中国电信天翼云对象存储系统
用户使用手册 V6

中国电信股份有限公司
云计算分公司

目录

产品介绍

中国电信天翼云对象存储系统（Object-Oriented Storage，OOS）是中国电信为客户提供的一种海量、弹性、高可用、高性价比的存储服务。客户只需花极少的钱就可以获得一个几乎无限的存储空间，可以随时根据需要调整对资源的占用，并只需为真正使用的资源付费。

OOS 提供了基于 Web 门户和基于 REST 接口两种访问方式，用户可以在任何地方通过互联网对数据进行管理和访问。OOS 提供的 REST 接口与 Amazon S3 兼容，因此基于 OOS 的业务可以非常轻松的与 Amazon S3 对接。对于无论是希望走出国门的客户，还是希望进入中国的客户，OOS 都是最好的选择。

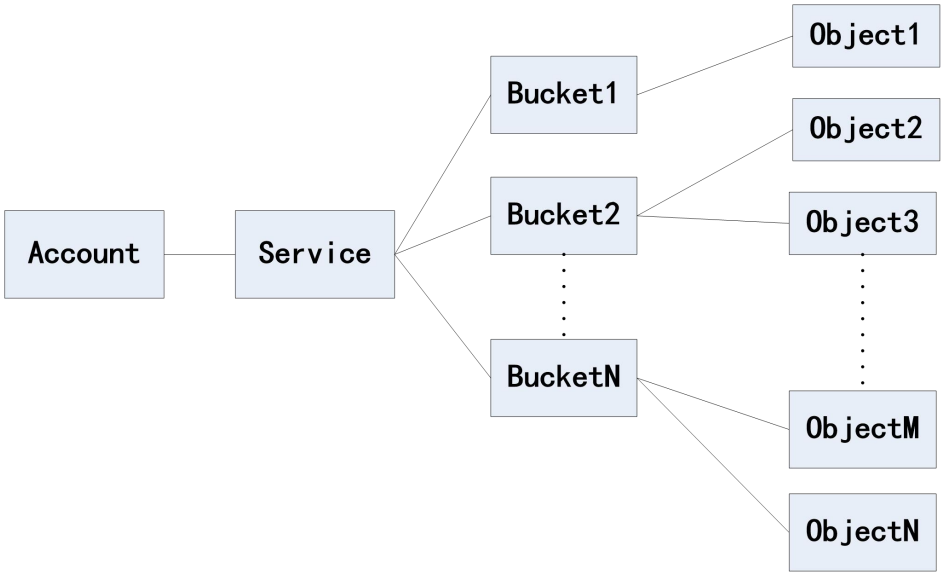
主要概念

OOS 的主要概念

中国电信天翼云对象存储系统的主要概念有：

- Account（账户）：用户登录时 OOS 使用的账户。
- Service（服务）：OOS 为注册成功用户提供的服务。
- Object（对象）：用户存储在 OOS 上的每个文件都是一个 Object。
- Bucket（对象容器）：存储 Object 的容器。

它们之间的关系如下所示。



在使用 OOS 之前，首先需要在天翼云网站 www.ctyun.cn 注册一个 Account（账户）。注册成功之后，OOS 会为该账户提供服务（Service），在该服务下，用户可以创建 1 个或多个 Bucket（对象容器），每个对象容器中可以存储不限数量的 Object（对象）。

Account

在使用 OOS 之前，需要在天翼云网站 www.ctyun.cn 注册一个 Account（账户）。注册时邮箱、密码和手机号码是必填项。正确填写所需信息并进行实名认证之后，在控制台页面点击开通 OOS 服务，提交订单后便可开通。开通成功之后，用户可以用该账户登录并使用 OOS 服务。

Service

Service 是 OOS 为注册成功用户提供的服务，该服务为用户提供弹性可扩展的存储空间,用户可以根据自己的业务需要建立 1 至 10 个的对象容器(Bucket)。

Bucket

Bucket 是存储 Object 的容器。中国电信天翼云对象存储系统的每个 Object 都必须包含在一个 Bucket 中。您可以设置容器的属性，用来控制数据存储位置、访问权限、生命周期等，这些属性设置直接作用于该容器内的所有对象，因此您可以通过灵活的属性设置，来创建不同的容器，完成不同的管理功能。每个用户最多可以建立 10 个 Bucket。用户只有对 Bucket 拥有相应的权限，才可以对其进行操作，这样保证了数据的安全性，防止非授权用户的非法访问。

Object

用户存储在 OOS 上的每个文件都是一个 Object。文件可以是文本、图片、音频、视频或者网页。OOS 支持的单个文件的大小从 1 字节到 5T 字节。

用户可以上传、下载、删除和共享 Object。此外用户还可以对 Object 的组织形式进行管理，将 Object 移动或者复制到目标目录下。

存储类型

OOS 提供两种类型的存储：标准存储和低频访问存储。用户可以根据不同业务场景选择不同的存储类型。

- **标准存储（STANDARD）**：访问时延低、吞吐量高，能够有效支持各种热点类型数据频繁访问。适用于各种音视频服务、图片服务、大型网站、大数据分析等应用的数据存储。标准存储是默认的存储类型。如果上载对象时未指定存储类，OOS 默认使用标准存储。
- **低频访问存储（STANDARD_IA）**：适合长期保存不经常访问的数据。对于不经常访问但仍需要实时访问的数据，可以采用低频访问存储，例如各类移动应用、智能设备、企业数据的长期备份。
  - 最短存储时间：低频访问存储的对象有最短存储时间，存储时间短于 30 天的对象被提前删除或变更时，会产生一定费用。

- 最小计费大小：低频访问存储对象有最小计费大小，即如果对象大小低于 64KB，会按照 64KB 计算收费，对象大于等于 64KB 按照实际存储收费。
- 数据取回：获取数据时会产生数据取回费用。

存储类型的对比

对比指标	标准存储类型	低频访问存储类型
数据持久性高达	99.99999999999%（13 个 9）	99.99999999999%（13 个 9）
服务设计的可用性	99.9%	99.9%
对象最小计费大小	按照对象实际大小计算	64KB
最少存储时间	无最短存储时间要求	30 天
数据取回费用	不收取数据取回费用	按实际获取的数据量收取，单位 GiB
数据访问特点	实时访问	实时访问
图片处理	支持	支持
HTTPS 加密传输	支持	支持
修改存储类型	支持	支持

存储类型转换

对象的存储类型之间支持相互转换：

- 标准存储转换为低频访问存储：可以通过设置生命周期规则、修改对象存储类型将标准存储转换为低频访问存储。
- 低频访问存储转换为标准存储：可以通过修改对象存储类型将低频访问存储转化为标准存储，但不能通过生命周期将低频访问存储转换为标准存储。

合规保留

OOS 提供合规保留功能，即开启 Bucket 合规保留功能后，任何用户（包括根用户）都不能对此 Bucket 内处于合规保留期的对象进行修改和删除。

可以根据需求，对 Bucket 级别开启合规保留功能，以天（Days）为单位设置合规保留时长。

注意：

- 合规保留一旦开启，不能关闭，不能缩短合规保留时长，但可以延长合规保留时长；
- 合规保留的时间精确到秒，例如对 Bucket A 设置合规保留时长为 10 天，对象 A 属于 Bucket A，A 的最后更新时间为 2019-3-1 12:00:00，该文件会在 2019-3-11 12:00:01 过合规保留期。
- 任何用户（包括根用户）都不能修改、覆盖、删除处于合规保留期的对象；
- 处于合规保留期的对象，无法通过调用 API、控制台修改对象的存储类型，只能通过生命周期修改存储类型。
- 处于合规保留期的对象，如果设置了生命周期规则，则修改存储类型的生命周期规则可以生效，设置删除操作的生命周期规则待对象过了合规保留期后才能生效。
- 对象过了合规保留周期后，通过生命周期进行了对象的存储类型修改，不会重新触发合规保留。

示例：

对象 A1、A2、A3 和 A4 都属于 Bucket A，2020 年 2 月 1 日对 Bucket A 设置了合规保留时长为 30 天。对象 A1、A2 分别设置的了生命周期规则，对象 A3、A4 未设置生命周期规则。

对象	生命周期规则
A1	对象创建 10 天由标准存储转换为低频访问存储
A2	对象创建 10 天后删除
A3	无
A4	无

对象	对象最后修改时间	合规保留失效时间	生命周期规则生效情况
A1	2020-03-01 00:00:00	2020-03-31 00:00:01	2020-03-11 后启动转换为低频访问存储操

			作
A2	2020-03-01 00:00:00	2020-03-31 00:00:01	待 2020-03-31 后启动删除操作。
A3	2020-01-01 00:00:00	不存在。因为合规保留 2020-02-01 创建的，在 2020-01-31 00:00:01 已经过了 30 天，故合规保留对 A3 不生效。	不涉及
A4	2020-01-29 00:00:00	2020-02-28 00:00:01	不涉及

统计分析

统计分析指用户可以查询指定 bucket 的使用情况、指定数据域的使用情况。用户可以根据统计分析数据，采取对应的措施。

基本概念

- **直接流量-互联网流量**：从互联网上传下载对象数据，并且未经对象存储网络内部调度产生的流量。
- **直接流量-非互联网流量**：从非互联网（例如内网）上传下载对象数据，并且未经对象存储网络内部调度产生的流量。
- **漫游流量-互联网流量**：从互联网上传下载对象，并且经过对象存储网络内部调度产生的流量。
- **漫游流量-非互联网流量**：从非互联网（例如内网）上传下载对象，并且经过对象存储网络内部调度产生的流量。
- **删除容量**：已删除对象的大小。

操作跟踪

操作跟踪用于记录 OOS 账户的管理事件，并将产生的跟踪日志保存到指定的 OOS 存储桶中。记录的信息包括用户的身份，API 调用的开始时间，源 IP 地址，请求参数以及服务返回的响应元素等。

操作跟踪功能主要包括：

- 管理事件记录：用户可以通过操作跟踪功能可以查看近 180 天内事件，

包括查看、创建、修改和删除资源的管理事件。

- 跟踪日志：当账户中发生一个管理事件时，OOS 会根据配置的跟踪参数与事件进行匹配，当与跟踪参数相匹配时，事件会以日志的形式存储到用户配置的存储桶中，即跟踪日志。

管理事件

在账户中执行的 Bucket 操作、统计操作、IAM 操作、跟踪操作均属于管理事件。

读事件

读事件为可以查看和获取资源但不进行更改的操作。

写事件

写事件为可以修改资源的操作，包括新建、修改和删除操作。

访问控制

用户身份管理和访问控制（Identity and Access Management，简称 IAM）是 OOS 为用户提供的用户身份与权限管理服务，您可以使用 IAM 创建、管理用户账号，并对这些账号进行权限分配，方便资源管理。

您只需为您在天翼云账户中的资源付费，无需为 IAM 单独付费。

功能特性

只要您拥有一个天翼云账号，即可拥有 IAM 功能，天翼云账号管理员可以：

- 创建、管理子用户账号；
- 控制子用户账号内资源具有的操作权限。
- 按需为用户分配不同权限，从而避免与其他用户共享资源使用、访问密钥的使用等，降低账号的信息安全风险。
- 多重身份认证：通过多因素操作认证（MFA）,在进行 IAM 相关操作时，可以使用 MFA，为操作增加一份安全保障。

应用场景

- 用户管理与分权

企业中有不同的员工，各自职责不同，权限不同。有的员工需要进行上传下载对象的操作，有的员工只需要查看统计信息，有的员工只需要查看日志信息。通过 IAM，可以为不同的员工分配不同的操作权限。

基本概念

根用户

用户首次创建 CTYUN 账户时，最初使用的是一个对账户中所有服务和资源有完全访问权限的登录身份，此身份称为根用户。

IAM 用户

IAM 用户是 OOS 中的一个实体，该实体代表使用它与 OOS 进行交互的人员或应用程序，由 CTYUN 账户在 OOS 中创建的用户，也称为子用户。默认情况下，全新的 IAM 用户没有执行任何操作的权限，新用户无权执行任何 OOS 操作或访问任何 OOS 资源。

用户组

用户组是用户的集合，IAM 可以将 IAM 用户添加到对应的用户组，通过对用户组进行授权管理 IAM 用户，用户组的权限会影响用户组内的 IAM 用户。建议具备相同权限的 IAM 用户添加到同一用户组，方便管理。同一个 IAM 用户可以同时加入多个用户组。

MFA

多因素认证（Multi-Factor Authentication，简称 MFA）是一种简单安全的二次认证方式，为用户增加了一层安全保护。仅子用户支持 MFA。

授权

通过给用户组和用户添加策略，用户就能获得策略中定义的权限，这一过程称为授权。

策略

策略是以 JSON 格式描述权限信息的集合，可以精确地描述被授权的资源集、操作集以及授权条件。支持系统策略和自定义策略：

- 系统策略：天翼云 OOS 预先创建好的策略，用户可以根据自身需求，直接引用。对于系统策略，用户只能使用，不能修改。
- 自定义策略：用户自己创建的策略，用户可以对该类型策略进行修改和删除。

服务限制

IAM 中的用户、用户组等有限定的配额。

项目	限额
账户中的 IAM 用户数量	500

账户中可存在的自定义策略数量	150
账户中可存在的组数量	30
附加到 IAM 用户的策略数量	10
账户根用户的访问密钥数量	2
IAM 用户的访问密钥数量	2
IAM 用户可加入的用户组数量	10
附加到 IAM 用户的标签数量	10
附加到 IAM 组的策略数量	10

