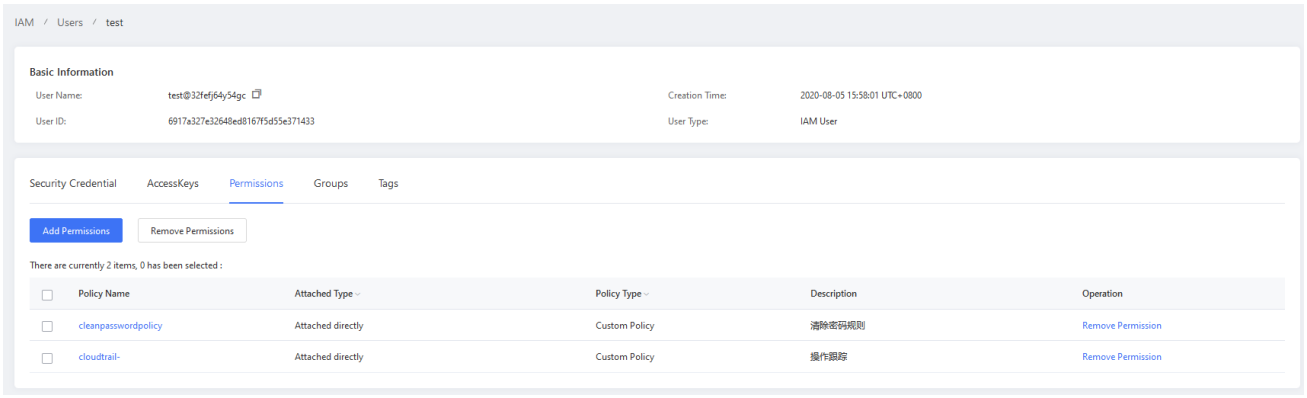
Note:

- 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.

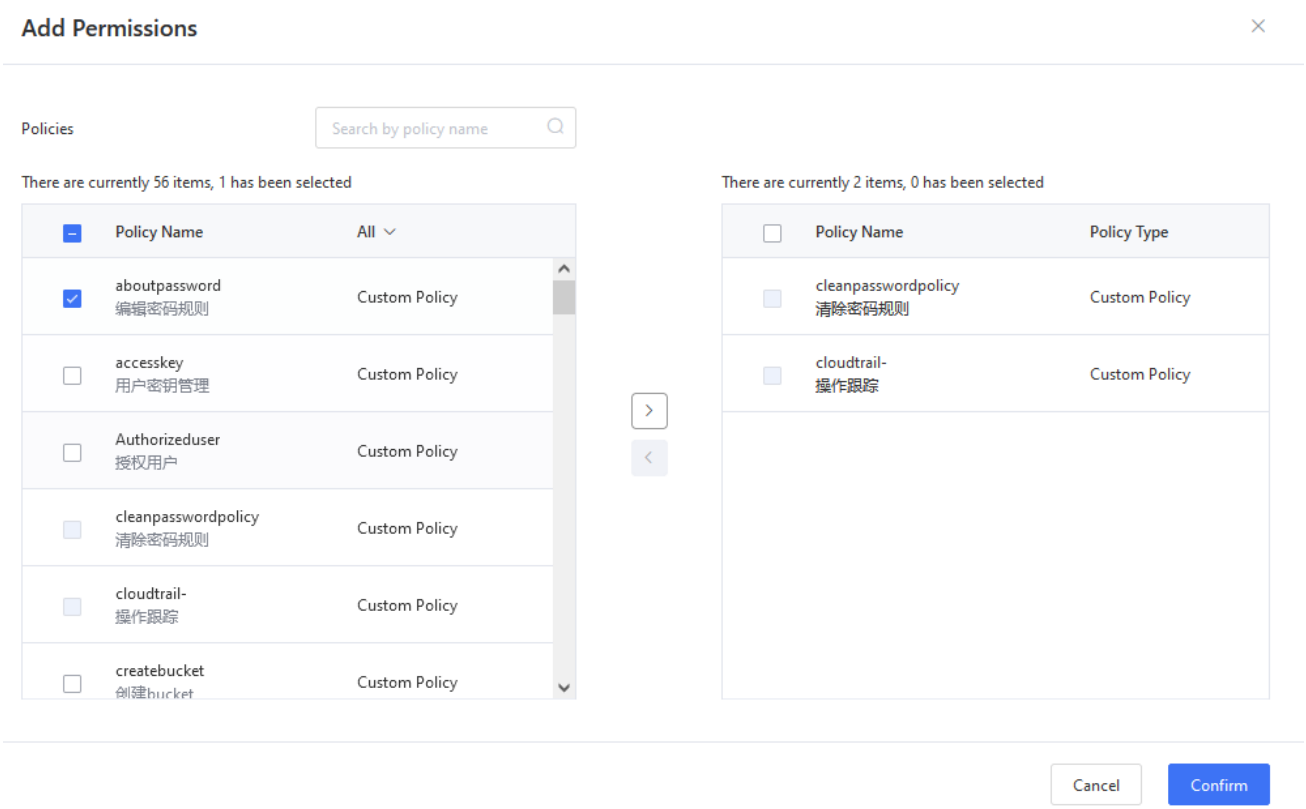


7.2.2.3 View and Modify Permissions

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.



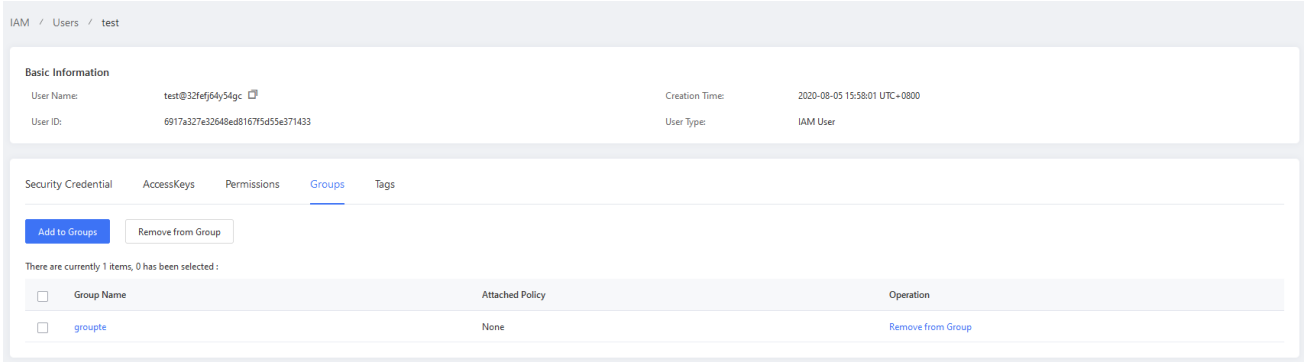
- Click **Add Permissions** to pop up the **Add Permissions** dialog box, you can associate a new policy for the user, and the gray policy in the dialog box indicates the policy that the user has associated.



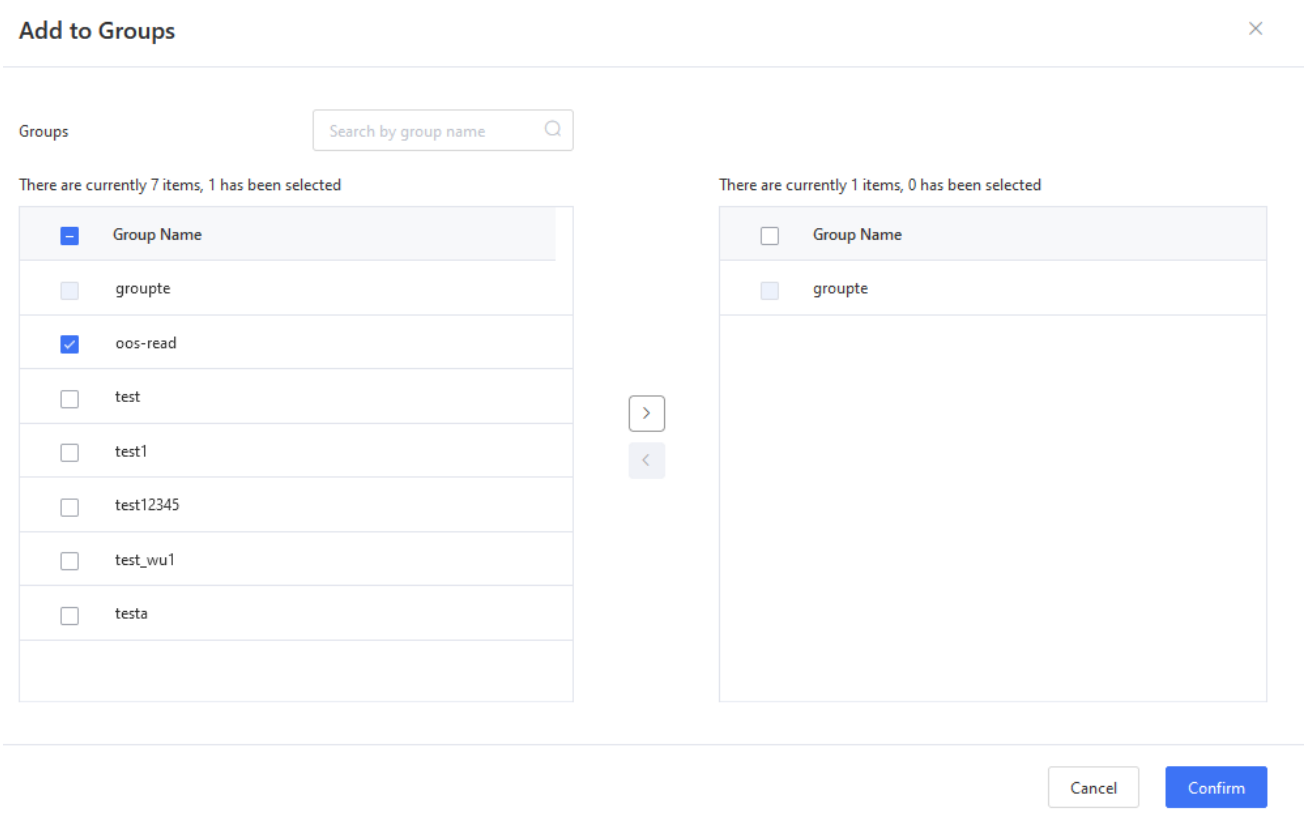
- Select policies that need to be removed, click **Remove Permissions** to delete multiple policies for the IAM user; click the **Remove Permission** to remove the associated policy; click **Remove from group**, the user will be removed from the corresponding group, and disconnect the policy associated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



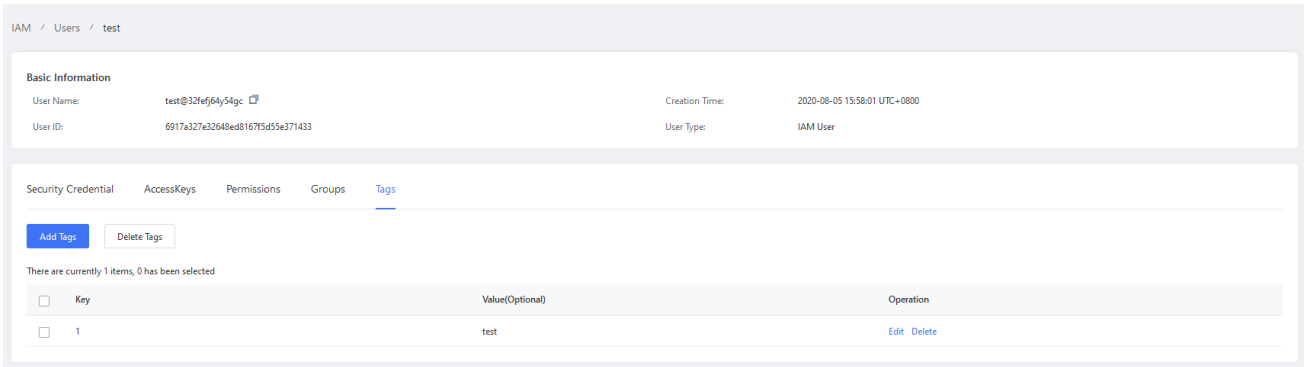
- Click **Add to Groups** to pop up the **Add to Groups** dialog box, you can select the group that the user needs to join, and click **Confirm**. The gray user group in the pop-up box indicates the user group that the user has joined.