账户管理

注册

用户通过填写邮箱、密码、联系方式及其他一些可选填信息来注册账户，依据提示完成注册。

登录

登录时需要输入邮箱和密码，或者通过手机 APP 扫描二位码登录。

找回密码

已注册用户在忘记密码的时候，可以在登录界面点击**忘记密码**，通过快捷通道找回密码。找回密码时，用户需要根据提示，按步骤输入相关信息找回密码。

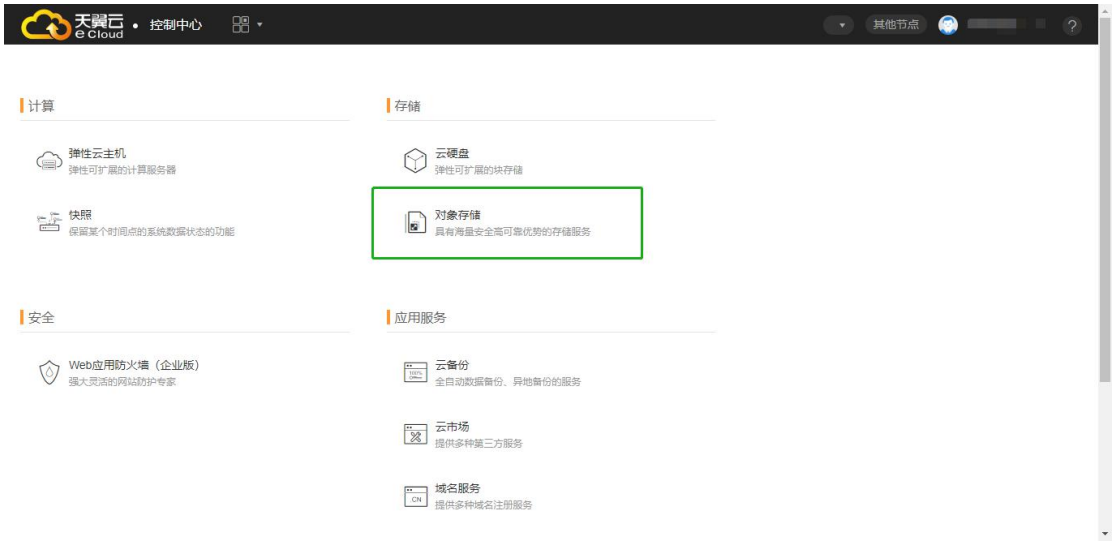
退出

登录的账户，点击**退出**按钮，退出当前登录的账户。

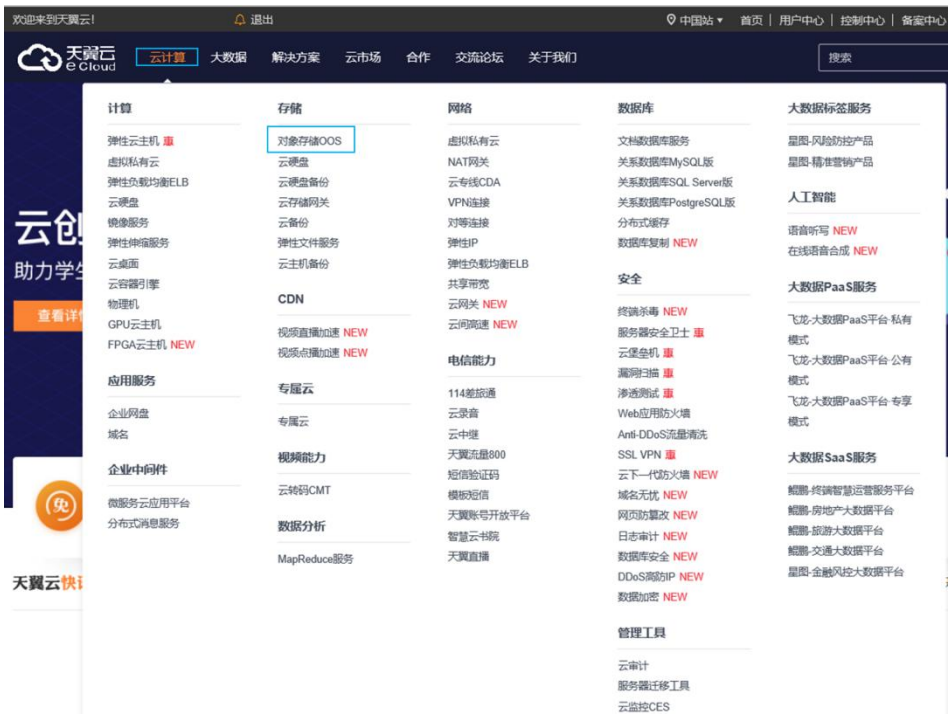
进入对象存储

用户可以通过以下两种方式进入对象存储 OOS：

1、 右上角**控制中心->对象存储**



2、 首页导航栏**云计算->对象存储 OOS->控制台**



地域切换

用户可以在右上角处对 OOS 地域进行切换，根据选择跳转到不同的区域。推荐使用**对象存储网络**。对象存储网络中包含分布在全国多个省、市、自治区及直辖市的资源池，这些资源池间的容器（Bucket）、对象（Object）、访问密钥（AccessKeyId 和 AccessSecretKey）信息互通，可以实现全国数据的就近读取和写入。除对象存储网络之外的其他地域，容器、对象、访问密钥信息是不互通的。

统计概览

在**统计概览**页，用户可以查询 **Bucket 当日统计**（包括：存储容量、互联网下行流量、互联网上行流量、GET 类、PUT 类）、**昨日关键数据、当月关键数据、容量、流量、请求次数、并发连接数。**

说明：对于 IAM 子用户，拥有相应的权限才可以查看统计相关信息，操作和需要拥有的权限如下：

操作	需具备的权限
统计	statistics:GetAccountStatistcsSummary

概览

点击**统计概览->概览**，可用查看 Bucket 当日统计，包括：存储容量、互联网下行流量、互联网上行流量、GET 类请求和 PUT 类请求。

点击该页面的**昨日关键数据**（统计时间范围为北京时间当前时刻的前一天 00:00-24:00 的数据），可用查看各数据位置昨日的**标准存储（峰值）、低频访问存储（峰值）、互联网下行流量、互联网上行流量、GET 类请求次数**（GET 类请求包括 HEAD 和 GET 请求）和 **PUT 类请求次数**（PUT 类请求包括 PUT 和 POST 请求）。

点击该页面的**当月关键数据**（统计时间范围为北京时间当前月份的 1 号 00：00 至当前时刻的能获取到的最后一个数据），可用查看各数据位置当月的**标准存储（峰值）**、低频访问存储（峰值）、**互联网下行流量**、**互联网上行流量**、**GET 类请求次数**和 **PUT 类请求次数**。

统计

容量

进入**统计**页面，点击**容量**，可以查看容量的统计信息，包括计费容量（标准存储、低频访问存储）、实际容量（标准存储、低频访问存储）。

容量的统计信息描述

项目	描述
时间选择	容量查询的时间段，可以选择查看下列时间段的容量： ● **今日**； ● **昨日**； ● **近 7 日**； ● **近 30 日**； ● 根据日历按钮，选择查询任意 90 天内容量。
时间粒度	容量查询的时间粒度，可以选择： ● **按五分钟查询**：统计信息按每 5 分钟展示，可以选择查询**今日**、**昨日**或按日历选择任意 1 天的数据； ● **按小时查询**：统计信息按每小时展示，可以查询**今**

	日、昨日、近 7 日或按日历选择任意 7 天内的数据； ● **按天查询**：统计信息按天展示，可以查询**今日、昨日、近 7 日、近 30 天**或按日历按钮选择任意 90 天内的数据。
数据位置	容量查询的数据位置，可以选择： ● **全部数据位置**：展示所有数据位置的容量和值。 ● **具体数据位置**：根据显示的数据位置进行选择，查看对应数据位置的容量。
存储桶	容量查询的存储桶，可以选择： ● **全部存储桶**：展示所有存储桶的容量之和； ● **具体存储桶**：根据显示的存储桶，选择查看对应存储桶的容量。
取值类型	选择容量查询的类型： ● **平均值**：选择时间段的容量平均值，只能按小时查询或按天查询。 ● **实时值**：选择时间段的容量实时值，可以选择按五分钟查询、按小时查询或按天查询。 ● **峰值**：选择时间段的容量峰值，只能按小时查询或按天查询。
存储类型	选择容量查询的类型： ● **全部存储类型**：分别展示标准存储和低频访问存储的容量 ● **标准类型**：标准存储的容量。 ● **低频类型**：低频访问存储的容量。

可以点击**下载**按钮，下载统计信息到本地查看。

项目	**描述**
Date	统计时间。
SampleCapacity	实时值，单位是 Byte。
MaxCapacity	峰值，单位是 Byte。
AverageCapacity	平均值，单位是 Byte。
RemainderChargeStorageUsage	补齐容量之和，包括时长补齐和大小补齐，单位是 Byte。
RemainderChargeOfDuration	时长补齐容量，单位是 Byte。
RemainderChargeOfSize	大小补齐容量，单位是 Byte。

删除量

进入**统计**页面，点击**删除量**，可以查看删除量的统计信息，包括标准类型的删除量、低频访问存储的删除量。

删除量的统计信息描述

项目	描述
时间选择	删除量查询的时间段，可以选择查看下列时间段的删除量： ● **今日**； ● **昨日**； ● **近 7 日**； ● **近 30 日**； ● 根据日历按钮，选择查询任意 90 天内删除量。
时间粒度	删除量查询的时间粒度，可以选择： ● **按五分钟查询**：统计信息按每 5 分钟展示，可以选择查询**今日**、**昨日**或按日历选择任意 1 天的数据； ● **按小时查询**：统计信息按每小时展示，可以查询**今日**、**昨日**、**近 7 日**或按日历选择任意 7 天内的数据； ● **按天查询**：统计信息按天展示，可以查询**今日**、**昨日**、**近 7 日**、**近 30 天**或按日历按钮选择任意 90 天内的数据。
数据位置	删除量查询的数据位置，可以选择： ● **全部数据位置**：展示所有数据位置的删除量之和。

	● **具体数据位置**：根据显示的数据位置进行选择，查看对应数据位置的删除量。
存储桶	删除量查询的存储桶，可以选择： ● **全部存储桶**：展示所有存储桶的删除量之和； ● **具体存储桶**：根据显示的存储桶，选择查看对应存储桶的删除量。
存储类型	选择删除量查询的类型： ● **全部存储类型**：分别展示标准存储和低频访问存储的删除量 ● **标准类型**：标准存储的删除量。 ● **低频类型**：低频访问存储的删除量。

可以点击**下载**按钮，下载统计信息到本地查看。

项目	**描述**
Date	统计时间。
StorageClass	存储类型，即产生删除量的存储类型
DeleteStorageUsage(Bytes)	用户删除及生命周期删除产生的删除量，单位是 Bytes

流量

进入**统计**页面，点击**流量**，可以查看**上行流量**和**下行流量**的统计信息，包括标准存储和低频访问存储的流量。

流量统计信息描述

项目	描述
时间选择	流量查询的时间段，可以选择查看下列时间段的流量： ● **今日**； ● **昨日**； ● **近 7 日**； ● **近 30 日**； ● 根据日历按钮，选择查询任意 90 天内的流量。
时间粒度	流量查询的时间粒度，可以选择： ● **按五分钟查询**：统计信息按每 5 分钟展示，可以选择查询**今日**、**昨日**或按日历选择任意 1 天的数据；

	● **按小时查询**：统计信息按每小时展示，可以查询**今日、昨日、近 7 日**或按日历选择任意 7 天内的数据； ● **按天查询**：统计信息按天展示，可以查询**今日、昨日、近 7 日、近 30 天**或按日历按钮选择任意 90 天内的数据。
数据位置	流量查询数据位置，可以选择： ● **全部数据位置**：展示所有数据位置的流量之和。 ● **具体数据位置**：根据显示的数据位置进行选择，查看对应数据位置的流量。
存储桶	容量查询的存储桶，可以选择： ● **全部存储桶**：展示所有存储桶的流量之和； ● **具体存储桶**：根据显示的存储桶，选择查看对应存储桶的流量。
存储类型	选择产生流量的存储类型： ● **全部存储类型**：分别展示标准存储和低频访问存储产生的流量。 ● **标准类型**：标准存储产生的流量。 ● **低频类型**：低频访问存储产生的流量。
流量类型	选择流量统计的类型（所有流量均为累计值）： ● **全部流量**：所有流量和值，包括互联网直接流量、互联网漫游流量、非互联网直接流量、非互联网漫游流量。 ● **互联网直接流量**：从互联网上传下载对象数据，并且未经对象存储网络内部调度产生的流量。 ● **互联网漫游流量**：从互联网上传下载对象，并且经过对象存储网络内部调度产生的流量。 ● **非互联网直接流量**：从非互联网（例如内网）上传下载对象数据，并且未经对象存储网络内部调度产生的流量。 ● **非互联网漫游流量**：从非互联网（例如内网）上传下载对象，并且经过对象存储网络内部调度产生的流量。

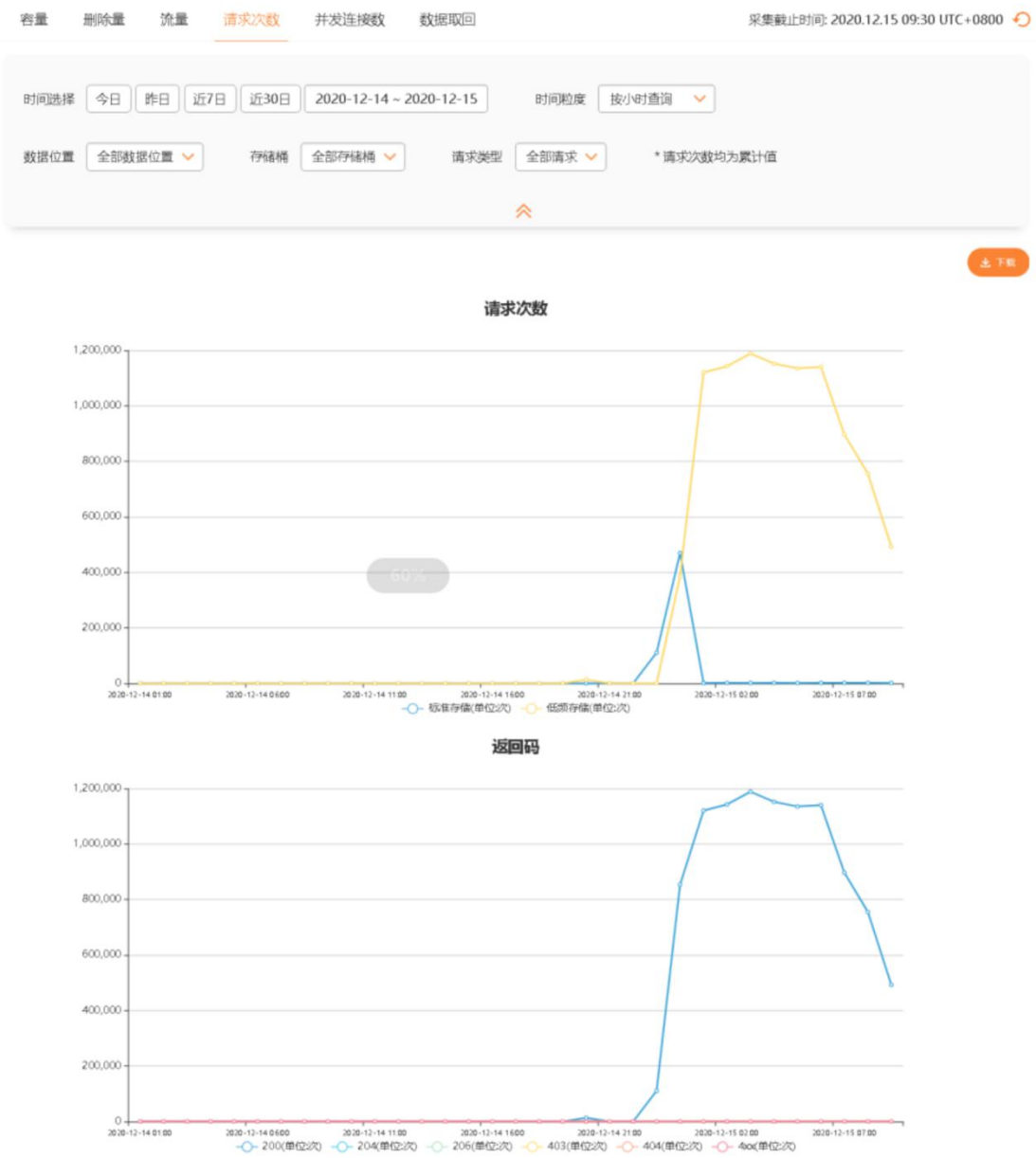
可以点击**下载**按钮，下载流量统计信息到本地查看。

项目	**描述**
Date	统计时间。
StorageClass	存储类型。
InternetDirectInbound	互联网直接上行流量，单位是 Byte。

InternetRoamInbound	互联网漫游上行流量，单位是 Byte。
NonInternetDirectInbound	非互联网直接上行流量，单位是 Byte。
NonInternetRoamInbound	非互联网漫游上行流量，单位是 Byte。
InternetDirectOutbound	互联网直接下行流量，单位是 Byte。
InternetRoamOutbound	互联网漫游下行流量，单位是 Byte。
NonInternetDirectOutbound	非互联网直接下行流量，单位是 Byte。
NonInternetRoamOutbound	非互联网漫游下行流量，单位是 Byte。

请求次数

进入**统计**页面，点击**请求次数**，可以查看请求次数及对应返回码统计信息，包括标准存储和低频访问存储的请求次数。



请求次数和返回码次数统计信息描述

项目	描述
时间选择	请求次数和返回码次数查询的时间段，可以选择查看下列时间段的请求次数和返回码次数： ● **今日；** ● **昨日；** ● **近 7 日；** ● **近 30 日；** ● 根据日历按钮，选择查询任意 90 天请求次数和返回码次数。
时间粒度	请求次数和返回码次数查询的时间粒度，可以选择：

	● **按五分钟查询**：统计信息按每 5 分钟展示，可以选择查询**今日**、**昨日**或按日历选择任意 1 天的数据； ● **按小时查询**：统计信息按每小时展示，可以查询**今日**、**昨日**、**近 7 日**或按日历选择任意 7 天内的数据； ● **按天查询**：统计信息按天展示，可以查询**今日**、**昨日**、**近 7 日**、**近 30 天**或按日历按钮选择任意 90 天内的数据。
数据位置	请求次数和返回码次数查询数据位置，可以选择： ● **全部数据位置**：展示所有数据位置的请求次数之和、返回码次数之和。 ● **具体数据位置**：根据显示的数据位置进行选择，查看对应数据位置的请求次数和返回码次数。
存储桶	请求次数和返回码次数查询的存储桶，可以选择： ● **全部存储桶**：展示所有存储桶的请求次数之和、返回码次数和值。 ● **具体存储桶**：根据显示的存储桶，选择查看对应存储桶的请求次数和返回码次数。
存储类型	选择产生请求次数的存储类型： ● **全部存储类型**：分别展示标准存储和低频访问存储产生的请求次数。 ● **标准类型**：标准存储产生的请求次数。 ● **低频类型**：低频访问存储产生的请求次数。
请求类型	请求次数和返回码次数的请求类型： ● **全部请求** ● **GET；** ● **HEAD；** ● **PUT；** ● **POST；** ● **DELETE；** ● **OTHERS。**

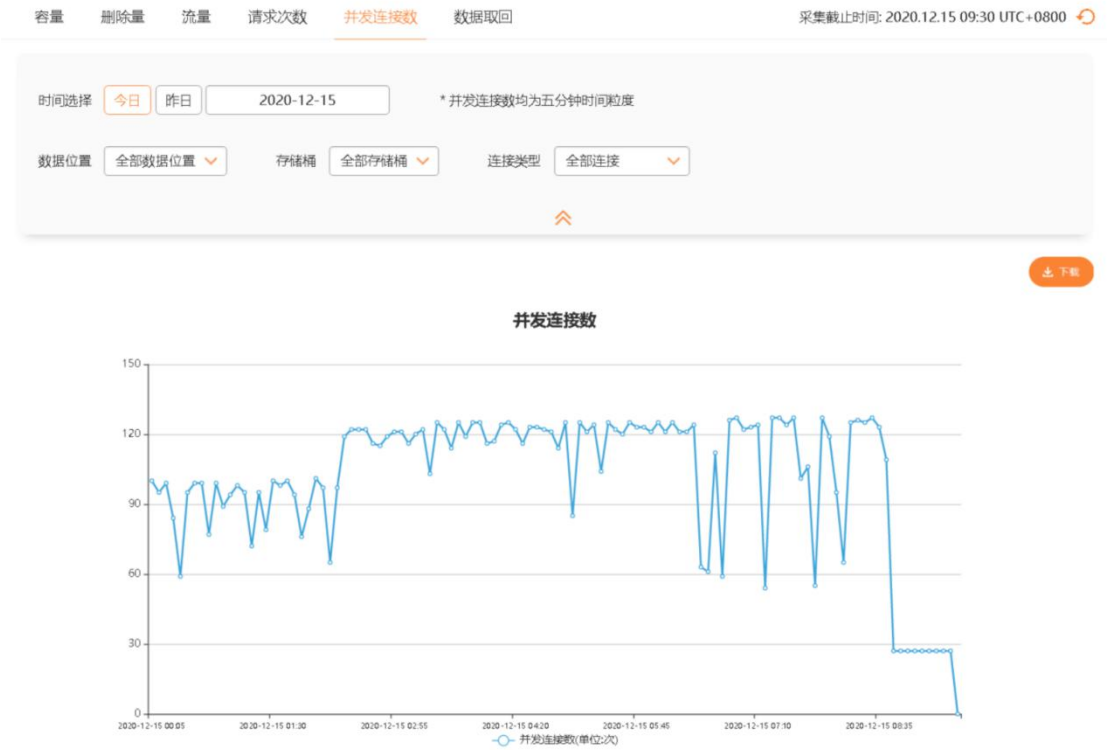
可以点击**下载**按钮，下载请求次数和返回码次数的统计信息到本地查看。

项目	**描述**
Date	统计时间。
StorageClass	存储类型。
Requests	请求次数。
Response200	返回 200 的请求次数。
Response204	返回 204 的请求次数。

Response206	返回 206 的请求次数。
Response403	返回 403 的请求次数。
Response404	返回 404 的请求次数。
Response4XX	返回除 403 和 404 外的其他 4XX 的请求。

并发连接数

进入**统计**页面，点击**并发连接数**，可以查看并发连接数的统计信息。



并发连接数的统计信息描述

项目	描述
时间选择	并发连接数查询的时间段，可以选择查看下列时间段的并发连接数： ● **今日**； ● **昨日**； ● 根据日历按钮，选择查询任意 1 天的并发连接数。
数据位置	并发连接数查询的数据位置，可以选择： ● **全部数据位置**：展示所有数据位置的并发连接数之和。 ● **具体数据位置**：根据显示的数据位置进行选择，查看对应数据位置的并发连接数。
存储桶	并发连接数数查询的存储桶，可以选择： ● **全部存储桶**：展示所有存储桶的并发连接数之和。

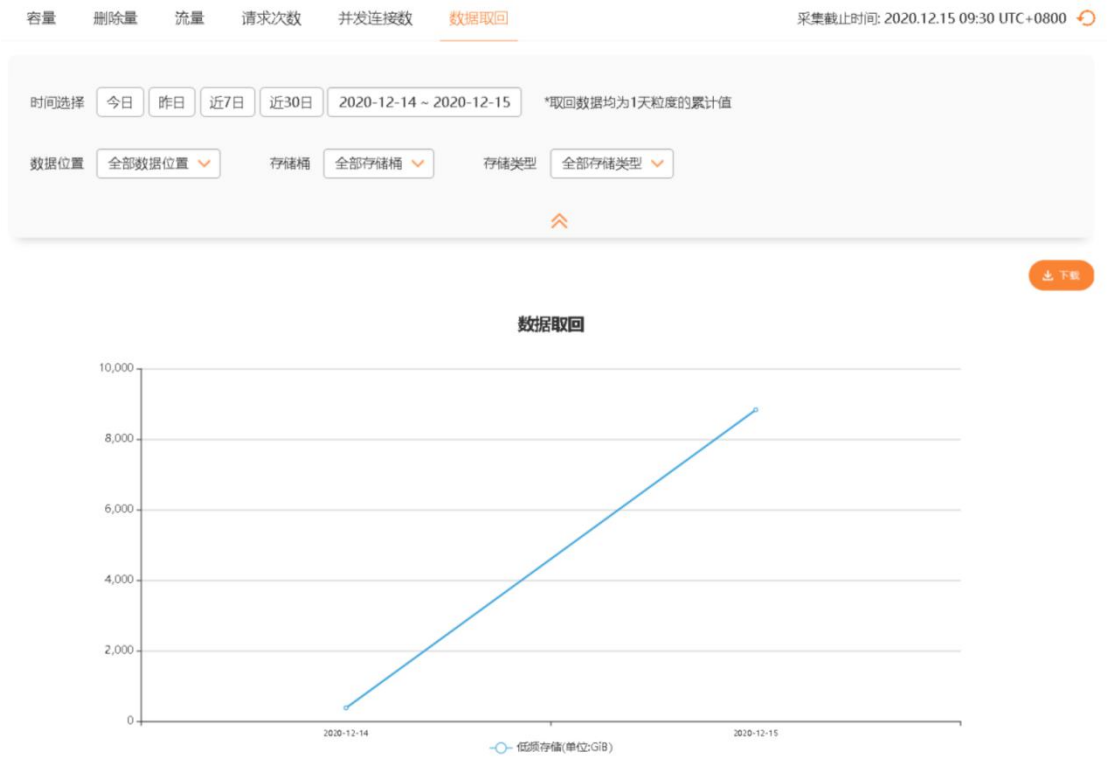
	● **具体存储桶**：根据显示的存储桶，选择查看对应存储桶的并发连接数。
连接类型	选择并发连接数的连接类型： ● **全部连接类型**：包含互联网连接数和非互联网连接数； ● **互联网连接数**； ● **非互联网连接数**。

可以点击**下载**按钮，下载并发连接数的统计信息到本地查看。

项目	描述
Date	统计时间。
Connection	所有并发连接数，包括互联网并发连接数和非互联网连接数。
InternetConnection	互联网并发连接数。
NonInternetConnection	非互联网并发连接数。

数据取回量

进入**统计**页面，点击**数据取回量**，可以查看数据取回量的统计信息。



数据取回量信息描述

项目	描述
时间选择	数据取回量查询的时间段，可以选择查看下列时间段的并发

	连接数： ● **今日**； ● **昨日**； ● **近 7 日**； ● **近 30 日**； ● 根据日历按钮，选择查询任意 90 天数据取回量。
数据位置	数据取回量查询的数据位置，可以选择： ● **全部数据位置**：展示所有数据位置的数据取回量之和。 ● **具体数据位置**：根据显示的数据位置进行选择，查看对应数据位置的数据取回量。
存储桶	数据取回量查询的存储桶，可以选择： ● **全部存储桶**：展示所有存储桶的数据取回量之和。 ● **指定存储桶**：根据显示的存储桶，选择查看对应存储桶的数据取回量。
存储类型	选择数据的存储类型： ● **全部存储类型**：分别展示不同存储类型的数据取回量； ● **低频访问存储**：低频访问存储的数据取回量。

可以点击**下载**按钮，下载并数据取回量的统计信息到本地查看。

项目	**描述**
Date	统计时间
StorageClass	存储类型，即产生数据取回量的存储类型
RestoreStorageUsage(Bytes)	用户获取数据产生的数据取回量，标准存储类型对象产生的数据取回量为 0，单位是 Bytes

容器列表

对于 IAM 子用户，拥有相应的权限才可以在控制台对容器进行操作，操作和需要拥有的权限如下：

操作	**需具备的权限**
创建容器	oos:PutBucket、oos:GetRegions 建议同时赋予的权限：oos:ListAllMyBucket
容器列表	oos:ListAllMyBucket

删除容器	oos:ListAllMyBucket、oos:DeleteBucket
查看/修改容器属性	oos:ListAllMyBucket、oos:GetBucketAcl、oos:PutBucket
区域属性	oos:ListAllMyBucket、oos:GetBucketLocation、oos:PutBucket、oos:GetRegions、oos:GetBucketAcl
安全策略	oos:ListAllMyBucket、oos:GetBucketPolicy、oos:PutBucketPolicy、oos:DeleteBucketPolicy
网站管理	oos:ListAllMyBucket、oos:GetBucketWebSite、oos:PutBucketWebSite、oos:DeleteBucketWebSite、oos:GetRegions
日志	oos:ListAllMyBucket、oos:GetBucketLogging、oos:PutBucketLogging
CDN 加速	oos:ListAllMyBucket、oos:GetBucketAccelerate、oos:PutAccelerateConfiguration
生命周期	oos:ListAllMyBucket、oos:GetLifecycleConfiguration、oos:PutLifecycleConfiguration
跨域设置	oos:ListAllMyBucket、oos:GetBucketCORS、oos:PutBucketCORS

容器管理

用户登录成功后，可以对拥有的 Bucket 及 Object 进行操作。

创建容器（Bucket）

创建容器（Bucket）时，需要输入容器名称，并设置其访问权限、索引位置、数据位置等信息。

1） 命名规范

对象容器（Bucket）的命名规范是：

- Bucket 名称必须全局唯一；
- Bucket 名称长度介于 3 到 63 字节之间；
- Bucket 名称只能由小写字母、数字、短横线（-）和点（.）组成；
- Bucket 名称可以由一个或者多个小节组成，小节之间用点（.）隔开，各个小节需要：
  - 必须以小写字母或者数字开始；
  - 必须以小写字母或者数字结束。
- Bucket 名称不能是 IP 地址形式（如 192.162.0.1）；
- Bucket 名称不能是一组或多组“数字.数字”的组合；
- Bucket 名称中不能包含双横线（--）、双点（..）、横线点（-.）和点横线（.-）；
- 不允许使用非法敏感字符，例如暴恐涉政相关信息等。

2） 访问权限

中国电信天翼云对象存储系统提供 Bucket 级别的权限控制，Bucket 目前有 3 种访问权限：public（公有），private（私有），public-read（只读）。各自的含义如下：

- public（公有）：任何人（包括匿名访问）都可以对该 Bucket 中的 Object 进行 Put，Get 和 Delete 操作。这些操作可能会造成 Bucket 所有者数据的增加或者丢失，且所有这些操作产生的费用由该 Bucket 的所有者承担，所以请慎用该权限。
- private（私有）：只有该 Bucket 的所有者可以对该 Bucket 内的 Object 进行读写操作（包括 Put、Delete 和 Get Object）；其他人无法访问该 Bucket 内的 Object。
- public-read（只读）：只有该 Bucket 的所有者可以对该 Bucket 内的 Object 进行写操作（包括 Put 和 Delete Object）；任何人（包括匿名访问）可以对该 Bucket 中的 Object 进行读操作（Get Object）。