- 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.



- **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

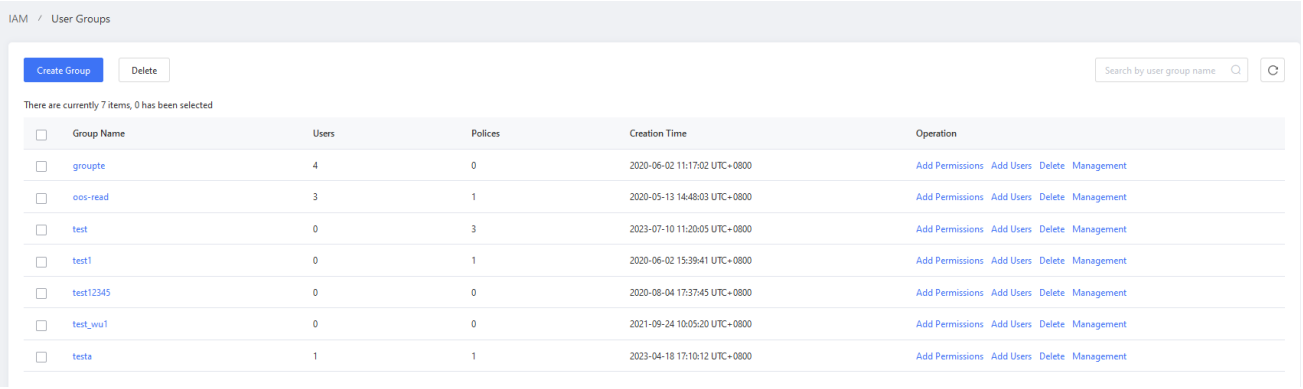
On the **Users** page, select IAM users to be deleted and click **Delete** to delete multiple IAM users; or click **Delete** behind the corresponding user to delete the IAM user.
When deleting a user, a dialog box will pop up to confirm whether to delete the selected user.

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

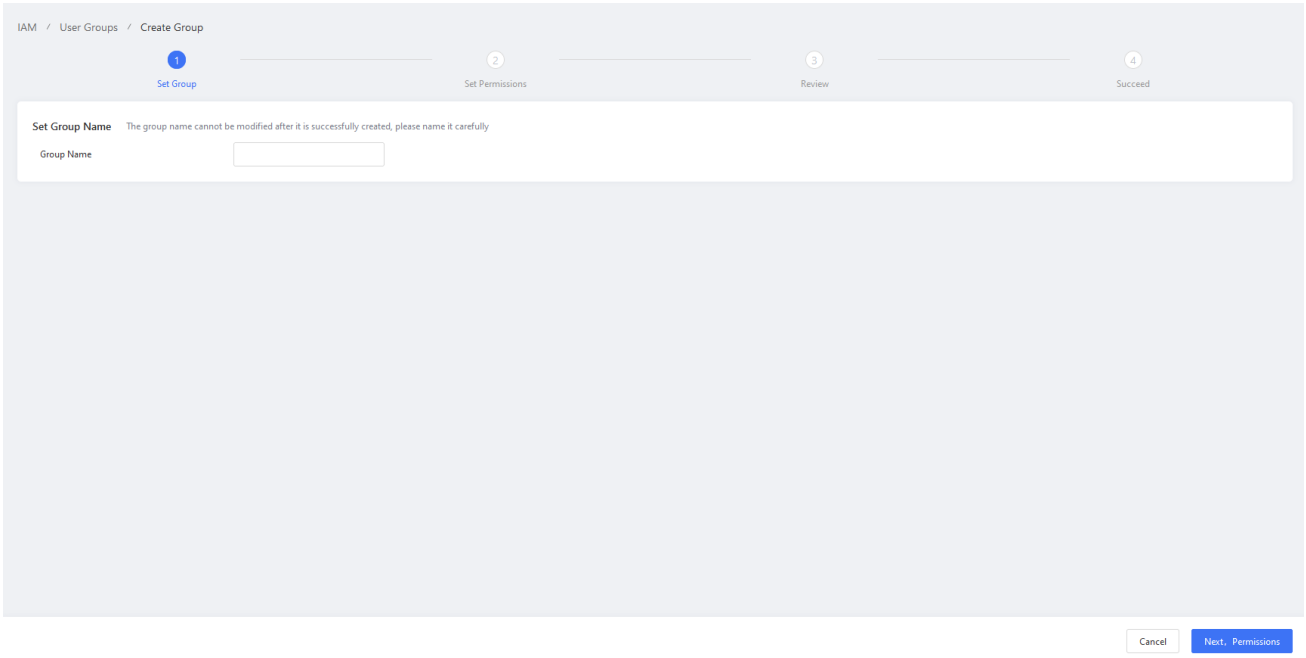
Administrators create user groups and authorize user groups. Users in the group can obtain the same authority policy, which is convenient for managing users.
Enter **Users Management** > **User Groups**, you can create a new user group, add permissions for the user group, delete user group, add IAM users for the user group, manage user groups.



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.

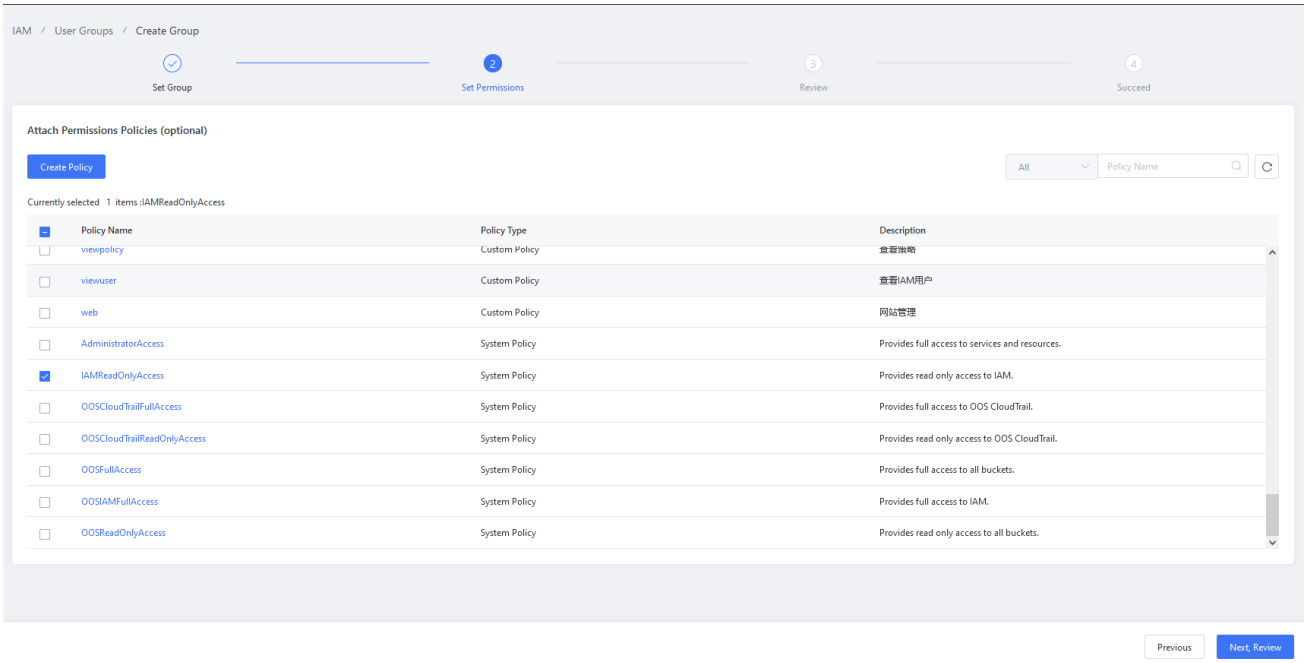
1. **Set Group**



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 (@).

2. Set Permissions

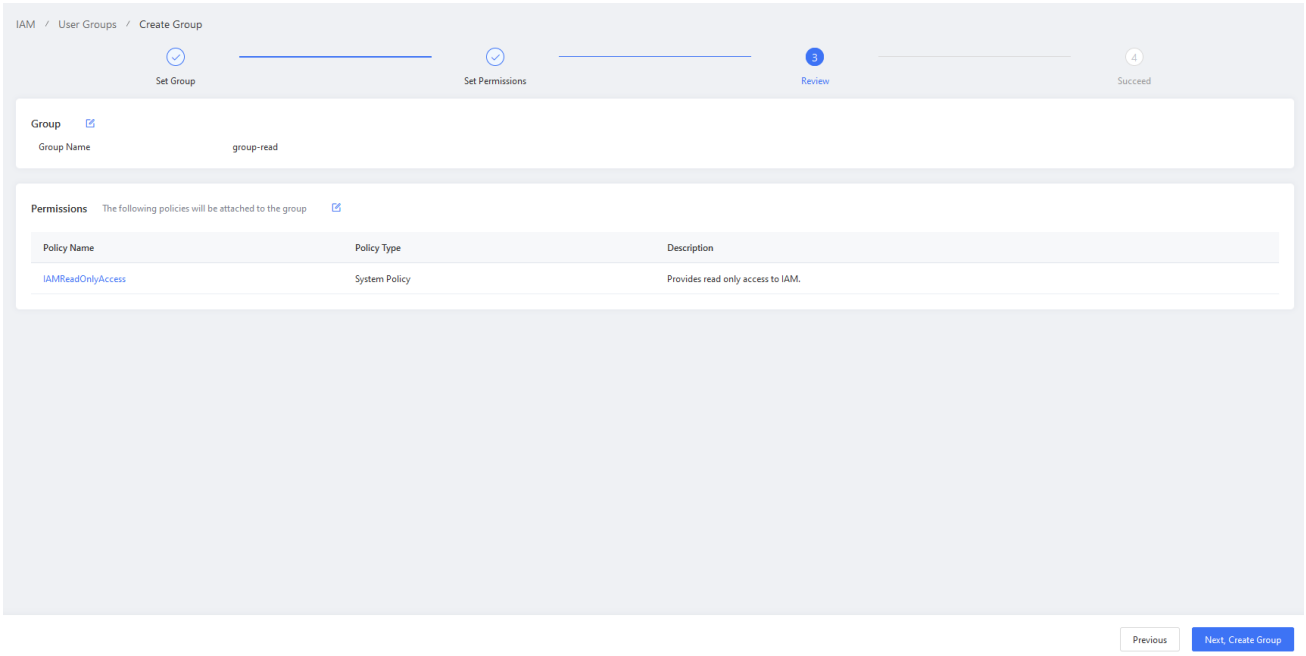


You can search for matching policies in the search box, and the searched matching policies are displayed in the form of a list. You can add policies to the user group by checking the corresponding policies.

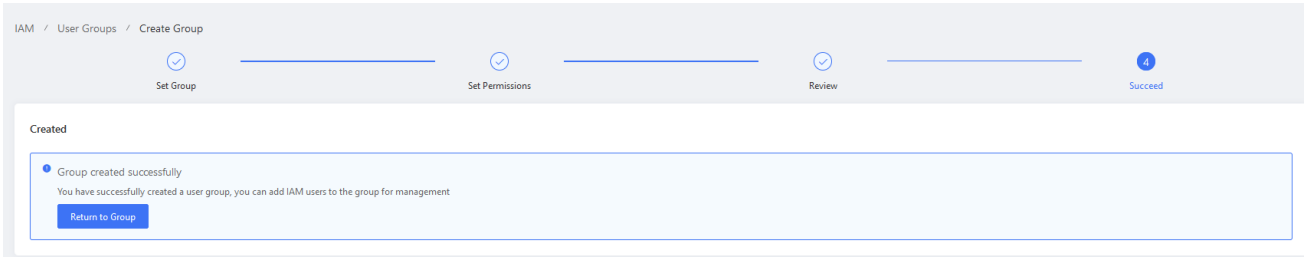
Note: You can add a policy to the user group when you create the user group, or you can add a policy to the user group after the user group is created. An IAM user can have up to 10 policies.

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.

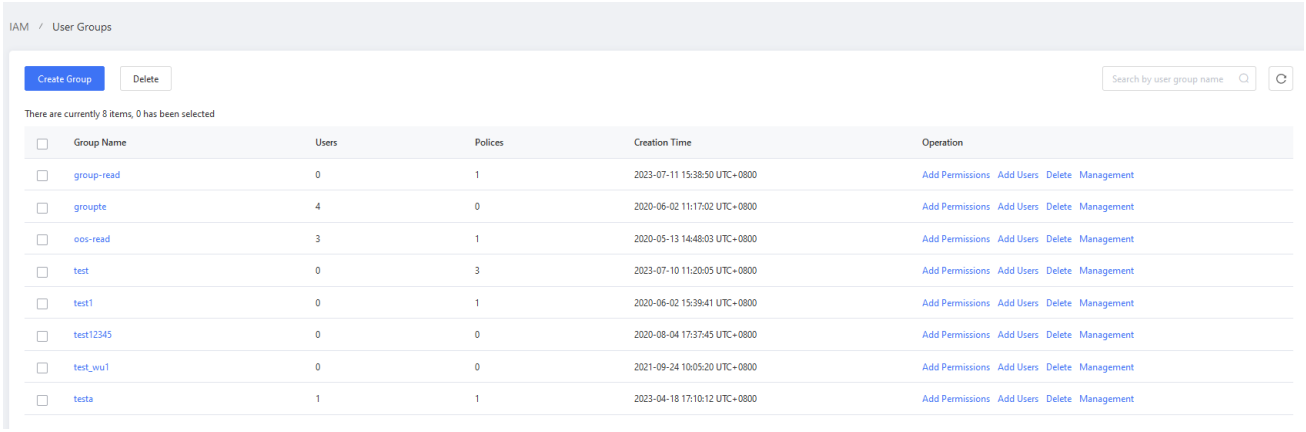


4. Succeed



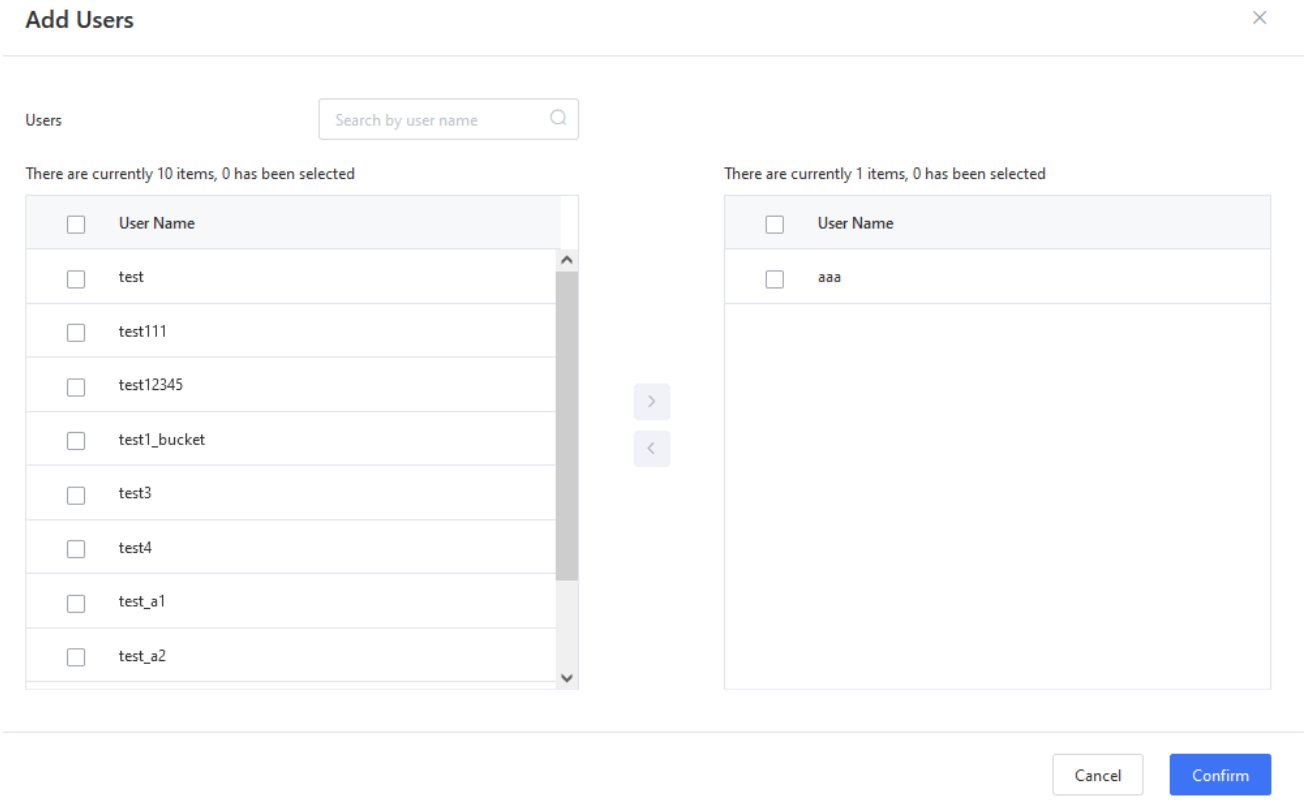
7.3.2 View and Modify the IAM User Group

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



7.3.2.1 Add or delete IAM users

- **Add IAM 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.

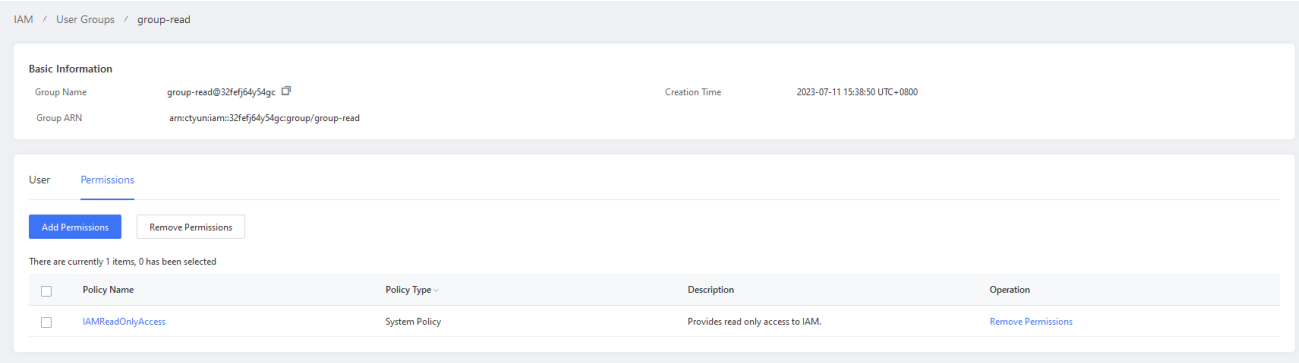


  - Click the corresponding user group name or **Management** to enter the user group details page, and click **User** > **Add User** to add users to the user group.

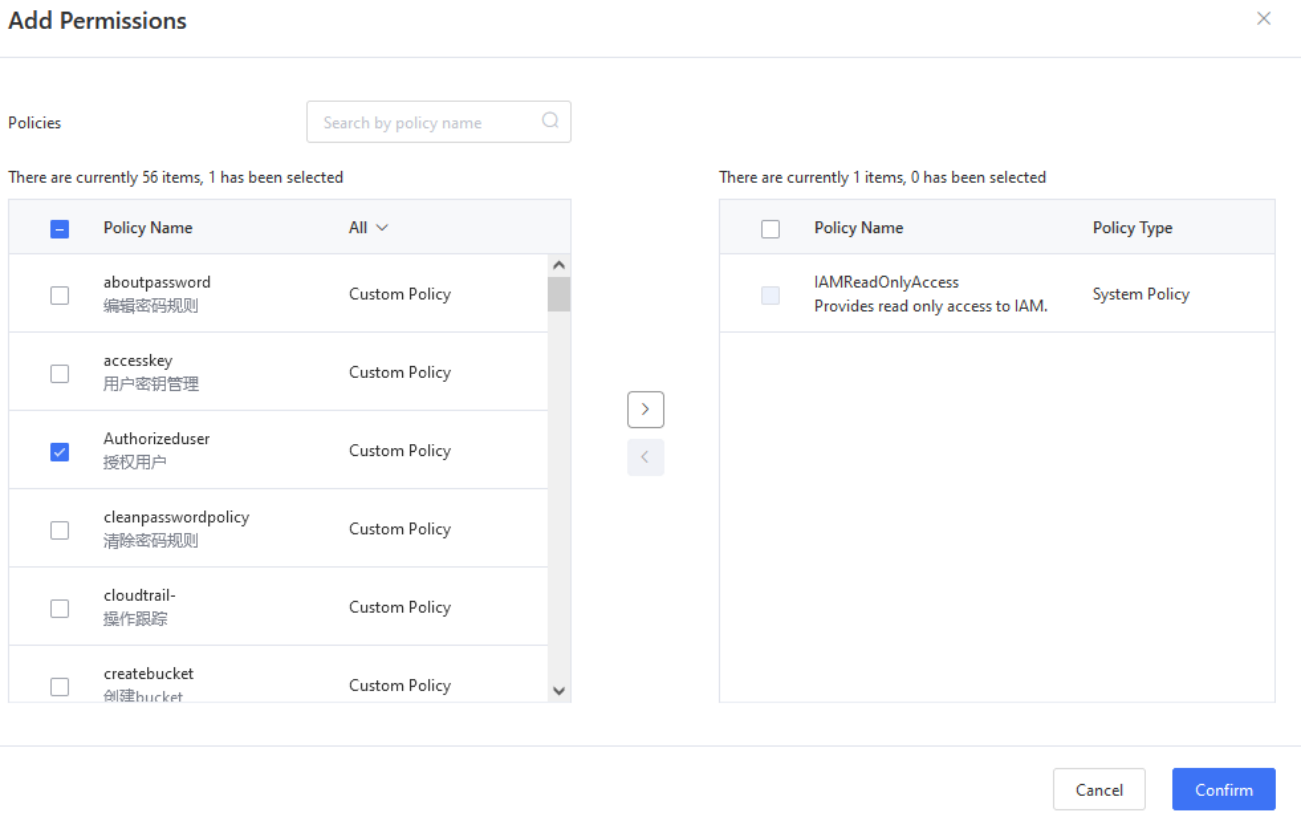
- **Remove IAM users**

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



- **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.



  - 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

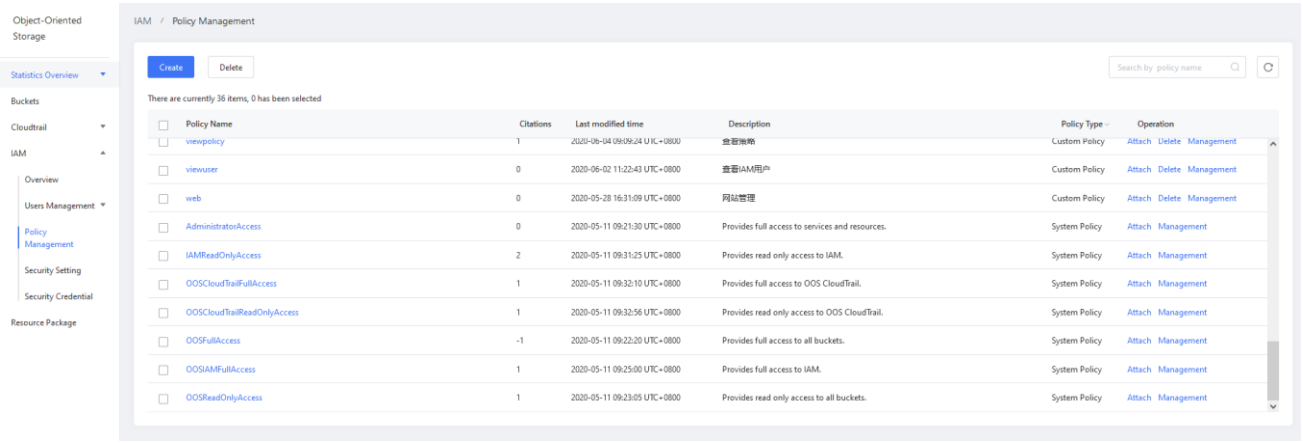
On the **User Groups** page, select user groups to be deleted and click **Delete** to delete multiple user groups; or click **Delete** behind the corresponding user group to delete the user group.