3) 索引位置

索引位置是指存放对象数据索引信息的位置，在创建 Bucket 时指定索引位置，创建成功后不能再对 Bucket 的索引位置进行更改。

4) 数据位置

数据位置是指存放对象数据的位置。

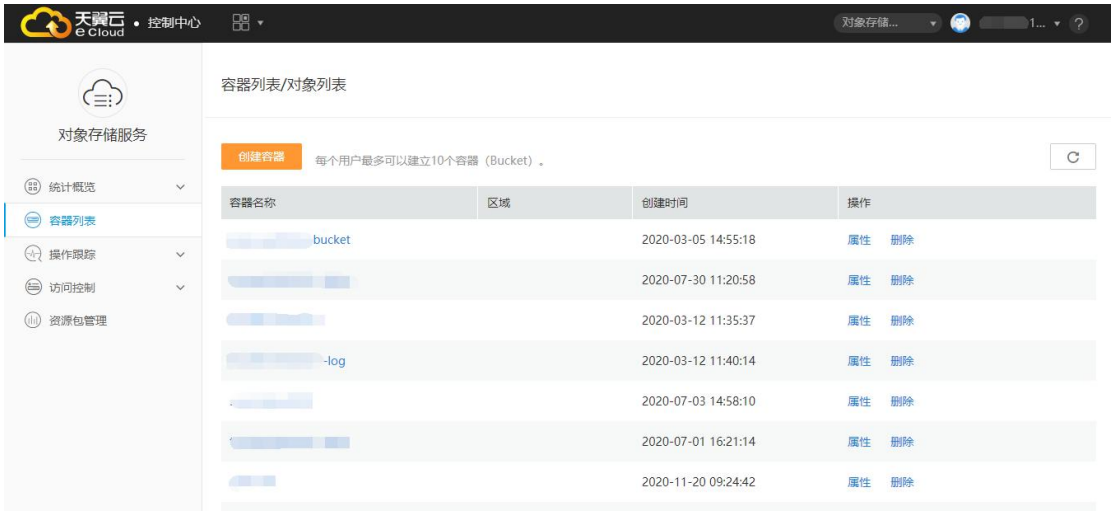
- 如果用户选择**就近写入**，那么对象数据将被存储在距离写入点最近的数据位置。
- 如果用户选择**指定位置**，那么用户可以指定多个数据位置存放对象数据，OOS 将按用户指定的位置顺序存储对象。

5) 数据调度策略

OOS 可以根据用户选择地区的实际使用情况，自动进行数据存储位置的调度，以便为用户提供更快的访问速度。

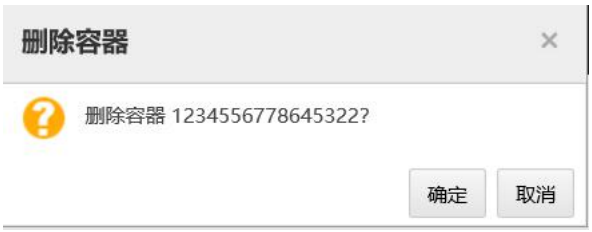
容器列表

容器列表展示了用户创建过的所有容器，以及对应的容器信息。



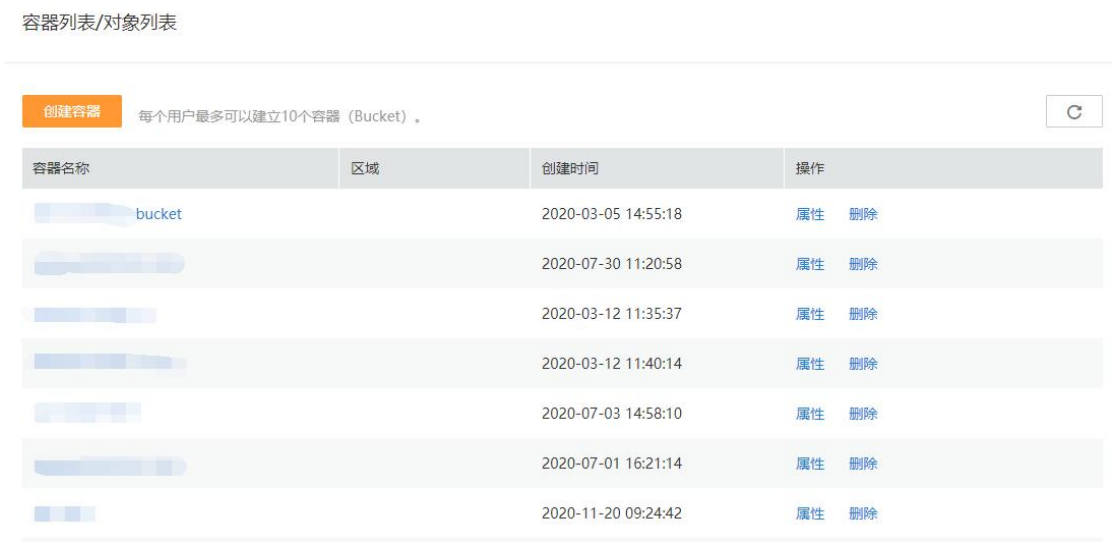
删除容器

只有容器中不包含任何文件夹和文件时，用户才可以删除该容器，当用户点击**删除**时，需要在弹窗进行二次确认后才可以进行删除。



查看/修改容器属性

点击**容器列表**->**属性**，即可查看所选存储容器的属性信息，如下所示。



属性包括容器名称、创建时间和访问权限。名称和创建时间只能查看，不可修改；访问权限可以修改。

区域属性

用户可以通过**区域属性**页更改容器（Bucket）的数据位置和数据调度策略，但不能修改索引位置。

安全策略

可以在 Bucket 属性中定义 Policy，设置 Bucket 的访问权限，点击编辑后输入区域启用，详细的 Policy 格式请参见《开发者文档》。

Policy 示例如下：

1、 Referer 设置

```
{
  "Version":"2012-10-17",
  "Id":"*",
  "Statement":[
    {
      "Sid":"*",
      "Effect":"Allow",
      "Principal":{ "AWS": ["*"] },
      "Action":"s3:*",
      "Resource":"arn:aws:s3:::example-bucket/*",
      "Condition":{
        "StringLike":{
          "aws:Referer":[
            "http://www.mysite.com/*",
            "http://mysite.com/*",
           ""
          ]
        }
      }
    }
  ]
}
```

如上所示，例如要配置名称为"example-bucket"的 bucket 的访问策略，只允许 Referer 头为以“http://www.mysite.com/”或“http://mysite.com/” 开头的 http 请求访问此 Bucket，那么可以采用如上的配置方式。如果也允许 Referer 头为空的请求访问 Bucket，那么可以在"aws:Referer"中加一个空串。

2、 IP 设置

```
{
        "Version": "2012-10-17",
        "Id": "S3PolicyId1",
        "Statement": [
          {
              "Sid": "IPAllow",
              "Effect": "Allow",
              "Principal": {
              "AWS": "*"
           },

           "Action": "s3:*",
```

```
            "Resource": "arn:aws:s3::: example-bucket/*",
            "Condition" : {
                "IpAddress" : {
                    "aws:SourceIp": "192.168.143.0/24"
                },
                "NotIpAddress" : {
                    "aws:SourceIp": "192.168.143.188/32"
                }
            }
        }
    ]
}
```

如上所示，用户如果希望只允许 IP 地址在 192.168.143.0/24 范围内的 IP 访问此 Bucket，不允许 IP 地址在"192.168.143.188/32"范围内的 IP 访问，那么可以采用如上的配置方式。

网站管理

用户可以配置 Bucket 的网站托管属性，并通过 Bucket 域名访问该静态网站。可以设置站点的首页和出错页面。

- 首页地址：指访问网站时跳转到的页面。
- 错误页面：指当访问网站，出现 4XX 错误时，跳转到的页面。

网站配置步骤如下：

1、 创建对象容器（Bucket）

创建一个和用户的域名名称一致的 Bucket，例如创建一个名为“yourdomain.com”的 Bucket。

2、 上传文件

将网站的所有文件（html、CSS、js、图片等）上传到之前创建的 Bucket 中， 注意要保持文件之间的相对路径。

3、 配置 Bucket 网站属性

进入 Bucket 网站属性设置，选择**启用**，输入首页地址和错误页地址。例如将“http://yourdomain.com”的首页地址设置为 index.html，那么当访问该网站时，将默认打开“http://yourdomain.com/index.html”页面。 配置出错页面为 error.html， 那么当访问网站出错时，将跳转到“http://yourdomain.com/error.html”。

4、 配置别名

在域名管理系统中增加一个别名。例如将“yourdomain.com”增加一个别名记录“yourdomain.com.oos-website-cn.oos.ctyunapi.cn”， 当您访问 http://yourdomain.com 时，页面自动跳转到您配置的首页，并展现您的静态网站。

日志

日志功能可以帮助您记录所有操作记录， 您可以通过点击右边的单选框来**开启/不开启**用户日志功能，同时还可以通过设置目标容器和路径来指定日志的存储位置。日志记录的格式，请参见《开发者文档》。

CDN 加速

OOS 为用户提供 CDN 加速功能，可以快速提高对象的下载速度。用户可以配置自己的 CDN 服务提供商的 IP 地址，对于来自这些 IP 的请求，OOS 将不再进行签名校验。

生命周期

用户可以通过此页面设置 Bucket 的生命周期规则。

生命周期是指对象从更新开始到被删除/转换存储类型之前的天数。

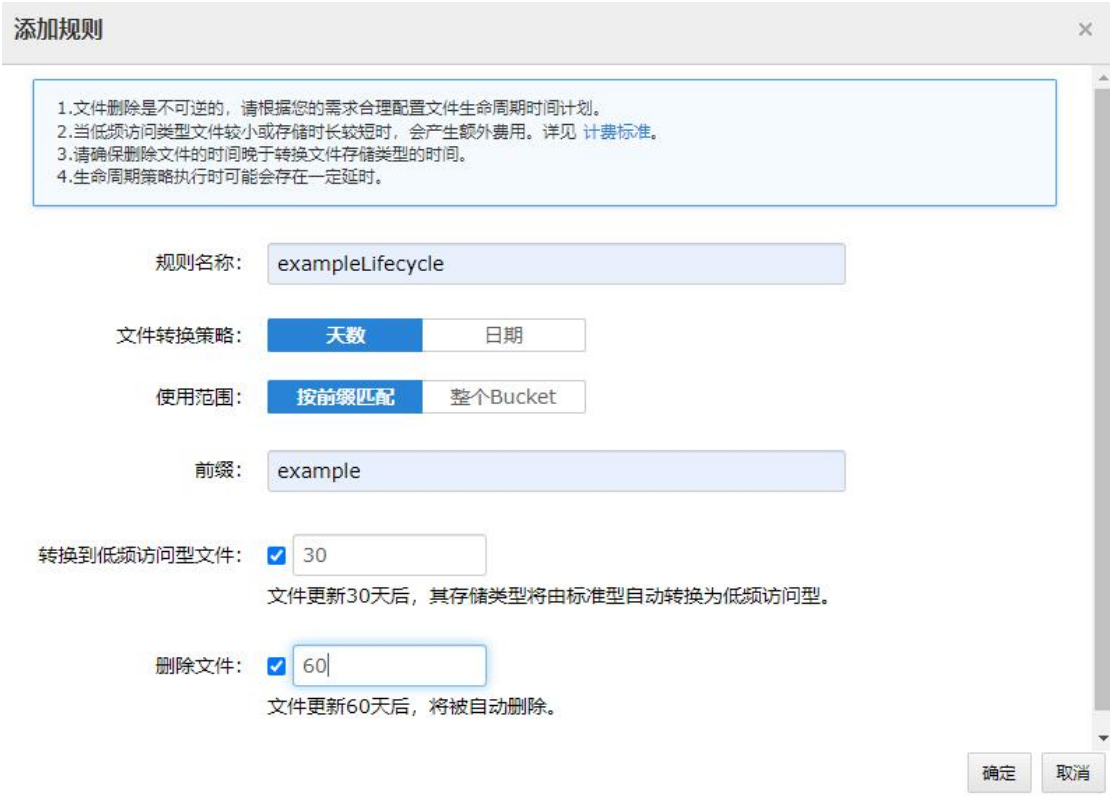
通过设置存储桶的生命周期规则，可以：

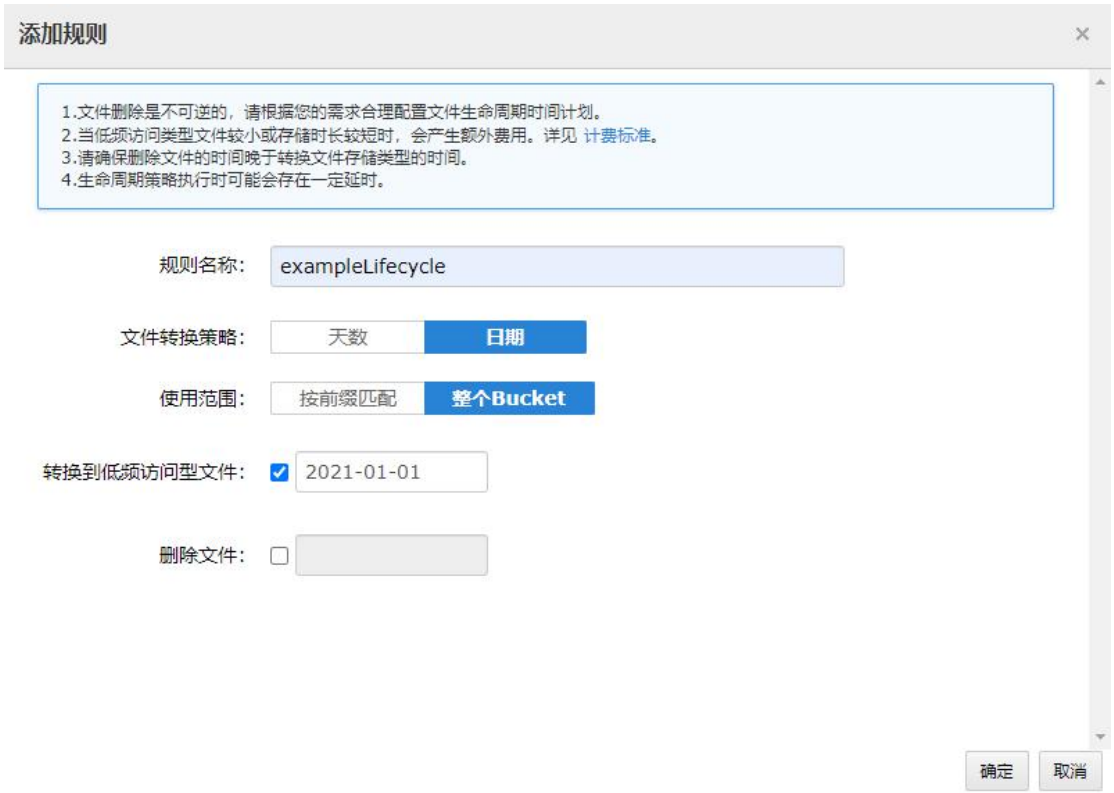
- 删除与生命周期规则匹配的对象。当对象的生命周期到期时，OOS 会异步删除它们。生命周期中配置的到期时间和实际删除时间之间可能会有一段延迟。对象到期被删除后，用户将不需要为到期的对象付费。OOS 删除到期对象后，会在 Bucket log 中记录一条日志，操作项是 "OOS.EXPIRE.OBJECT"。