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.



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:

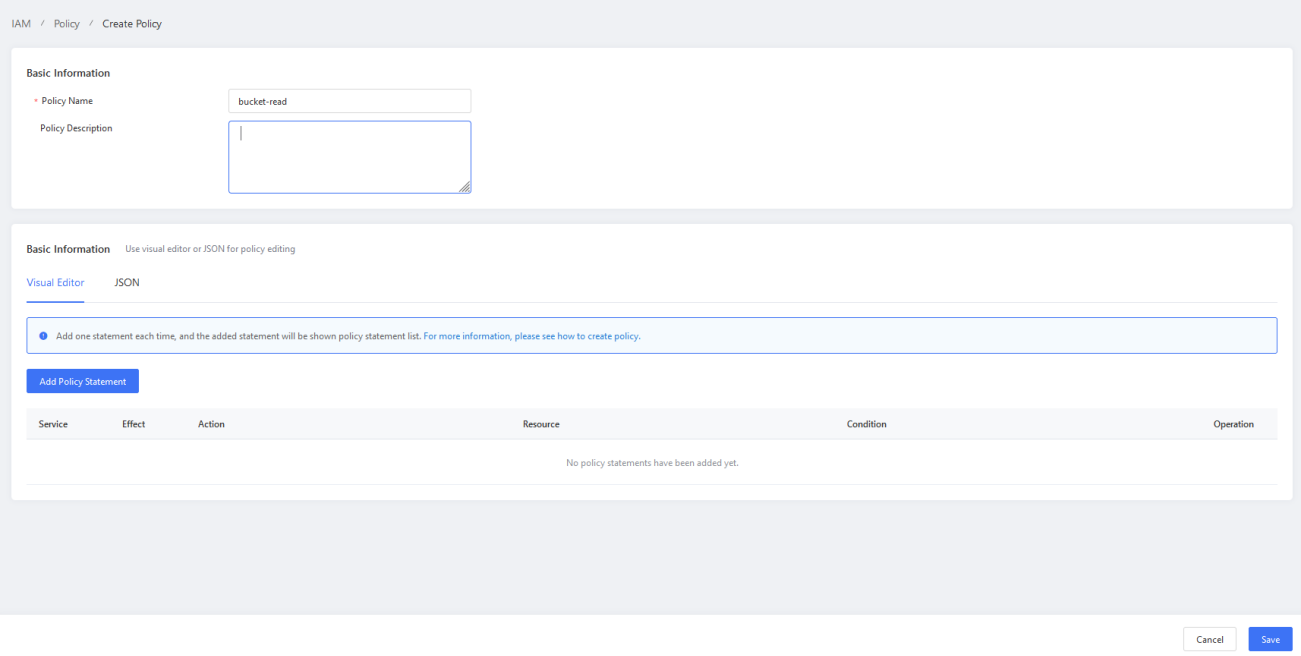
	GetTrailStatus, 、 DescribeTrails, LookupEvents, GetEventSelectors, GetObject, GetService.。
OOSFullAccess	All permissions of OOS, including all operations of Bucket and Object.
OOSIAMFullAccess	All permissions of IAM.
OOSReadOnlyAccess	OOS related read permissions, including Bucket and Object GET and 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.

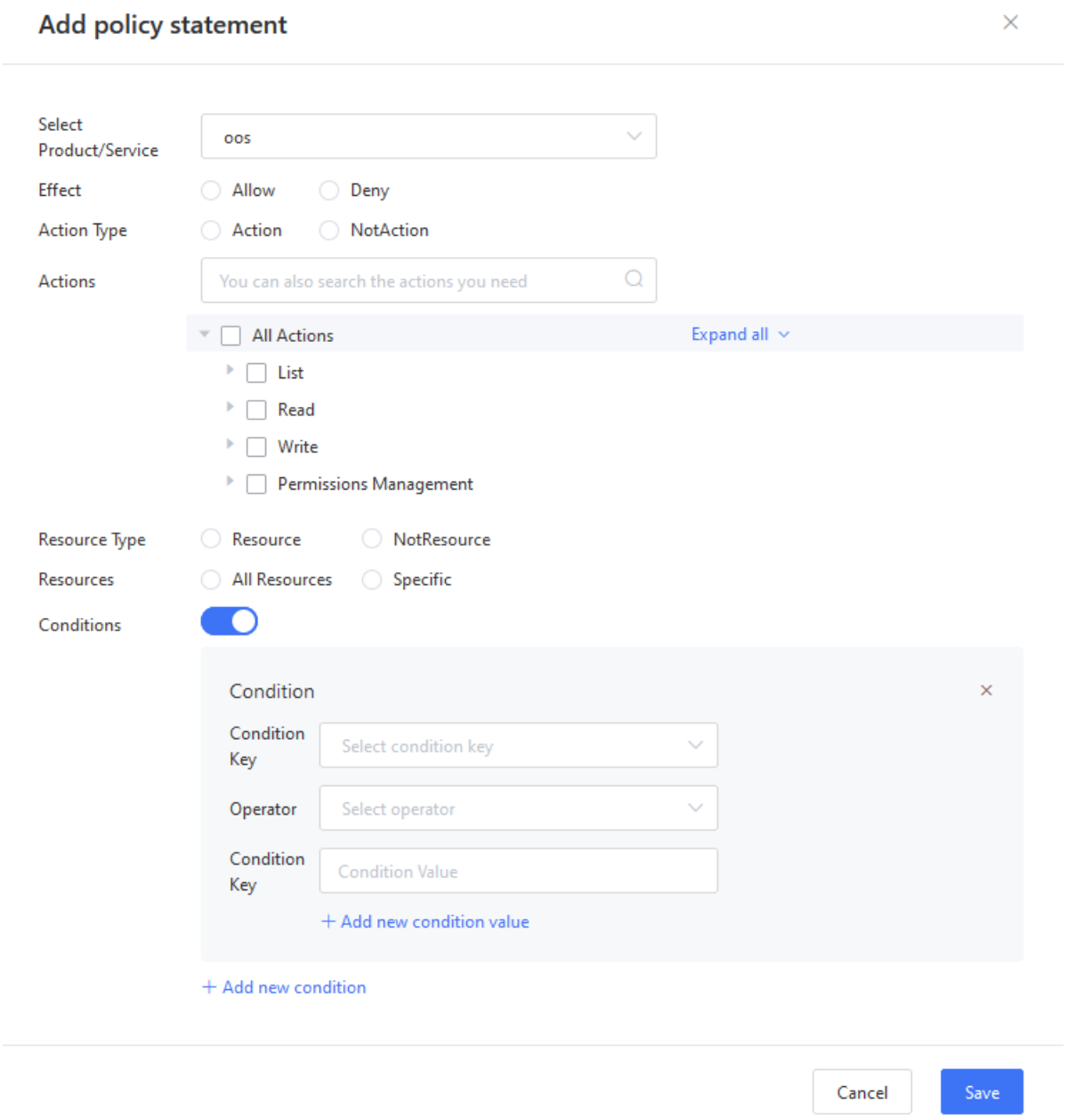
Note: For specific resources and APIs corresponding to each Action, please refer to **Action List and Corresponding API**.



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.



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

	● Deny: According to the selected operation category, the performance of the selected operation effect is denied.
Action Type	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. **Action Type**: ● Action: Match the specified operation. ● NotAction: The policy element that matches the operation other than the specified operation. When using NotAction: ■ If Allow effects are used, all applicable operations or services not listed are permitted; ■ If the Deny effect is used, such unlisted operations or services will be denied.
Actions	You can select the policy that needs to be implemented for the operation in the action list. See the **Action List** for the policies contained in each service.
Resource Type	The resource is the entity on which the policy takes effect: ● Resource: The resource for which the policy takes effect. ● NotResource: For resources other than the specified resource, the policy takes effect.
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 (optional)	The conditions under which the user policy takes effect. **Note**: 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: ● ListBucket ● ListAllMyBucket ● GetRegions
	Read: ● ListBucketMultipartUploads ● GetBucketAcl ● GetBucketLocation ● GetBucketPolicy ● GetLifecycleConfiguration ● GetBucketWebsite ● GetBucketCORS ● GetBucketLogging ● GetObject

	• ListMultipartUploadParts • GetBucketInventoryConfiguration
	Write: • DeleteBucket • PutLifecycleConfiguration • PutBucketWebsite • DeleteBucketWebsite • PutBucketCORS • PutBucketLogging • PutObject • DeleteObject • DeleteMultipleObjects • AbortMultipartUpload • PutBucket • PutBucketInventoryConfiguration
	Permissions Management: • PutBucketPolicy • DeleteBucketPolicy
cloudtrail	List • DescribeTrails • LookupEvents
	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
	Read: • GetUser • GetGroup • GetPolicy • GetAccountPasswordPolicy • GetAccountLoginSecurityPolicy
	Write: • CreateAccessKey • DeleteAccessKey • UpdateAccessKey • GetSessionToken • CreateUser • DeleteUser • TagUser • UntagUser • CreateGroup • DeleteGroup • AddUserToGroup • RemoveUserFromGroup • ChangePassword • UpdateAccountPasswordPolicy • DeleteAccountPasswordPolicy • UpdateAccountLoginSecurityPolicy • DeleteAccountLoginSecurityPolicy • CreateVirtualMFADevice • DeleteVirtualMFADevice • EnableMFADevice • DeactivateMFADevice • CreateLoginProfile • DeleteLoginProfile • UpdateLoginProfile
	Permissions Management:

	• CreatePolicy • DeletePolicy • AttachUserPolicy • DetachUserPolicy • AttachGroupPolicy • DetachGroupPolicy

Condition description

Condition Keys	Condition Operators	Condition Values
ctyun:CurrentTime	• DateEquals: Match the specified date. • DateNotEquals: Not equal to the specified date. • DateLessThan: Before the specified date. • DateLessThanEquals: Before or equal to the specified date. • DateGreaterThan: Later the specified date. • DateGreaterThanEquals: Later or equal to the specified date.	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:SourceIp	• IpAddress: Match the specified IP address or IP range. • NotIpAddress: Match all IP addresses except the specified IP address or IP range.	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	• StringEquals: Matches exactly the specified value and is case sensitive. • StringNotEquals: Does not match the specified value and is case sensitive. • 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-	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 (*) 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 specified value and is case sensitive. ● StringNotEquals: Does not match the specified value and is case sensitive. ● 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.	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 (@). Note: The condition operators for StringLike and StringNotLike can include wildcard characters.
ctyun:UserAgent	● StringEquals: Matches exactly the specified value and is case sensitive. ● StringNotEquals: Does not match the specified value and is case sensitive. ● 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.	A string that can contain special characters.
ctyun:Referer	● StringEquals: Matches exactly the specified	A string that can contain special characters.

	value and is case sensitive. ● `StringNotEquals`: Does not match the specified value and is case sensitive. ● `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.	
ctyun:SecureTransport	`Bool`: Boolean match.	● `true` ● `false`
ctyun:MultiFactorAuthPresent	`Bool`: Boolean match. **Note**: Only IAM service supports this condition operator.	● `true` ● `false`
ctyun:MultiFactorAuthAge	● `NumericEquals`: Match the specified value. ● `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.	An integer.
oos:prefix	● `StringEquals`: Matches exactly the specified value and is case sensitive. ● `StringNotEquals`: Does not match the specified value and is case sensitive. ● `StringEqualsIgnoreCase`: Matches exactly the specified value and is not case sensitive.	The value is a string. **Note**: The condition key is only valid for the operation authority of **oos:ListBucket**.

	• `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 value and is case sensitive. • `StringNotEquals`: Does not match the specified value and is case sensitive. • `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 (?).	The value is a string. The value: • `private`: only the owner can operate the bucket. • `public-read`: all can read the bucket. • `public-read-write`: all can operate the bucket, including read and write operations. **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`.

- 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
Statement: Policy authorization statement. There can be multiple Statements, representing different authorization structures.	Effect	Effect on selection operation.	● Allow: Allow execution. ● Deny: Deny execution. **Note**: When the Effect in the same Action contains both Allow and Deny, the Deny priority principle is followed.
	● Action: Match the specified operation. ● NotAction: The policy element that matches the operation other than the specified operation. **Note**: For a Statement, choose one of Action and	Action type.	The format is as follows: ● Service: ● oos; ● cloudtrail; ● statistics; ● iam. ● **Actions**: For details, see **Action List**.

	NotAction.		
	• Resource：The resource for which the policy takes effect. • NotResource: For resources other than the specified resource, the policy takes effect.	Resource type.	The format can be: • arn:ctyun:*service*::*accountid*:*resource* • arn:ctyun:*service*::*accountid*:*resourcetype/resource* **Note**: • *service*: Service name. • *accountid*: Account ID. • *Resource*: Specific resources. 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::*accountID*:*bucket/object*, where *bucket* and *object* are the actual resource names of the user. • *Resourcetype*: Resource Type. The wildcard * represents all resource types. Different services have different corresponding resourcetypes: ▪ The resource type of iam can be: *user*, *group*, *policy*, *mfa* or *; ▪ The resource type of cloudtrail can be: *trail* or *; ▪ The resource of statistic can be *.
	Condition	The conditions under which the user policy takes effect.	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**: 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.

- **…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.

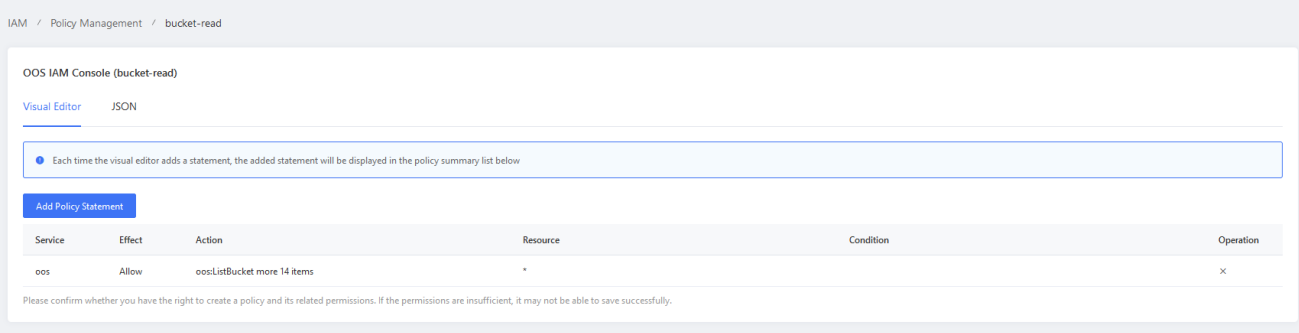
```
"Effect" : "Allow",
"Condition" : { " NumericLessThanEqualsIfExists" : { "ctyun:MultiFactorAuthAge " :
1800 } }
```