注意：如果对象的生命周期规则设置的是到期后删除，对象到期后将被永久删除，无法恢复。

- 将与生命周期规则匹配的对象由标准存储转换为低频访问存储。OOS 转换存储类型为低频存储后，会在 access logs 中记录一条日志，操作项是"OOS.TRANSITION_SIA.OBJECT"。

点击**添加规则**后，在弹窗中添加新的生命周期规则。





添加规则描述

项目	名称
规则名称	生命周期规则名称。
文件转换策略	文件按生命周期规则转换的策略： ● 天数：生命周期规则在匹配对象创建多少天后生效。 ● 日期：生命周期规则生效日期，对于最后修改时间在在此日期之前的对象执行生命周期规则。最后修改时间在此后的对象不会被执行生命周期规则。
适用范围	生命规则适用的范围： ● 按前缀匹配：输入生命周期规则匹配前缀，符合该前缀的对象执行生命周期规则；不符合的不执行生命周期规则。 ● 整个 Bucket：创建的生命周期规则适用该 Bucket 内的所有对象。

转换到低频访问文件	匹配生命周期规则的对象，到期后转换成低频访问文件。
删除文件	匹配生命周期规则的对象，到期后删除。

注意：

- 如果 Bucket 没有配置过生命周期规则，执行该操作将创建新的生命周期规则；如果 Bucket 已存在相同名称的生命周期规则，则执行此操作将覆盖原有规则。
- 每个 Bucket 最多创建 100 条生命周期规则。
- 同一 Bucket，同一类型（到期删除或者到期转成低频存储）的生命周期规则不能存在叠加前缀，例如已创建到期删除对象的生命周期规则的前缀是 ABC，则无法再创建前缀为 ABCD 或 AB 或 A 的到期删除对象的生命周期规则。
- 当用户为 Bucket 设置了生命周期规则，这些规则将同时应用于已有对象和后续新创建的对象。例如，用户今天增加了一个生命周期，指定过期时间为 30 天，那么 OOS 将会将最后修改时间在 30 天前的对象都加入到待删除队列中。

OOS 通过将对象的最后修改时间加上生命周期时间来计算到期时间，并且将时间近似到下一天的 GMT 零点时间。例如，一个对象的最后修改时间为 GMT 2016 年 1 月 15 日 10:30，生命周期为 3 天，那么对象的到期时间是 GMT 2016 年 1 月 19 日 00:00。如果对象在上传之后没有修改过，则最后修改时间为该对象的上传时间。

跨域设置

用户可以设置 Bucket 的跨域规则，解决 JavaScript 的跨域访问问题。通过跨域资源共享 (Cross-Origin Resource Sharing，CORS) ，客户可以构建丰富的客户端 Web 应用程序，同时可以选择性地允许跨域访问 OOS 资源。

以下是有关使用 CORS 的示例场景：

- ✓ 场景 1：比如用户的网站 www.example.com，后端使用了 OOS。在 web 应用中提供了使用 JavaScript 实现的上传对象功能，但是在该 web 应用中，只能向 www.example.com 发送请求，向其他网站发送的请求都会被浏览器

拒绝。这样就导致用户上传的数据必须从 www.example.com 中转。如果设置了跨域访问的话，用户就可以直接上传到 OOS，而无需从 www.example.com 中转。

- ✓ 场景 2：假设用户在名为 website 的 Bucket 中托管网站，网站的 Endpoint 是 http://website.oos-website-cn.oos-xx.ctyunapi.cn。现在，用户想要使用网页上的 JavaScript（存储在此 bucket 中），通过 OOS API endpoint oos-xx.ctyunapi.cn 向 bucket 发送 GET 和 PUT 请求。浏览器通常会阻止 JavaScript 发送这些请求，但借助 CORS，用户可以配置 Bucket 支持来自 website.oos-website-cn.oos-xx.ctyunapi.cn 的跨域请求。

注意：如果您使用 JS SDK，CORS 配置请参考《OOS JS 开发者指南》。

点击**添加规则**可以增加新的跨域访问规则：

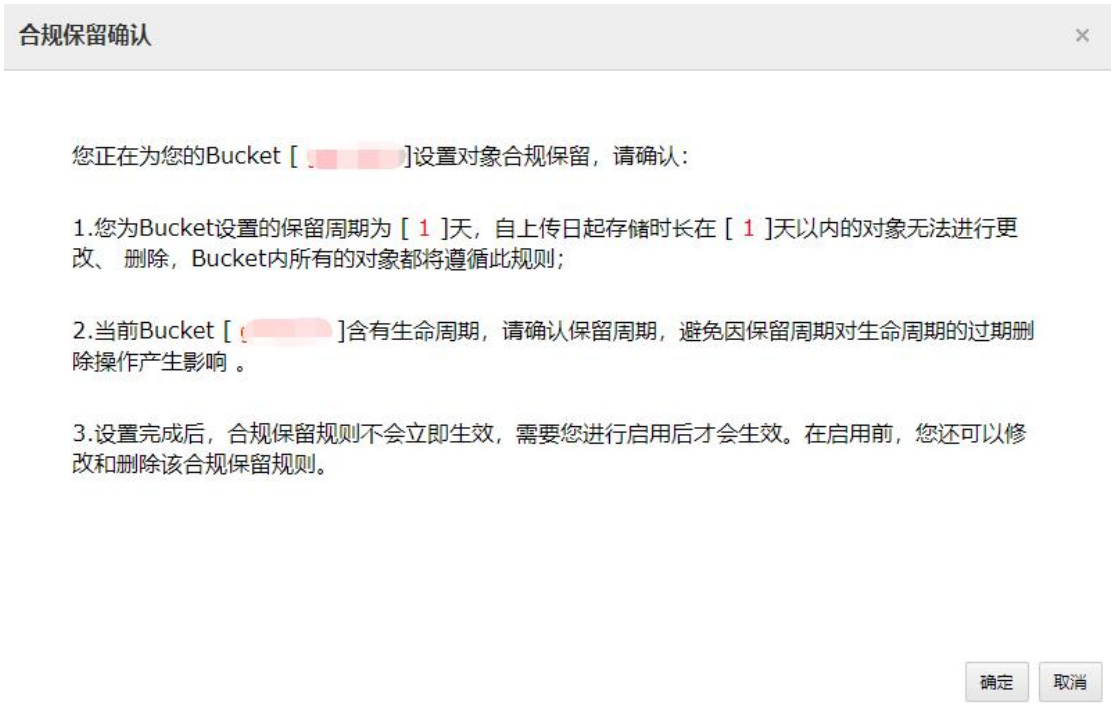
合规保留

可以通过此页面，添加合规保留规则，开启合规保留功能。合规保留开启后，对 Bucket 内的所有对象生效。

开启 Bucket 合规保留功能后，任何用户（包括根用户）都不能对此 Bucket 内处于合规保留期的对象进行修改和删除。

点击**添加规则**，添加合规保留。

点击确定后，会让用户在进行二次确认，是否要开启合规保留。



说明：合规保留创建后，默认是关闭状态，需要用户开启后，才能生效：

- 如果已经开启合规保留策略：设置合规保留时长大于或等于上次设置的时长，才能生效。
- 如果未开启合规保留策略：设置合规保留时长可以大于、等于或小于上次设置的时长。

注意：

- 合规保留一旦开启，不能关闭，不能缩短合规保留时长，但可以延长合规保留时长；
- 合规保留的时间精确到秒，例如对 Bucket A 设置合规保留时长为 10 天，对象 A 属于 Bucket A，A 的最后更新时间为 2019-3-1 12:00:00，该文件会在 2019-3-11 12:00:01 过合规保留期。
- 任何用户（包括根用户）都不能修改、覆盖、删除处于合规保留期的对象；
- 处于合规保留期的对象，无法通过调用 API、控制台修改对象的存储类型，只能通过生命周期修改存储类型。

- 处于合规保留期的对象，如果设置了生命周期规则，则修改存储类型的生命周期规则可以生效，设置删除操作的生命周期规则待对象过了合规保留期后才能生效。

对象管理

对于 IAM 子用户，拥有相应的权限才可以在控制台对对象进行操作，操作和需要拥有的权限如下：

操作	需具备的权限
上传对象	oos:ListAllMyBucket、oos:ListBucket、oos:PutObject
对象下载	oos:ListAllMyBucket、oos:ListBucket、oos:GetObject
对象预览	oos:ListAllMyBucket、oos:ListBucket、oos:GetObject
对象分享	oos:ListAllMyBucket、oos:ListBucket、oos:GetObject
创建文件夹	oos:ListAllMyBucket、oos:ListBucket、oos:PutObject
删除对象	oos:ListAllMyBucket、oos:ListBucket、oos:DeleteObject
移动对象	源和目的都需要的权限：oos:ListAllMyBucket、oos:ListBucket 对于源对象需要具有的权限：oos:GetObject、oos:DeleteObject 对于目的端需要的权限：oos:PutObject
复制对象	源和目的都需要的权限 oos:ListAllMyBucket、oos:ListBucket 对于源对象需要具有的权限：oos:GetObject 对于目的端需要的权限：oos:PutObject
搜索文件	oos:ListAllMyBucket、oos:ListBucket

上传对象

用户可以通过 web 界面上传对象，或者通过 API 上传对象。通过 web 界面上传的对象大小有限制，单个对象不能超过 5GB。若用户需要上传大于 5GB 的对象时，可以通过 API 访问 OOS 服务进行上传。

通过 Web 上传对象时，点击上传，弹出浮窗，选择存储类型（标准存储或者低频访问存储），然后对文件进行上传：

- 将本地目录或多个文件拖到浮层中，自服务门户将您拖进浮层的文件自动上传至 OOS 中，并保留您上传时的目录层级。

  例如：将 photo 文件上传至 OOS，photo 的目录结构如下：

  photo/20190101/1.jpg

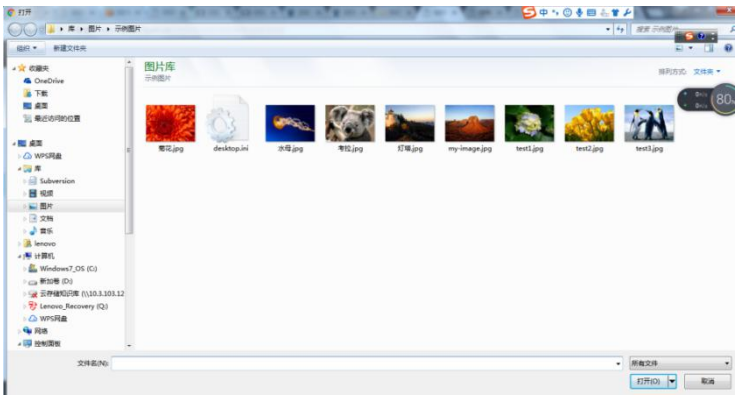
  Photo/20190102/2.jpg

  上传至 OOS 后，保留上传时的目录层级，目录结构如下：

photo/20190101/1.jpg

Photo/20190102/2.jpg

- 点击**直接上传**，弹出上传文件的对话框，可以选择一个或多个对象进行上传。



上传过程中，如果关闭上传的对话框，弹出提示提示信息框。

- **确定**：关闭，结束上传。
- **取消**：继续上传文件。

文件成功上传后，状态为**上传成功**。上传中，显示总进度和各文件的进度。如果上传失败，状态显示**上传失败**。

对象下载

选中一个或者多个对象可以进行下载或批量下载。

对象预览

当鼠标悬停在某一个对象时，对象名称后面会出现预览的操作链接。目前，中国电信天翼对象存储系统支持 pdf、txt、常见格式图片（包括 jpg, png, gif）的在线预览功能。

对象分享

当选择某一个对象进行共享时，需要设置其过期时间及是否要进行下载限速，过期时间以天为单位，下载限速以 KB/s 为单位，当用户设置下载限速时，用户通过该链接下载对象将不高于设置的下载速度。点击**生成**按钮，即可生成一个带有签名认证的 URL。用户可以直接将该 URL 分享给其他人，在有效期内，通过该 URL 可以访问此对象。

对于私有 Bucket 内的 Object，用户可以创建临时的“共享链接”，以便在不破坏 Bucket 的私有属性的前提下，与他人分享 Object。

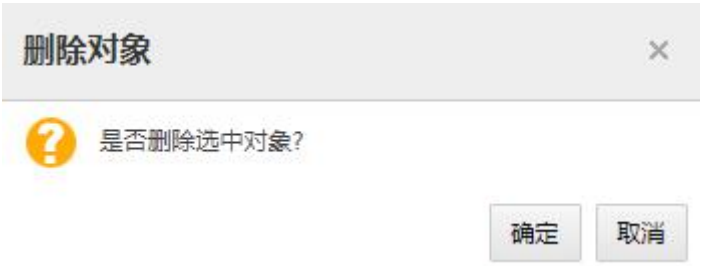
创建文件夹

点击**创建文件夹**打开弹窗设置要创建的文件夹名称，文件夹中可以包含 Object（对象）。文件夹存在的意义是便于 Object（对象）的管理，按照用户的意愿自行组织对象的层次结构。新建文件夹时需要输入**文件夹名称**。其中文件夹名称：