- 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 } }
```

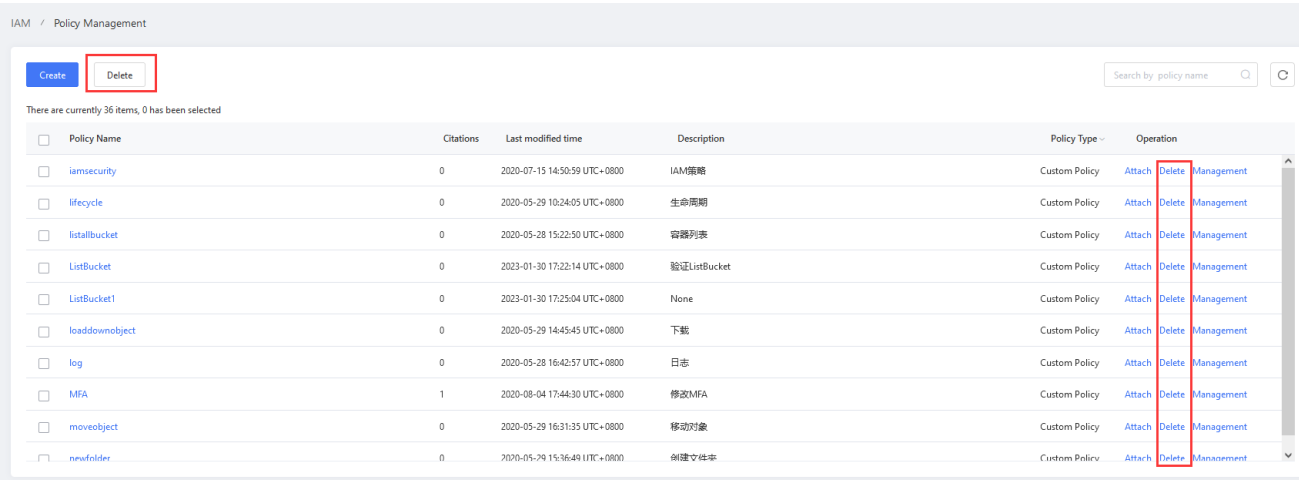
7.4.2.2 Modify the Custom Policy

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**.



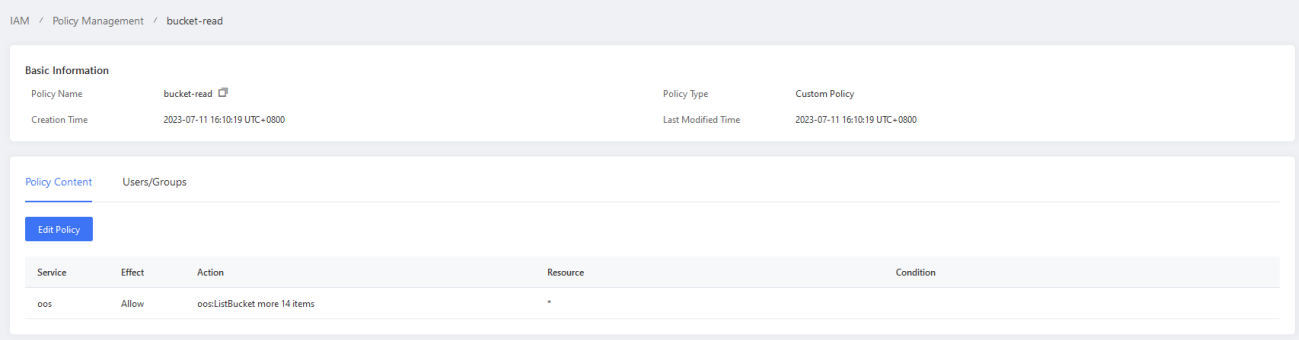
7.4.2.3 Delete the Custom Policy

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.



7.4.3 View the Policy Basic Informaion

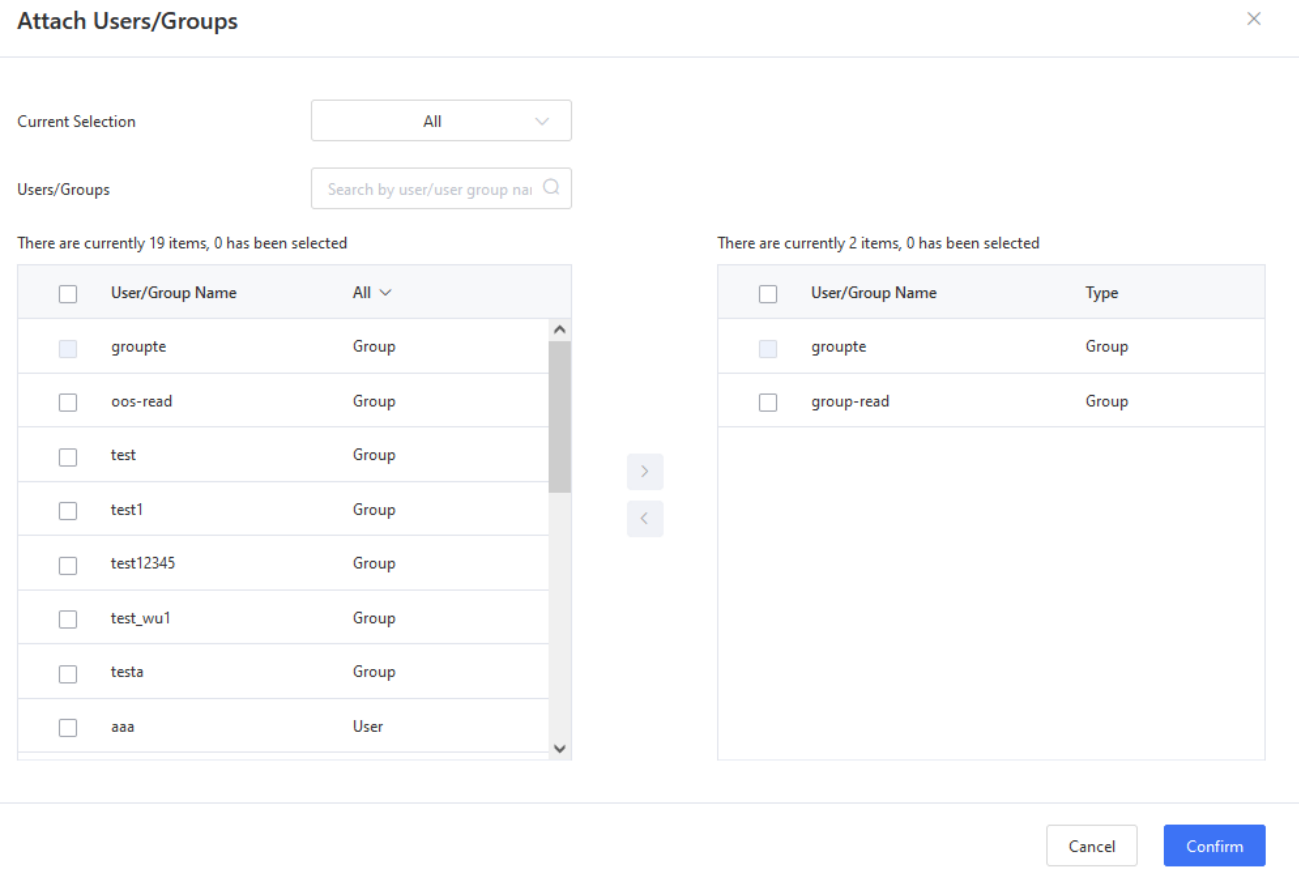
Enter **IAM** > **Policy Management**, click the corresponding policy name or **Management**, enter the policy details page. On this page, you can view the policy basic information and modify the policy.
The basic information including `Policy Name`, `Policy Type`, `Creation Time`, `Last Modified Time` and `Description`.



7.4.4 Attach Policy

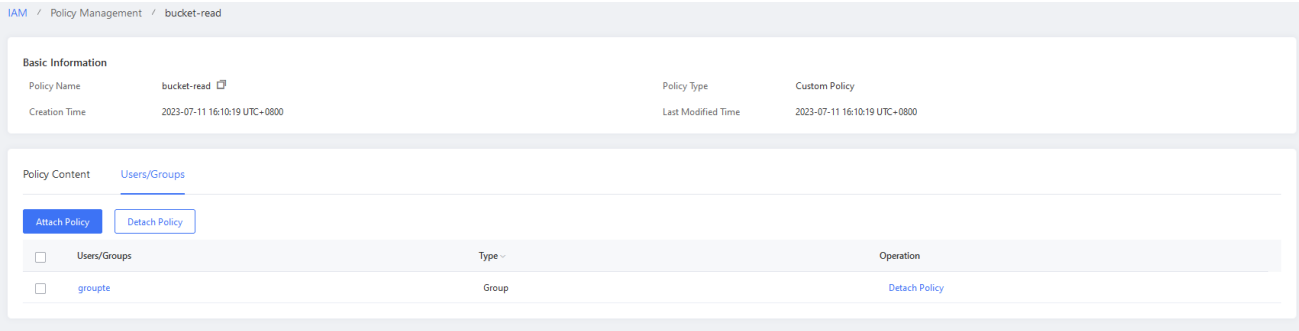
- **Attach Policy**

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.



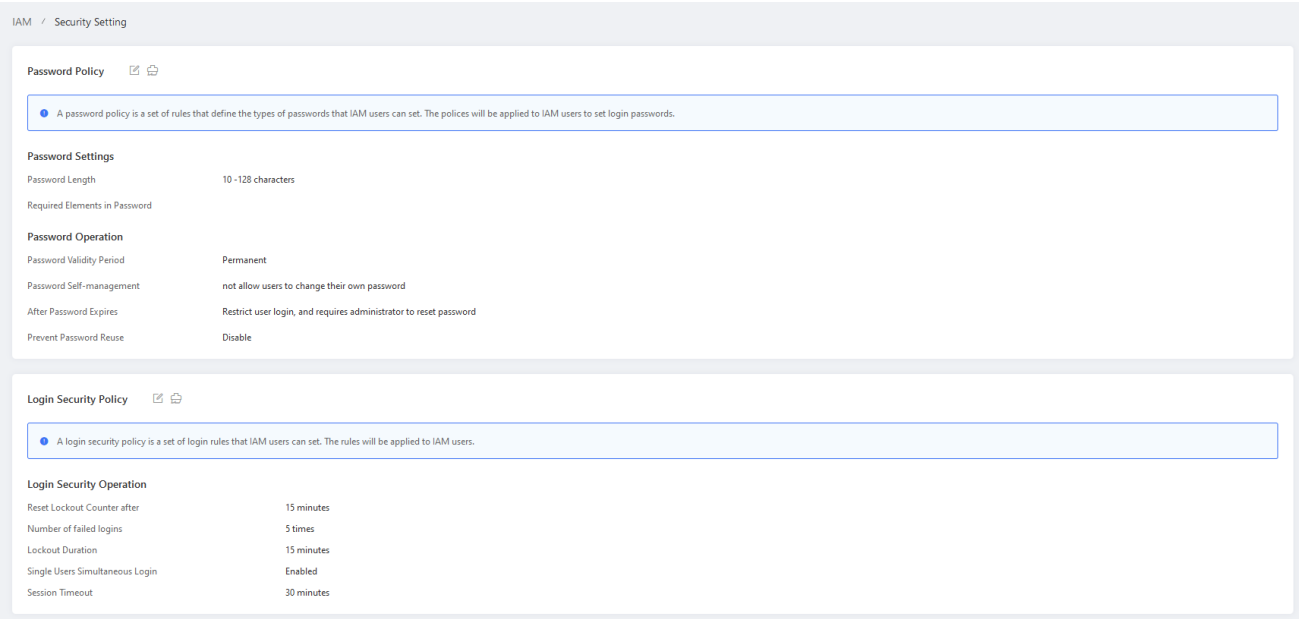
- **View attached users/groups**

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.



7.5 Security Setting

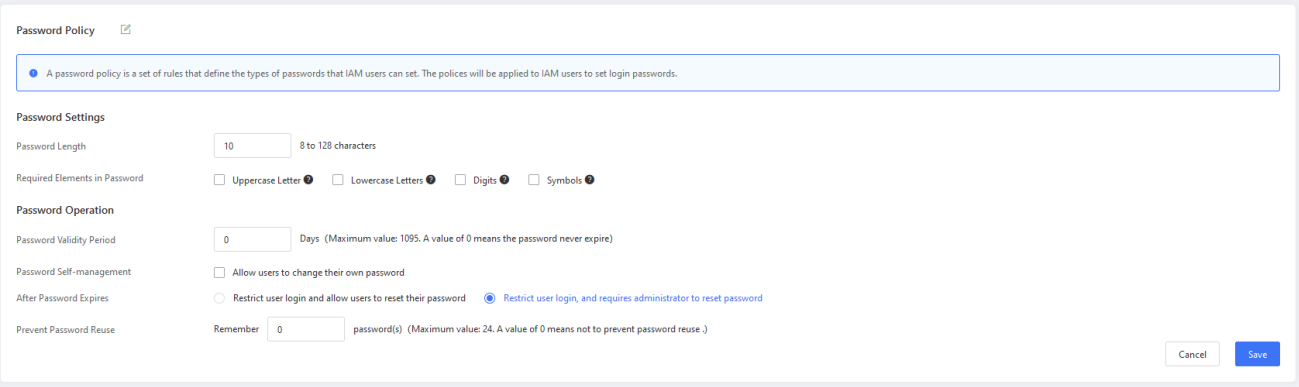
Click **IAM** > **Security Setting**, you can set password policy and login security policy.



7.5.1 Password Policy

7.5.1.1 Edit Password Policy

Click **Edit Password Policy** to reset the password policy.



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 Password	You can select any one or more of the following: ● `Uppercase Letters`: A~Z; ● `Lowercase Letters`: a~z; ● `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-management	● Allow users to change their own password. ● If this item is not checked, only the administrator can change the password.
After Password Expires	● Restrict user login and allow users to reset their password; ● Restrict user login, and requires administor 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 **`Prevent Password Reuse`** 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 password	Do not allow users to change their own password
Restrict user login and allow users to reset their password	At any time, IAM users can change their passwords by themselves.	Only after the password expires, the IAM user is allowed to change the password once.
Restrict user login, and requires administor to reset password	At any time, the IAM user cannot modify the password through the console, but can be modified through the API.	IAM users cannot change their passwords by themselves at any time.

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:

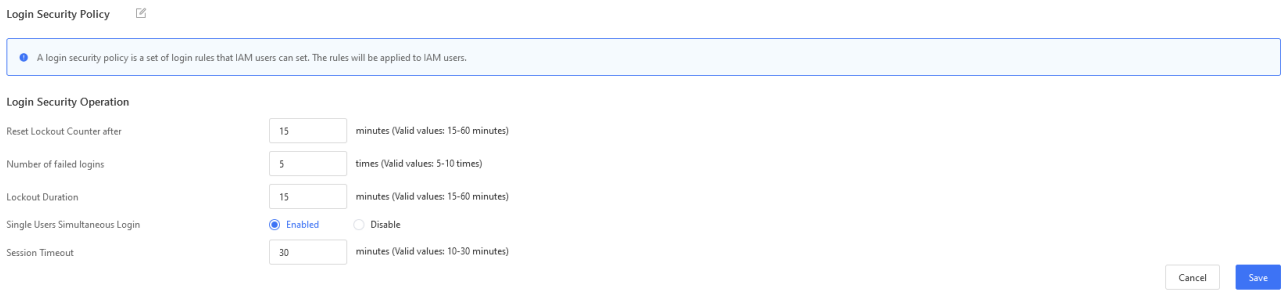
- **`Password Length`**: 8 – 128 characters.
- **`Required Elements in Password`**: Lowercase Letters, Digits.
- **`Password Validity Period`**: Permanent.
- **`Password Self-management`**: Allow users to change their owner password.
- **`After Password Expires`**: Restrict user login and allow users 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.



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:

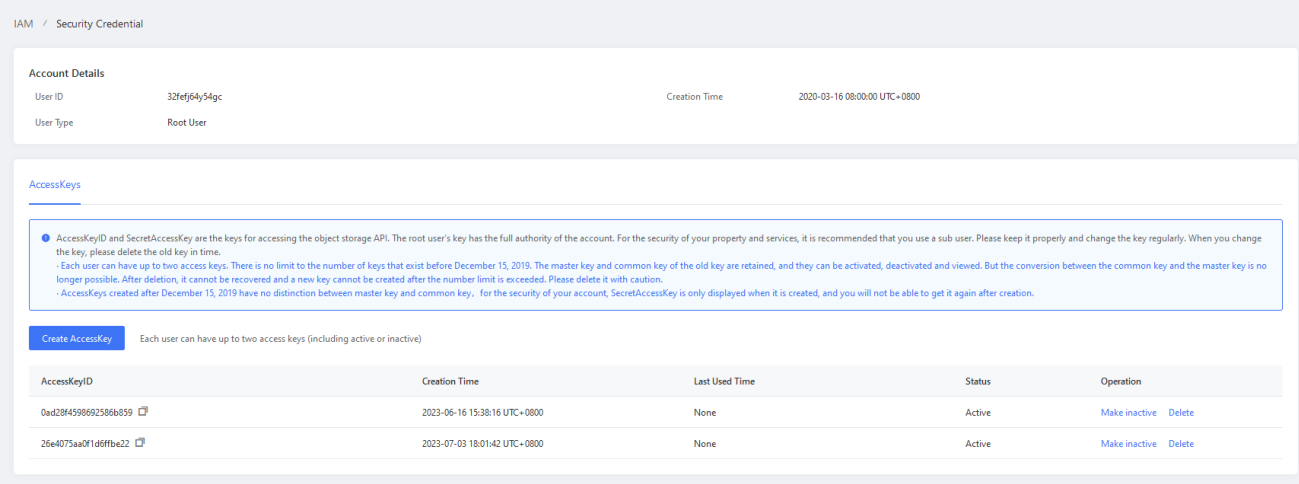
- **`Reset Lockout Counter after`**: 15 minutes.
- **`Number of failed logins`**: 5.
- **`Lockout Duration`**: 15 minutes.
- **`Single Users Simultaneous Login`**: Enabled.
- **`Reset Lockout Counter after`**: 30 minutes.

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.

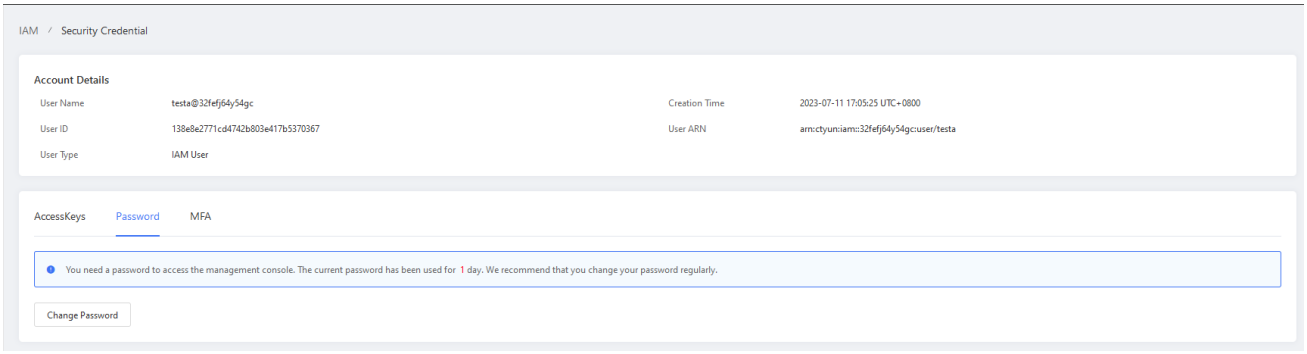


AccessKeys Description

Item	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.
Type	● `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` ● `Make active` ● `Delete`

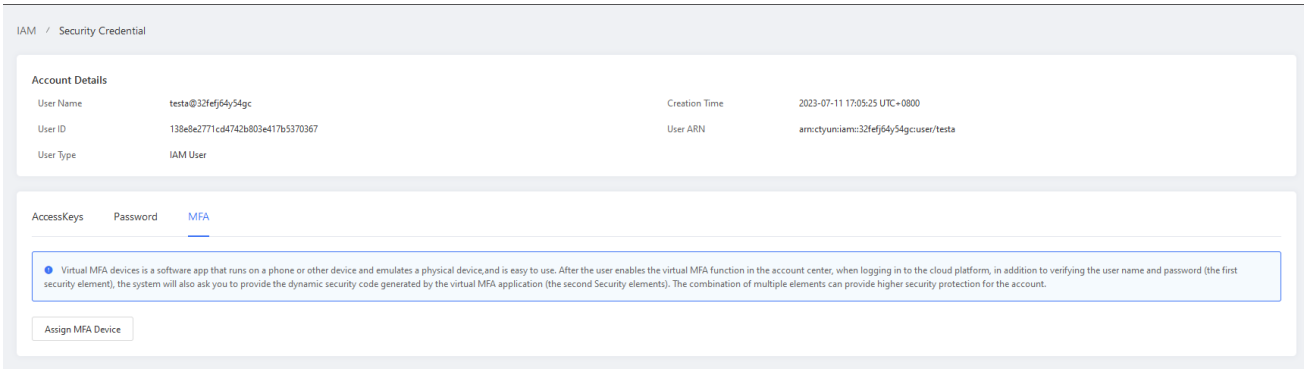
7.6.2 Password

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.



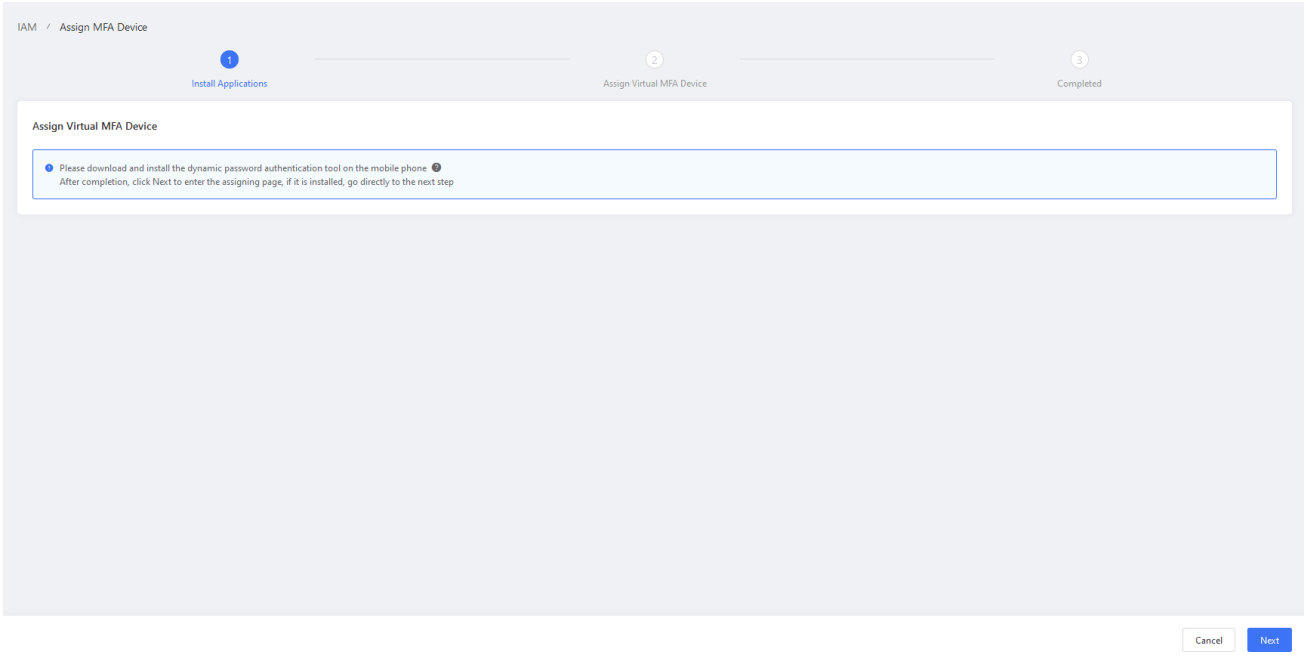
7.6.3 MFA

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.



The MFA binding steps are as follows:

1. Click **`Assign MFA Device`** to enter **`Install Applications`**.

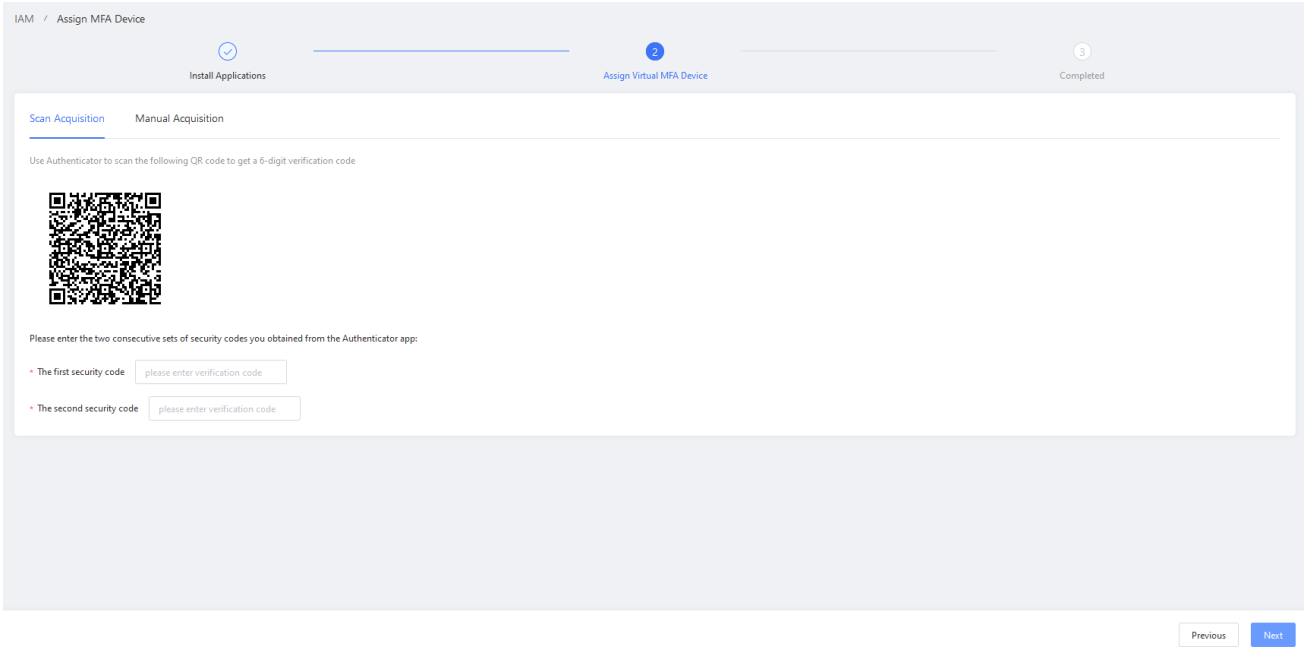


Note: You need to install a Time-based One-Time Password (TOTP) authentication tool on the mobile

phone.

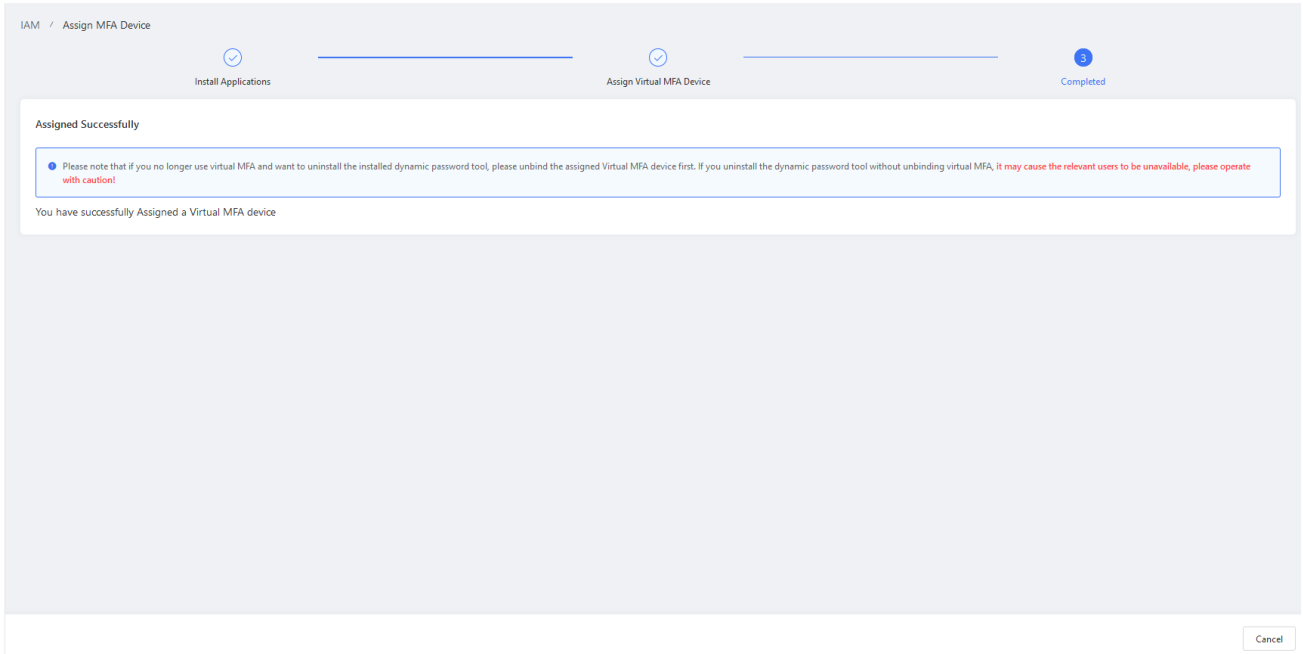
2. Assign Virtual MFA Device: Codes can be obtained by scanning acquisition or manual acquisition.

   Note: The entered first group of security codes and second group of security codes must be consecutive.



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!



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
Confidential Data Authority Group	Supervisor A and Supervisor B	They can view the confidential data in secretBucket, but they cannot change it.
IAM Management Group	Supervisor A	Related management operations for IAM.
Cloudtrail Management Group	Supervisor B	Related management operations for cloudtrail. Have permission to view the data in the operation tracking bucket.
Storage Object group	Staff C and staff D	View and upload object permissions.
Upload Object Group	Programming users	Upload data to the specified bucket through the API.

Confidential Data Authority Group policy

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

```
        "oos:ListBuckets",
        "oos:Get*"
      ],
      "Effect": "Allow",
      "Resource": [
//secretBucket
        "arn:ctyun:oos::10rc2arpn6306:secretBucket",
//all objects in bucket 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": [
        {
            "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": [
        {
            "Sid": "AllowGroupToGetObject",
            "Effect": "Allow",
            "Action": "oos:GetObject",
            "Resource": "arn:ctyun:oos::10rc2arpn6306:appbucket/*"
        }
    ]
}
```

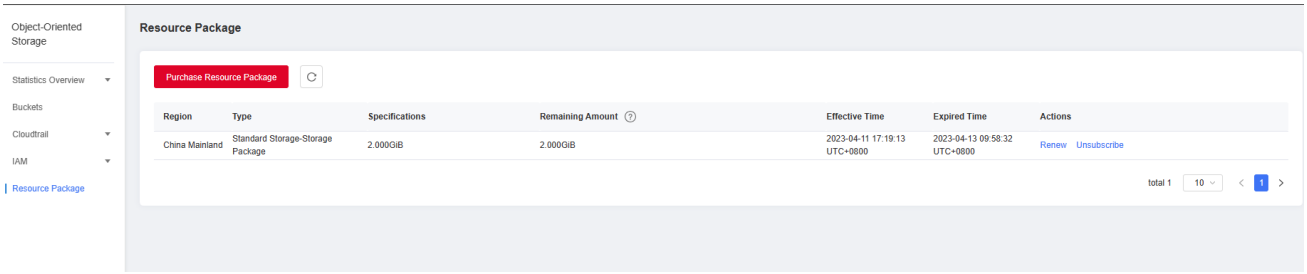
Upload object group policy

```
{
    "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.