- 不为空 ；
- 不包含 ？〞：/ ’ \ ；
- 不能以 | 开头并且不能以|结尾；
- 不能为：.或者+。

删除对象

删除对象（文件/文件夹）时，需要用户的二次确认，这样做可以有效防止文件误删。

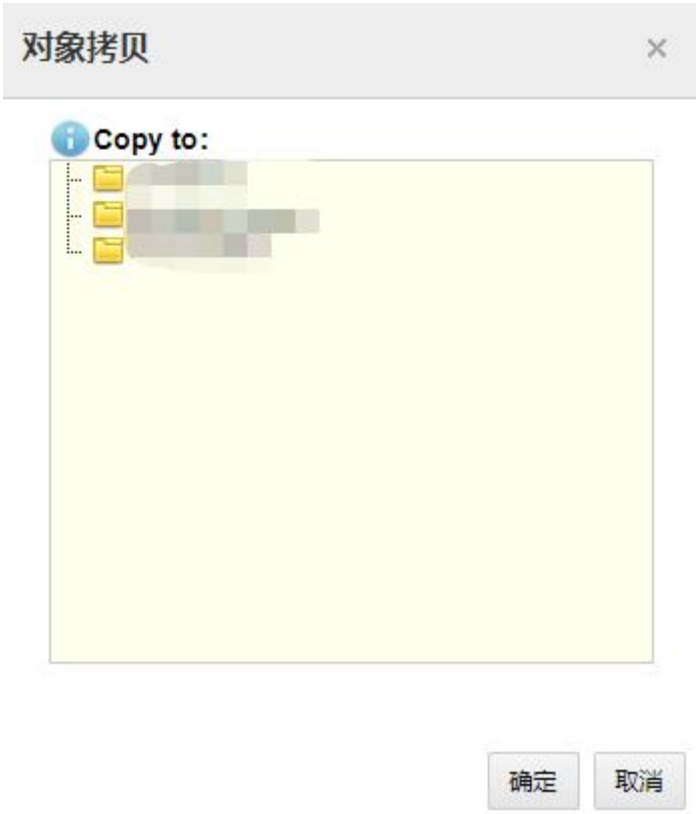


移动对象

用户可以将对象移动到其他存储容器中。

复制对象

用户可以通过**对象拷贝**功能将对象复制到其他 Bucket（容器）中。



搜索文件

当用户存储的对象较多时，可以通过搜索对象前缀来查找符合条件的文件和文件夹。

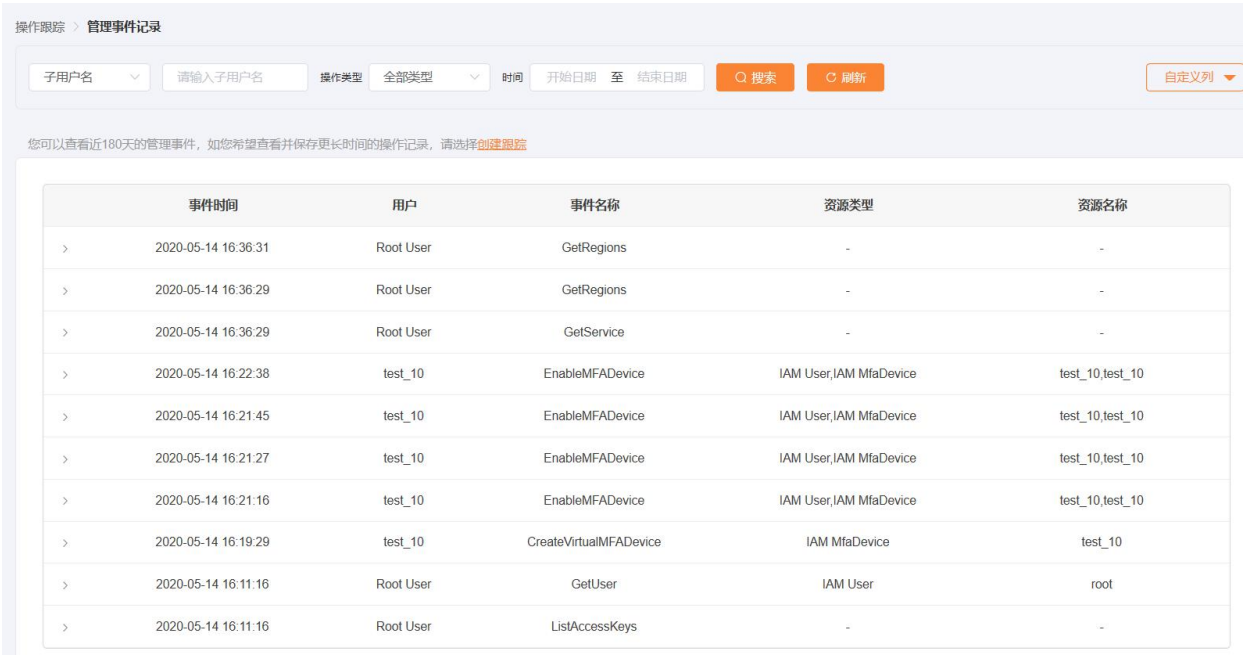
操作跟踪

对于 IAM 子用户，拥有相应的权限才可以在控制台对对象进行操作，操作和需要拥有的权限如下：

操作	需具备的权限
查看管理事件	cloudtrail:LookupEvents
查看跟踪列表	cloudtrail:DescribeTrails、cloudtrail:GetTrailStatus
创建跟踪	oos:ListAllMyBuckets、cloudtrail:CreateTrail、 cloudtrail:PutEventSelectors、cloudtrail:StartLogging
查看跟踪	cloudtrail:DescribeTrails、cloudtrail:GetTrailStatus、 cloudtrail:GetEventSelectors
编辑跟踪	oos:ListAllMyBuckets、cloudtrail:UpdateTrail、 cloudtrail:PutEventSelectors、cloudtrail:DescribeTrails、 cloudtrail:GetEventSelectors、cloudtrail:GetTrailStatus、 cloudtrail:StartLogging、cloudtrail:StopLogging
删除跟踪	cloudtrail:DescribeTrails、cloudtrail:DeleteTrail、 cloudtrail:GetTrailStatus

管理事件记录

进入**操作跟踪->管理事件记录**，可以查看近 180 天的管理事件，如您希望查看并保存更长时间的操作记录，可以点击该页面的**创建跟踪**，创建一个事件跟踪日志。



可以在根据需要，选择**子用户名、访问密钥、事件 ID、事件名称、事件源、资源名称、资源类型**进行查询，同时也可以**选择操作类型**（包括：全部类型、读操作、写操作）、**起止时间**进行搜索。默认显示所有的管理操作。

在**自定义列**，可以选择时间显示的项：**事件时间、用户、事件名称、资源类型、资源名称、事件源、事件 ID、请求 ID、访问密钥、源 IP 地址、操作类型、错误代码**。其中默认显示**事件时间、用户、事件名称、资源类型、资源名称**。

查看详细事件

点击对应事件，可以查看事件的详细信息。

事件详细信息描述

项目	描述
请求时间	事件发生的时间。
事件 ID	由跟踪生成的用来唯一标识每个事件的 ID。
事件源	处理请求的服务端： ● OOS：oos-cn.ctyunapi.com ● 操作跟踪：oos-cn-cloudtrail.ctyunapi.cn ● IAM：oos-cn-iam.ctyunapi.cn

	● 管理 API：oos-cn-mg.ctyunapi.cn ● 自服务门户：oos-cn.ctyun.cn
用户	用户名。
资源类型	操作涉及的资源模块： ● OOS Bucket：存储桶； ● CloudTrail：操作跟踪； ● IAM User：IAM 用户； ● IAM Group：IAM 用户组； ● IAM Policy：IAM 权限策略； ● IAM AccessKey：IAM 密钥； ● IAM MfaDevice：IAM MFA； ● -：事件对应资源类型的所有资源，或者不涉及。
源 IP	用户发起请求的源 IP 地址。
访问密钥	用户发起操作使用的密钥 ID： -：表示控制台访问。
请求 ID	发送请求后，服务端返回的 x-amz-request-id 响应。
事件名称	请求操作的名称。
操作类型	操作类型： ● 读操作； ● 写操作。
资源名称	操作访问的资源： -：表示事件对应的所有资源。
错误码	产生的错误码： -：表示正确访问，无错误码。

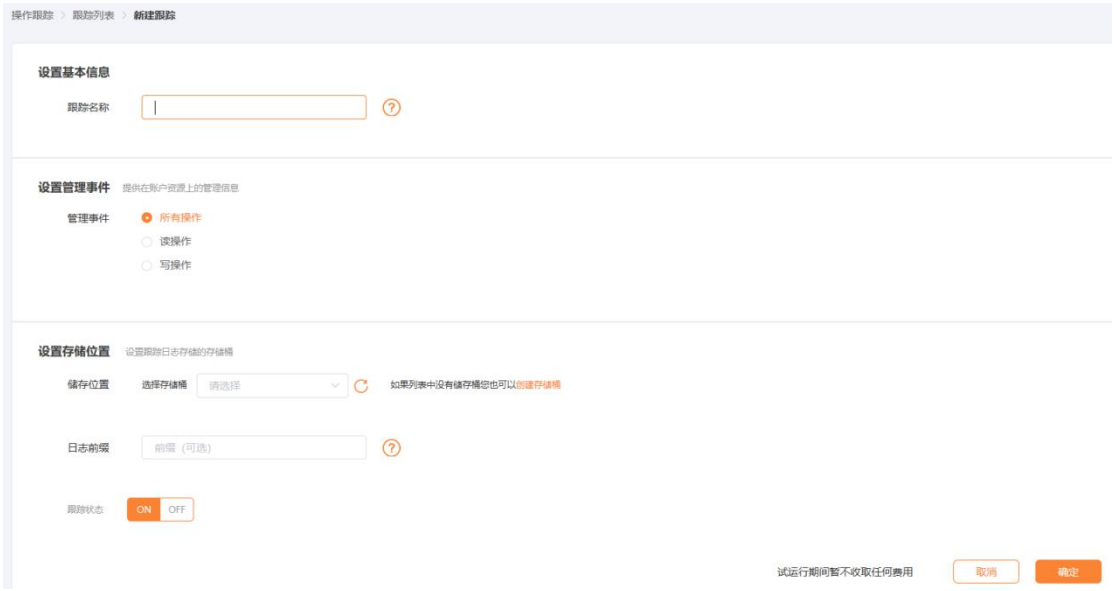
跟踪列表

进入**跟踪列表**页面，可以查看目前账户下的所有跟踪信息，包括：**跟踪名称、日志所在存储桶、日志文件前缀、状态、操作**。

创建跟踪

可以按照下列步骤进行创建跟踪：

1. 在**管理事件记录**页面点击**创建跟踪**，或在**跟踪列表**页面点击**新建**，进入**新建跟踪**页面。
2. 根据提示创建跟踪：



- **设置基本信息**：填写**跟踪名称**，跟踪名称的规则如下：
  - 3~128 位字符串；
  - 可以包含 ASCII 字母（a-z，A-Z），数字（0-9），句点（.），下划线（_）或短划线（-）；
  - 必须以字母或数字开头，以字母或数字结尾；
  - 不能是 IP 地址格式（例如：192.168.5.4）；
  - 不能包含相邻句点（.）、下划线（_）、短划线（-）任意组合。如不能包含类似点点（..）,点下划线（._）的组合。
- **设置管理事件**：可以将管理事件设置为下来三种类型中的一种：
  - **所有操作**：包括读操作和写操作；
  - **读操作**；
  - **写操作**。
- **设置存储位置**：设置跟踪日志存储的**存储位置**、**日志前缀**和**跟踪状态**.
  - **存储位置**：可以存储到现有存储桶（用户需要有对应的存储桶权限），也可以在账户中新建存储桶（用户需要有新建存储桶的权限），并将跟踪日志存储至新建的存储桶；
  - **日志前缀**：0-200 个字符串；

- 指定日志前缀的存储路径为：oos://<bucket>/<日志的名称前缀>/OOSLogs/<账号 ID>/CloudTrail/<年>/<月>/<日>/<日志数据文件>；
- 未指定日志前缀的存储路径为：oos://<bucket>/OOSLogs/<账号 ID>/CloudTrail/<年>/<月>/<日>/<日志数据文件>。

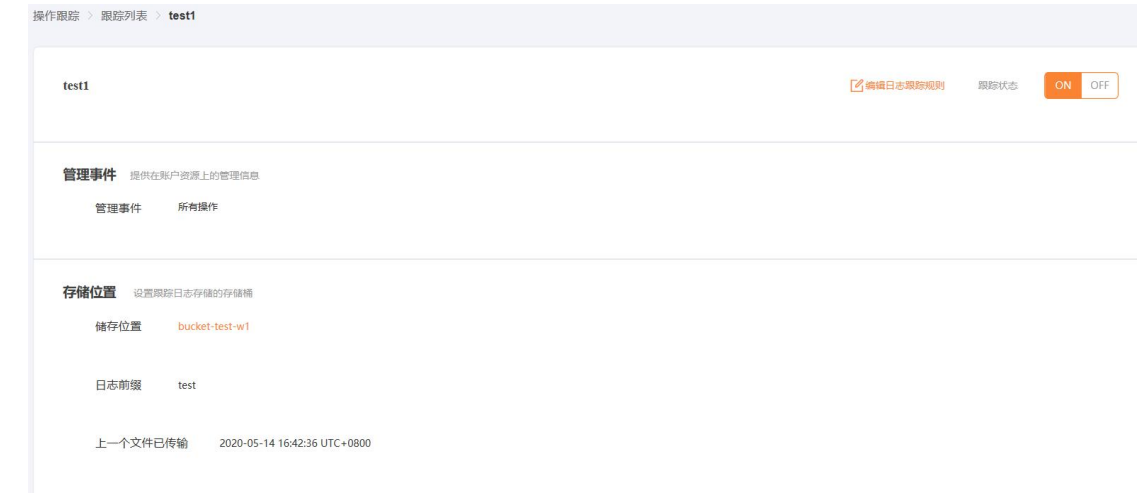
➢ **跟踪状态：**

- **ON：表示跟踪日志开启；**
- **OFF：表示跟踪日志未开启。**

修改跟踪

在**跟踪列表**页面，在需要修改的跟踪后，可以**开启/关闭**、**管理**和**删除**跟踪。

点击需要修改跟踪中的**管理**，进入具体跟踪的详细页面，点击**编辑日志跟踪规则**，可以重新设置管理事件、存储位置、日志前缀和跟踪状态。



访问控制

对于 IAM 子用户，拥有相应的权限才可以在控制台进行 IAM 相关操作，操作和需要拥有的权限如下：

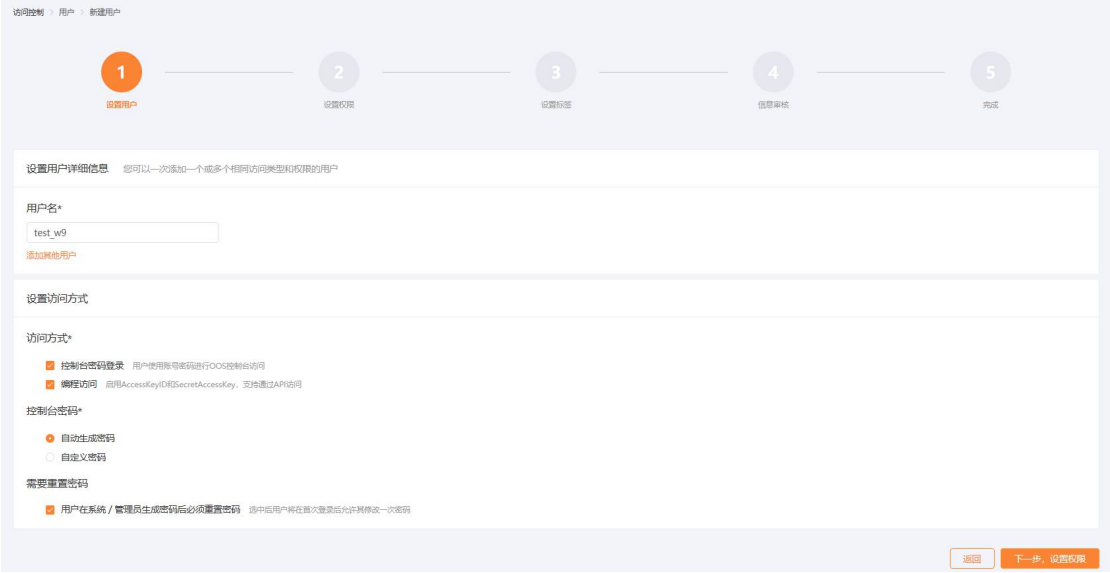
操作		需具备的权限
IAM 用户	创建 IAM 用户	iam:CreateUser、iam:CreateAccessKey、iam:CreateLoginProfile、iam:GetAccountPasswordPolicy、iam:GetUser 建议同时赋予的权限：iam:AddUserToGroup、iam:AttachUserPolicy、iam:ListUsers、iam:ListGroups、iam:ListPolicies
	删除 IAM 用户	iam:ListUsers、iam:DeleteAccessKey、iam:DeleteUser、iam:RemoveUserFromGroup、iam:DeactivateMFADevice、iam:DeleteLoginProfile、iam:DetachUserPolicy
	查看 IAM 用户信息	iam:ListAccessKeys、iam:ListUsers、iam:ListUserTags、iam:ListGroupsForUser、iam:ListAttachedUserPolicies、iam:ListEntitiesForPolicy、iam:ListMFADevices、iam:GetUser
	安全	iam:GetLoginProfile、iam:ListUsers、iam:GetUser、iam:GetAccountPasswordPolicy、iam:CreateLoginProfile、iam:DeleteLoginProfile、iam:UpdateLoginProfile
	密钥	iam:ListAccessKeys、iam:ListUsers、iam:GetUser、iam:CreateAccessKey、iam:DeleteAccessKey、iam:UpdateAccessKey
	权限	iam:ListUsers、iam:ListGroupsForUser、iam:ListPolicies、iam:ListAttachedGroupPolicies、iam:ListAttachedUserPolicies、iam:GetUser、iam:RemoveUserFromGroup、iam:AttachUserPolicy、iam:DetachUserPolicy
	用户组	iam:ListUsers、iam:ListGroups、iam:ListGroupsForUser、iam:GetUser、iam:GetGroup、iam:AddUserToGroup、