9 Appendix

9.1 Endpoints

The endpoint of the **Object Storage Network** is different from the endpoint of **Hongkong** node.

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 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 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.

Table1 OOS action list and corresponding API

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

	PutBucketObjectLockConfiguration	Bucket (*bucketname* or *)	PUT Bucket Object Lock
	DeleteBucketObjectLockConfiguration	Bucket (*bucketname* or *)	DELETE Bucket Object Lock
	PutBucketInventoryConfiguration	Bucket (*bucketname* or *)	PUT Bucket Inventory Configuration, DELETE Bucket Inventory Configuration
Bucket Permissions	PutBucketPolicy	Bucket (*bucketname* or *)	PUT Bucket policy
	DeleteBucketPolicy	Bucket (*bucketname* or *)	DELETE Bucket policy
Object Read	ListMultipartUploadParts	Object (*bucketname*/*objectname* , *bucketname*/*, or *)	List Parts
	GetObject	Object (*bucketname*/*objectname* , *bucketname*/*, or *)	GET Object、HEAD Object
Object Write	PutObject	Object (*bucketname*/*objectname* , *bucketname*/*, or *)	PUT Object, PUT Object-Copy, POST Object, Initiate Mulitipart Upload, Upload Part, Compelete Multipart Upload, Upload Part –Copy
	DeleteObject	Object (*bucketname*/*objectname* , *bucketname*/*, or *)	DELETE Object
	AbortMultipartUpload	Object (*bucketname*/*objectname* , *bucketname*/*, or *)	Abort Multipart Upload

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/*trailname*, trail/*, or *)	GetEventSelectors
	GetTrailStatus	trail (trail/*trailname*, trail/*, or *)	GetTrailStatus

Write	PutEventSelectors	trail (trail/*trailname*, trail/*, or *)	PutEventSelectors
	StopLogging	trail (trail/*trailname*, trail/*, or *)	StopLogging
	CreateTrail	trail (trail/*trailname*, trail/*, or *)	CreateTrail
	UpdateTrail	trail (trail/*trailname*, trail/*, or *)	UpdateTrail
	DeleteTrail	trail (trail/*trailname*, trail/*, or *)	DeleteTrail
	StartLogging	trail (trail/*trailname*, trail/*, or *)	StartLogging

Table4 IAM action list and corresponding API

Action		Resource	API
List	GetAccountSummary	All (*)	GetAccountSummary
	GetLoginProfile	user (user/*username*, user/*, or *)	GetLoginProfile
	ListAccessKeys	user (user/*username*, user/*, or *)	ListAccessKeys
	ListUsers	user (user/* or *)	ListUsers
	ListUserTags	user (user/*username*, user/*, or *)	ListUserTags
	ListGroups	group (group/* or *)	ListGroups
	ListGroupsForUser	user (user/*username*, user/*, or *)	ListGroupsForUser
	ListPolicies	policy (policy/* or *)	ListPolicies
	ListAttachedGroupPolicies	group (group/*groupname*, *group/** or *)	ListAttachedGroupPolicies
	ListAttachedUserPolicies	user (user/*username*, user/*, or *)	ListAttachedUserPolicies
	ListEntitiesForPolicy	policy (policy/*policyname*, policy/*, or *)	ListEntitiesForPolicy
	ListMFADevices	user (user/username, user/*, or *)	ListMFADevices
	ListVirtualMFADevices	mfa (mfa/* or *)	ListVirtualMFADevices
Read	GetUser	user (user/*username*, user/*, or *)	GetUser
	GetAccessKeyLastUsed	user (user/*username*, user/*, or *)	GetAccessKeyLastUsed
	GetGroup	group (group/*groupname*, *group/** or *)	GetGroup
	GetPolicy	policy (policy/*policyname*, policy/*, or *)	GetPolicy
	GetAccountPasswordPolicy	All (*)	GetAccountPasswordPolicy
	GetAccountLoginSecurityPolicy	All (*)	GetAccountLoginSecurityPolicy
Write	CreateAccessKey	user (user/*username*, user/*, or *)	CreateAccessKey
	DeleteAccessKey	user (user/*username*, user/*, or *)	DeleteAccessKey
	UpdateAccessKey	user (user/*username*, user/*, or *)	UpdateAccessKey
	GetSessionToken	user (user/*, or *)	GetSessionToken
	CreateUser	user (user/*username*, user/*, or *)	CreateUser
	DeleteUser	user (user/*username*, user/*, or *)	DeleteUser
	TagUser	user (user/*username*, user/*, or *)	TagUser
	UntagUser	user (user/*username*, user/*, or *)	UntagUser
	CreateGroup	group (group/*groupname*, *group/** or *)	CreateGroup

	DeleteGroup	group (group/*groupname*, *group/** or *)	DeleteGroup
	AddUserToGroup	group (group/*groupname*, *group/** or *)	AddUserToGroup
	RemoveUserFromGroup	group (group/*groupname*, *group/** or *)	RemoveUserFromGroup
	ChangePassword	user (user/*username*, user/*, or *）	ChangePassword
	UpdateAccountPasswordPolicy	All (*)	UpdateAccountPasswordPolicy
	DeleteAccountPasswordPolicy	All (*)	DeleteAccountPasswordPolicy
	UpdateAccountLoginSecurityPolicy	All (*)	UpdateAccountLoginSecurityPolicy
	DeleteAccountLoginSecurityPolicy	All (*)	DeleteAccountLoginSecurityPolicy
	CreateVirtualMFADevice	mfa (mfa/mfaname, mfa/*, or *)	CreateVirtualMFADevice
	DeactivateMFADevice	user (user/*username*, user/*, or *）	DeactivateMFADevice
	DeleteVirtualMFADevice	mfa (mfa/mfaname, mfa/*, or *)	DeleteVirtualMFADevice
	EnableMFADevice	user (user/*username*, user/*, or *）	EnableMFADevice
	CreateLoginProfile	user (user/*username*, user/*, or *）	CreateLoginProfile
	DeleteLoginProfile	user (user/*username*, user/*, or *）	DeleteLoginProfile
	UpdateLoginProfile	user (user/*username*, user/*, or *）	UpdateLoginProfile
Policy	CreatePolicy	policy (policy/*policyname*, policy/*, or *)	CreatePolicy
	DeletePolicy	policy (policy/*policyname*, policy/*, or *)	DeletePolicy
	AttachUserPolicy	user (user/*username*, user/*, or *）	AttachUserPolicy
	DetachUserPolicy	user (user/*username*, 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"
            ],
            "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

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
     "Action": [
       "oos:GetObject",
       "oos:PutObject"
     ],
     "Effect": "Allow",
     "Resource": ["arn:ctyun:oos::123456789012:mybucket/${ctyun: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,

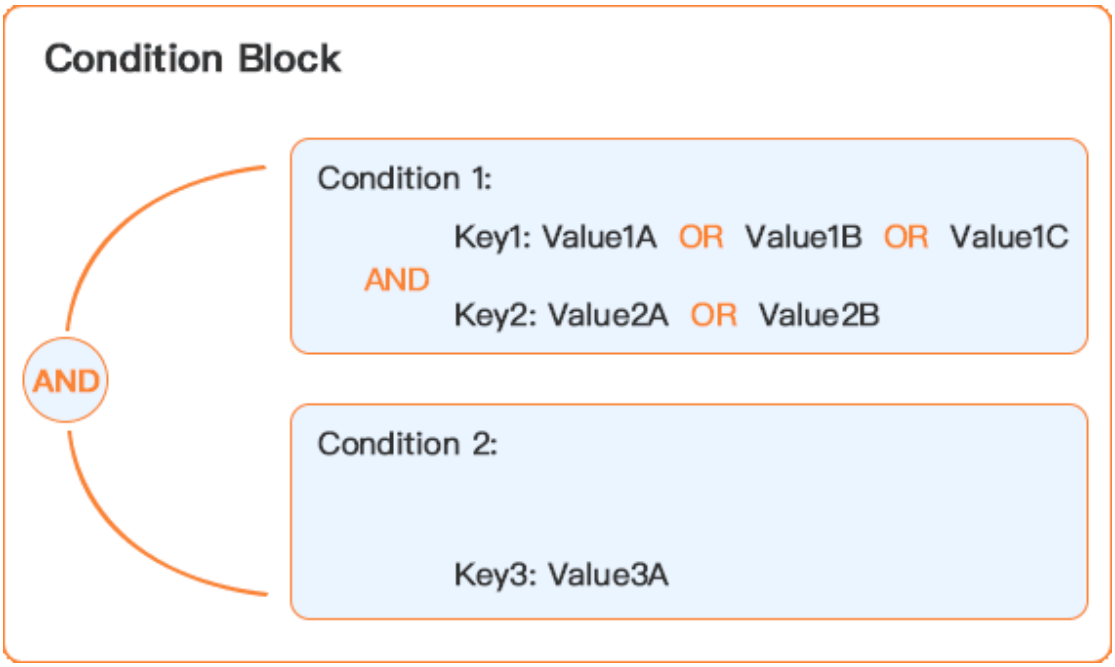
- If Allow is used, all resources not listed, including resources in all other services, will be allowed
- If Deny is used, all resources not listed will be denied.

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.



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 keys, condition operators, and condition values, see the table.

Condition Keys	Condition Operators	Condition Values
ctyun:CurrentTime	• `DateEquals`: Match the specified date. • `DateNotEquals`: Not equal to the specified date. • `DateLessThan`: Before the specified date. • `DateLessThanEquals`: Before or equal to the specified date. • `DateGreaterThan`: Later the specified date. • `DateGreaterThanEquals`: Later or equal to the specified date.	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:SourceIp	• `IpAddress`: Match the specified IP address	IPv4: The value is in dotted

	or IP range. ● NotIpAddress: Match all IP addresses except the specified IP address or IP range.	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	● StringEquals: Matches exactly the specified value and is case sensitive. ● StringNotEquals: Does not match the specified value and is case sensitive. ● 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.	The value is a string of 1 to 32 lowercase letters and numbers. The operators for StringLike and StringNotLike can include wildcard characters.
ctyun:username	● StringEquals: Matches exactly the specified value and is case sensitive. ● StringNotEquals: Does not match the specified value and is case sensitive. ● 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-	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 (@). Note: The condition 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:UserAgent	● StringEquals: Matches exactly the specified value and is case sensitive. ● StringNotEquals: Does not match the specified value and is case sensitive. ● 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.	A string that can contain special characters.
ctyun:Referer	● StringEquals: Matches exactly the specified value and is case sensitive. ● StringNotEquals: Does not match the specified value and is case sensitive. ● 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	A string that can contain special characters.

	specified value and is case sensitive, or does not match the specified value by padding wildcards.	
ctyun:SecureTransport	`Bool`: Boolean match.	• `true` • `false`
ctyun:MultiFactorAuthPresent	`Bool`: Boolean match. **Note**: Only IAM service supports this condition operator.	• `true` • `false`
ctyun:MultiFactorAuthAge	• `NumericEquals`: Match the specified value. • `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.	An integer.
oos:prefix	• `StringEquals`: Matches exactly the specified value and is case sensitive. • `StringNotEquals`: Does not match the specified value and is case sensitive. • `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	The value is a string. **Note**: The condition key is only valid for the operation authority of **oos:ListBucket**.

	matching wildcards (*) or single-character matching wildcards (?).	
oos:x-amz-acl	• `StringEquals`: Matches exactly the specified value and is case sensitive. • `StringNotEquals`: Does not match the specified value and is case sensitive. • `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 (?).	The value is a string. The value: • `private`: only the owner can operate the bucket. • `public-read`: all can read the bucket. • `public-read-write`: all can operate the bucket, including read and write operations. **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`.

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}/*"]}}
    }
  ]
}
```