		iam:RemoveUserFromGroup
	标签	iam:ListUsers、iam:GetUser、iam:TagUser、iam:UntagUser
用户组	创建用户组	iam:CreateGroup 建议同时赋予的权限：iam:ListGroups、iam:ListPolicies、iam:AttachGroupPolicy
	查看用户组信息	iam:ListGroups、iam:ListAttachedGroupPolicies、iam:GetGroup
	修改用户组	iam:ListUsers、iam:ListGroups、iam:ListGroupsForUser、iam:ListPolicies、iam:ListAttachedGroupPolicies、iam:GetGroup、iam:AddUserToGroup、iam:RemoveUserFromGroup、iam:AttachGroupPolicy、iam:DetachGroupPolicy
	删除用户组	iam:ListGroups、iam:DeleteGroup、iam:RemoveUserFromGroup、iam:DetachGroupPolicy
策略	查看策略	iam:ListPolicies、iam:ListEntitiesForPolicy、iam:GetPolicy
	新建自定义策略	iam:CreatePolicy、iam:GetPolicy 建议同时赋予的权限：iam:ListPolicies
	修改自定义策略	iam:CreatePolicy、iam:GetPolicy、iam:ListPolicies
	删除自定义策略	iam:ListPolicies、iam:DeletePolicy、iam:DetachUserPolicy、iam:DetachGroupPolicy
	授权/移除用户/用户组	iam:ListUsers、iam:ListGroups、iam:ListPolicies、iam:ListAttachedGroupPolicies、iam:ListAttachedUserPolicies、iam:ListEntitiesForPolicy、iam:AttachUserPolicy、iam:DetachUserPolicy、iam:AttachGroupPolicy、iam:DetachGroupPolicy
安全设	编辑密码规则	iam:GetAccountPasswordPolicy、iam:UpdateAccountPasswordPolicy
	清除密码	iam:GetAccountPasswordPolicy、

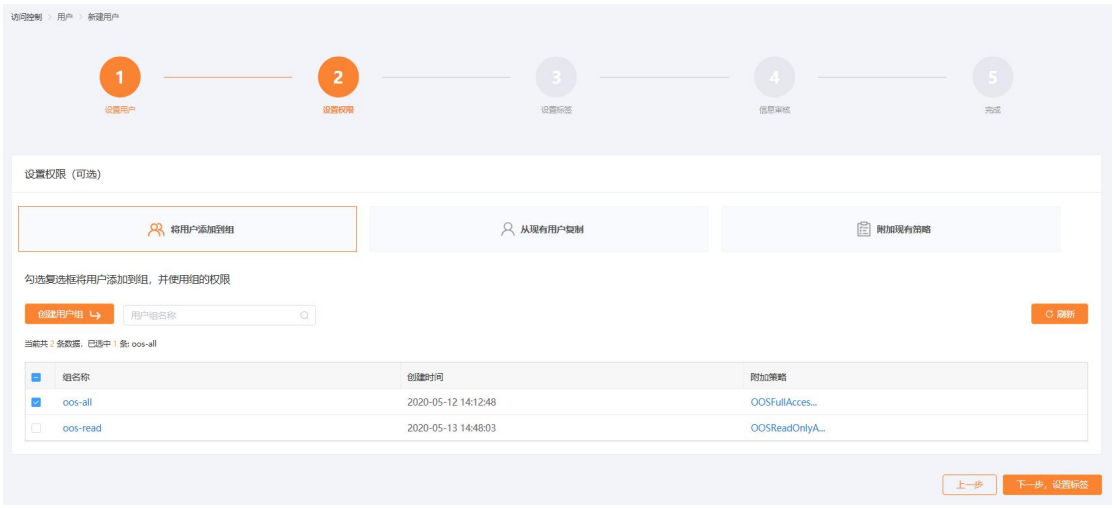
置	规则	iam:DeleteAccountPasswordPolicy
安全凭证	密钥	iam:ListAccessKeys、iam:GetUser、iam:CreateAccessKey、iam:DeleteAccessKey、iam:UpdateAccessKey
	密码	iam:GetLoginProfile、iam:GetUser、iam:ChangePassword
	MFA	iam:ListMFADevices、iam:GetUser、iam:CreateVirtualMFADevice、iam:DeleteVirtualMFADevice、iam:EnableMFADevice、iam:DeactivateMFADevice

快速入门

1. 进入**访问控制->概览**，点击**创建用户**，进入**新建用户**页面，启动创建用户。
2. **创建用户**：根据页面提示添加**用户名**，可以添加一个或多个用户，并为新创建的用户**设置访问方式**。

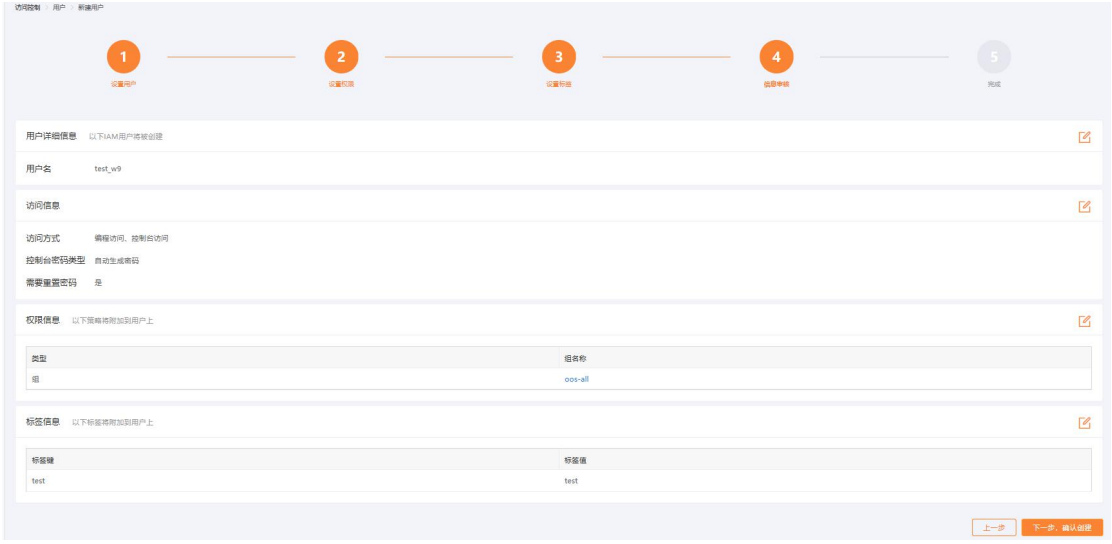


3. **设置权限（可选）**：为用户添加权限，有三种添加权限的方式（只能选择一种）：
   - **将用户添加到组**（前提：已经有用户组）：用户将继承该用户组的所有权限；
   - **从现有用户复制**（前提：现有用户有通过直接附加的方式被授权的策略），每次只能复制一个用户的权限。只能复制现有用户直接附加的策略，不能复制用户所在组的策略。
   - **附加现有策略**。



4. **设置标签（可选）**：可以为新建用户添加标签键和标签值。每个用户最多可添加 10 个标签。

5. **信息审核**：对新建用户的信息进行审核，如果需要更改，可以在此页面点击对应的编辑标识，然后到对应的页面进行修改。



6. **完成**：可以在完成页面查看用户名、访问密钥、用户登录密码。也可以通过**下载凭证**，查看用户名、访问密钥、密码、子用户登录链接。

IAM 用户

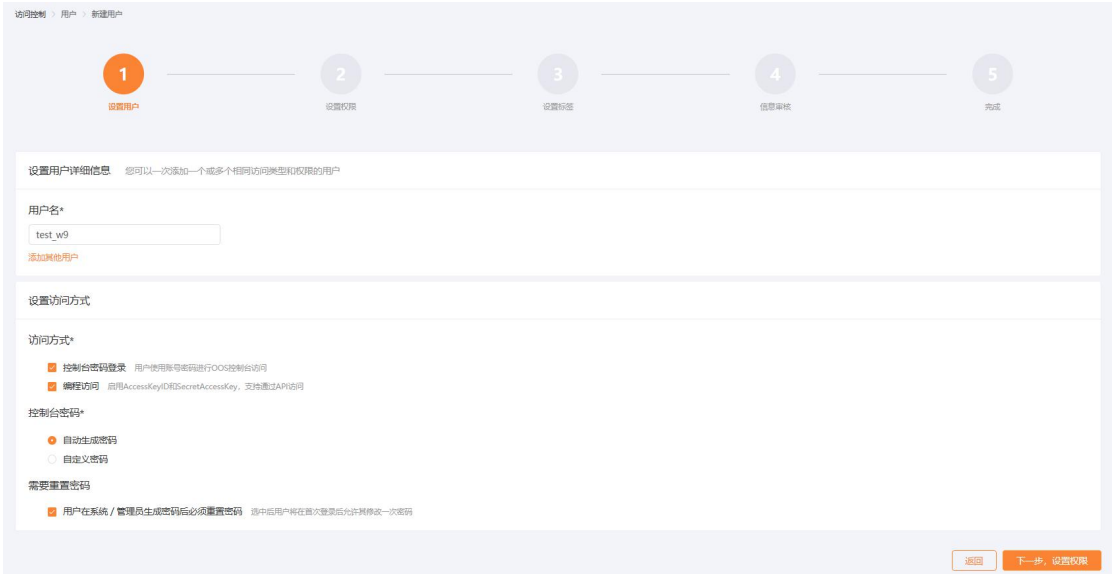
如果您是根用户，即已经开通天翼云 OOS 服务的注册用户，您可以将资源分配给不同的子用户（IAM 用户）使用，为每一个 IAM 用户分配对应的权限。

默认情况下 IAM 用户没有任何权限，根用户或具有 IAM 授权的相关子用户可以给 IAM 子用户授权。授权后，IAM 用户可以根据自己的权限对资源进行操作。

创建 IAM 用户

操作步骤：

1. 登录**访问控制->概览**，单击**创建用户**；或者登录**访问控制->用户**，点击**新建**创建用户。
2. 在**新建用户**页面创建用户信息。



- **用户名**：为登录 OOS 的用户名，管理员一次可以添加 1-10 个具有相同访问类型和访问权限的 IAM 用户。用户名需遵循下列原则：
  - 本账户下，IAM 用户名必须唯一；
  - 1~64 位字符串组成，字符只能包含字母、数字或特殊字符，字母不区分

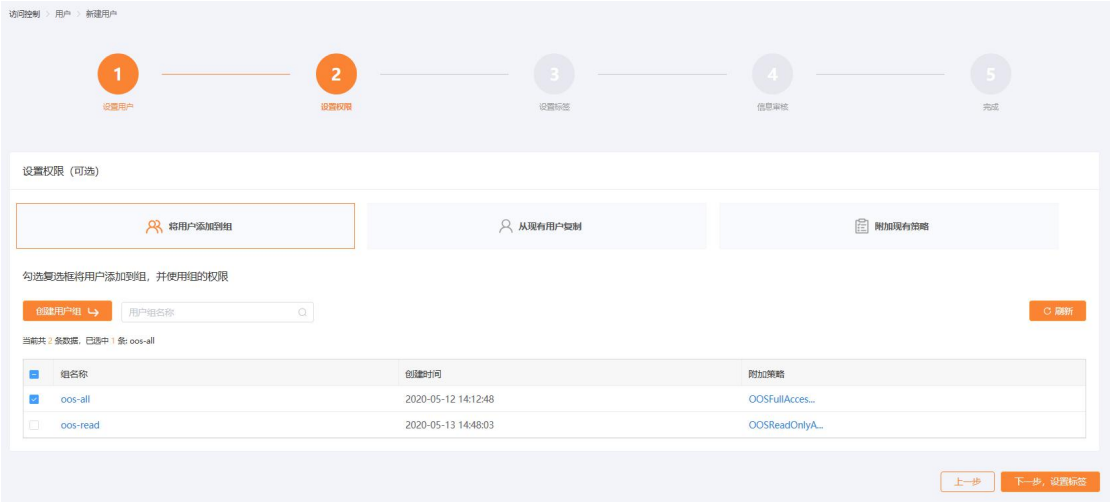
大小写，特殊字符只能是：下划线（_）、中划线（-）、逗号（,）、句点（.）、加号（+）、等号（=）和 at 符号（@）。

- **访问方式**：IAM 用户登录的方式，选择**控制台密码登录**或**编程访问**，至少必须选择一种访问方式：
  - **控制台密码登录**：IAM 用户使用账号密码的方式进行 OOS 控制台访问。
  - **编程访问**：IAM 用户使用密钥通过 API 进行 OOS 服务访问。
- **控制台密码**：管理员可选择为 IAM 用户**自动生成密码**或**自定义密码**：
  - **自动生成密码**：由系统生成随机密码；
  - **自定义密码**：管理员为 IAM 用户自行设置的登录密码。密码规则符合已设置的密码策略。如果还未设置密码策略，则遵循默认的密码规则，默认的密码规则为：密码必须是包含小写字母和数字的 8-128 字符串。
- **需要重置密码**：设置新 IAM 用户在首次登录时是否需要重置密码。若勾选**用户在系统/管理员生成密码**，必须重置密码，即 IAM 用户在首次登录时，必须重置密码。

  注意：您只有**选择控制台密码登录**，才会出现**控制台密码**和**需要重置密码**。

3. 为 IAM 用户设置权限

完成**设置用户**后，进入**设置权限**界面，为 IAM 用户设置权限。



- **将用户添加到组**：用户获得所在组已有的权限，一个用户可以最多加入 10 个组。
- **从现有用户复制**：选择现有用户，获得该用户被直接附加的策略。

  说明：该用户通过用户组获得的策略不会被复制。用户只能复制 1 个用户的权限。
- **附加现有策略**：直接为用户添加现有的策略，每个用户最多可以直接添加 10 个策略。

用户设置权限时，只能选择以上三种方式中的一种为用户授权，当用户已经选择某一种权限设置方式，并进行了必要的勾选后，再切换其他授权方式会弹出提示框：

- **取消**：不进行权限类型更改；
- **更改类型**：确认对现有权限类型进行更改，更改后现有权限信息将不进行保留。

说明：可以创建用户时为用户添加策略，也可以用户创建完成后，再为其添加策略。

注意：每个用户最多可以直接附加 10 条策略，不包含随组附加的策略。

4. 为 IAM 用户设置标签

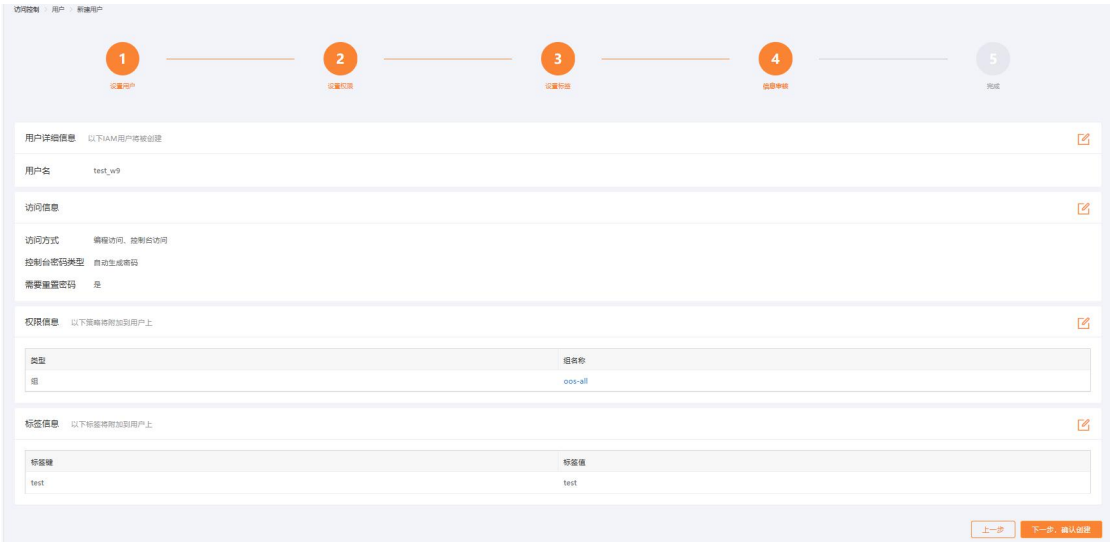
管理员可以为 IAM 用户设置标签，标签为 IAM 用户的附加属性。

一个用户最多可以添加 10 个标签：

- **标签键**：可以包含字母、数字、空格以及加号(+)、等号(=)、句点(.)、at 符号(@)、下划线(_)、连字符(-)、冒号(:)、正斜杠(/)符号的任意组合。标签键不区分大小写，但保留大小写。如不能同时存在 Department 和 department 标签键，如果使用 Department=foo 标签标记用户后又添加 department=bar 标签，则它会替换第一个标签，标签值变为 bar。
- **标签值**：可以为空。
- 不能为单个标签指定多个值，但多个标签键可以有相同的标签值。

5. 信息审核

对于新建用户的信息，可以进行审核。如果有需要修改的地方，可以点击编辑标识 ，到对应页面进行修改。



6. 下载凭证

点击下载凭证，保存新建用户的密钥和密码。

注意：安全凭证仅能下载一次，务必妥善保管。如果某一用户的密钥丢失，可以在该用户详情页，先对原密钥进行删除，然后通过**新建密钥**的方式重新获取新的密钥；如果密码丢失，需要有修改密码权限的用户在控制台进行对该用户密码重置。

查看和修改 IAM 用户信息

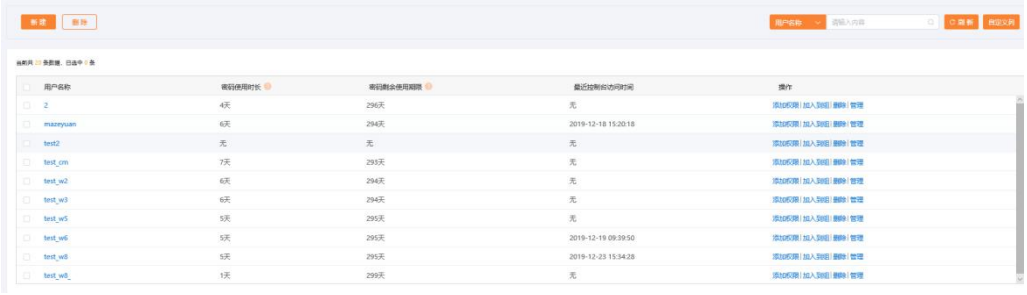
点击导航栏中的**访问控制->用户管理->用户**，出现用户列表。

用户可以根据需要，点击**自定义列**选择显示相应的用户信息，可以选择下列中的几项进行显示:

- **用户名**
- **密码使用时长**
- **密码剩余使用期限**
- **最近控制台访问时间**
- **用户 ID**
- **ARN**

- **是否启用 MFA**
- **编程访问**
- **控制台访问**

其中**用户名**、**操作**为必选项。如果未进行选择，默认显示**用户名**、**密码使用时长**、**密码剩余使用期限**、**最近控制台访问时间**、**操作**。



项目	描述
用户名	IAM 用户名。
用户 ID	IAM 用户的唯一标识符，创建用户时系统随机产生的。
密码使用时长	从密码创建成功起，密码已创建的天数。如果无控制台访问权限，则显示**无**。
密码剩余使用期限	密码剩余时长： ● 用户的密码无过期时间，则显示**永久**； ● 密码未过期，显示剩余天数； ● 密码已过期，显示已过期天数，密码当天显示为**已过期 0 天**。
最近控制台访问时间	IAM 用户最近成功访问控制台的时间。
ARN	IAM 用户名的 ARN，唯一标识 IAM 用户。
是否启用 MFA	MFA 启用状态： ●**启用** ●**不启用**
编程访问	是否启用编程访问： ●**启用** ●**不启用**
控制台访问	是否启用控制台访问： ●**启用** ●**不启用**
操作	**添加权限**：添加该用户所需的策略； ● **加入到组**：将用户加入到用户组； ● **删除**：删除该用户；

	● **管理**：进入用户详情页。

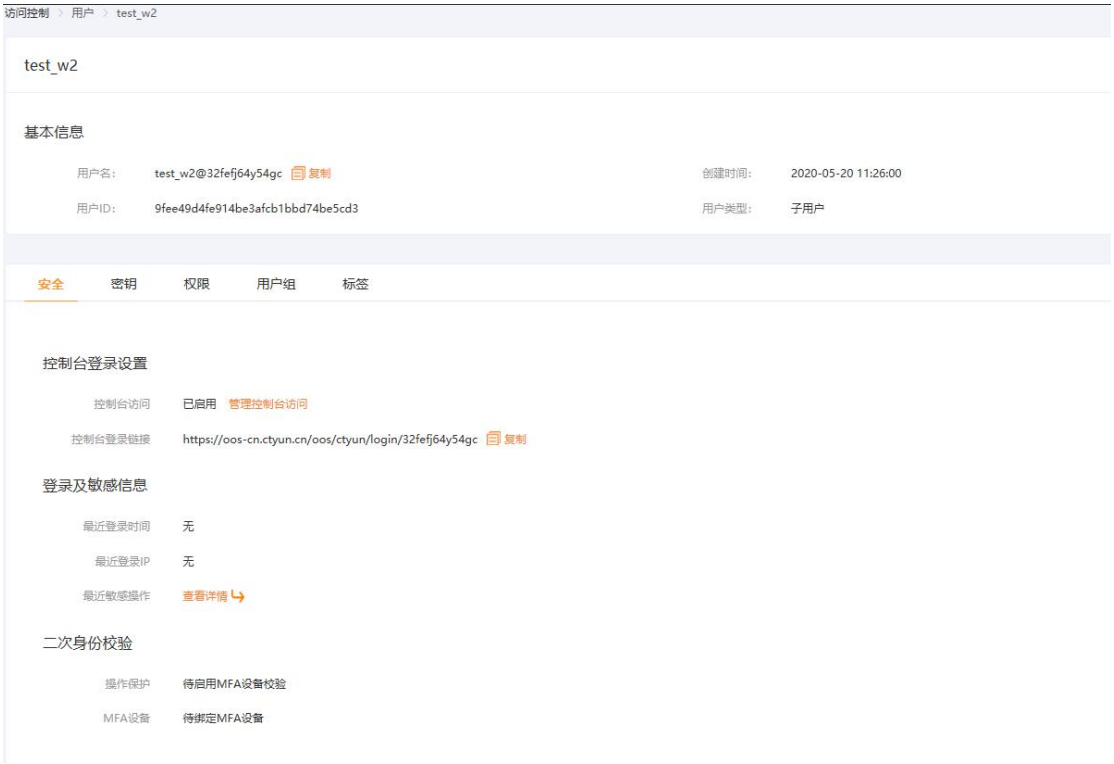
点击对应的**用户名**或者**操作**中的**管理**，查看对应用户的详细信息。

用户基本信息描述

项目	**描述**
用户名	*<子用户名>@<账户 ID>*。 在子用户登录时，用户名使用的是*<子用户名>*。
创建时间	用户创建的时间。
用户 ID	用户 ID。
用户类型	用户类型： ● 根用户 ● 子用户

查看和修改用户安全

点击**安全**，进入**安全**界面，可以对控制台访问方式进行修改，复制子用户控制台登录链接。



点击**管理控制台访问**，可以重新进行控制台登录设置。

控制台登录设置描述

项目	描述
控制台密码登录	控制台密码登录是否开启： ● **开启**：启用控制台密码登录，当前无控制台登录密码时，会生成新登录密码； ● **关闭**：禁用控制台密码登录，删除当前密码。
设置登录新密码	设置新密码方式： ● 保留当前密码：使用用户当前的登录密码，只有

	当前密码存在时才会有此项； ● 重新自动生成密码：系统重新随机生成登录密码； ● 重新设置自定义密码：管理员重新设置登录密码。
重置密码	设置新 IAM 用户在下次登录时是否需要重置密码。若勾选**用户在系统/管理员生成密码，**必须重置密码，即 IAM 用户在下次登录时，必须重置密码。

查看和修改密钥

点击**密钥**，可以对该用户密钥进行**新建、启用/禁用、删除，**

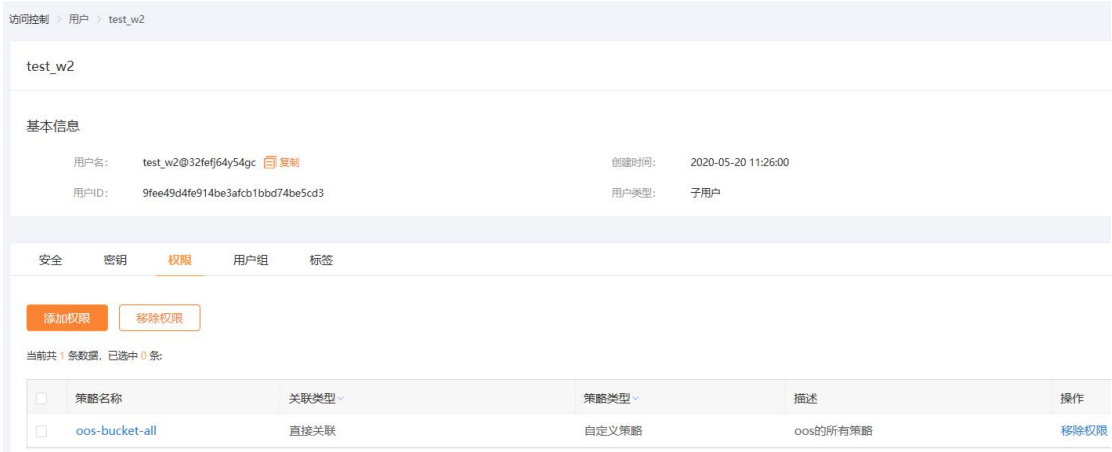
注意：

- 只有密钥少于 2 个时才能**新建密钥（1 个用户最多只能创建 2 个密钥）**。
- 如果用户的密钥丢失，可以对原密钥进行删除，然后通过**新建密钥**的方式获取新的密钥，并进行**密钥下载凭证**。

注意：密钥只能下载一次，关闭弹窗后无法再次看到私有访问密钥的信息。

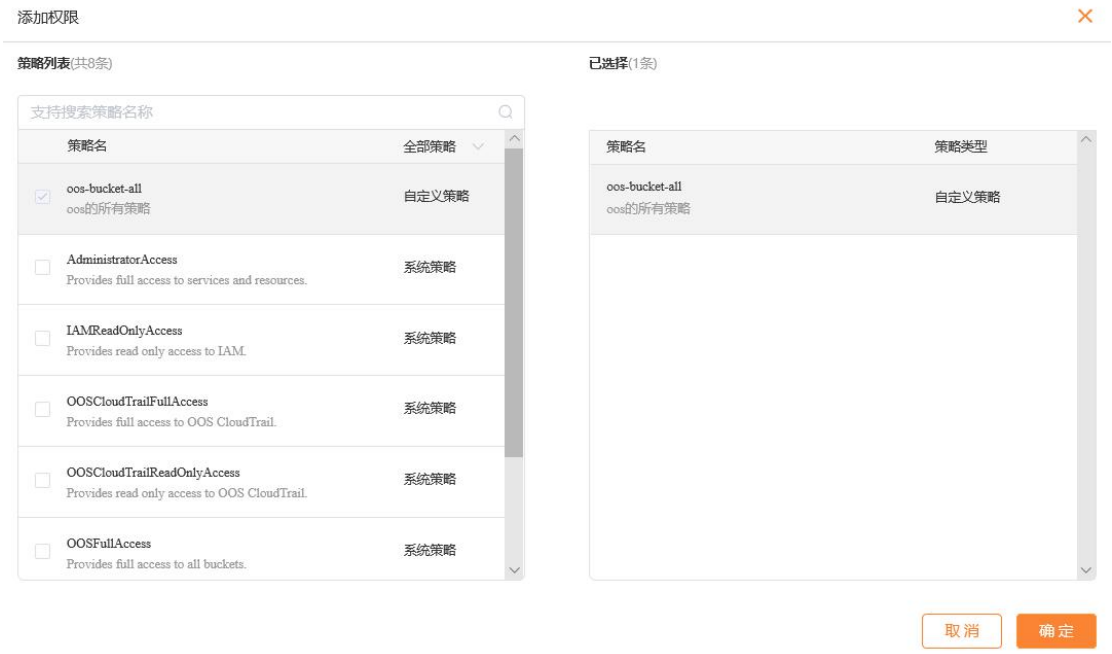
查看和修改权限

点击**权限**，可以查看用户权限、为用户**添加权限、移除权限**和**从组移出：**



- 点击**添加权限**，弹出**添加权限**弹框，可以为用户关联新的策略，弹框中灰色

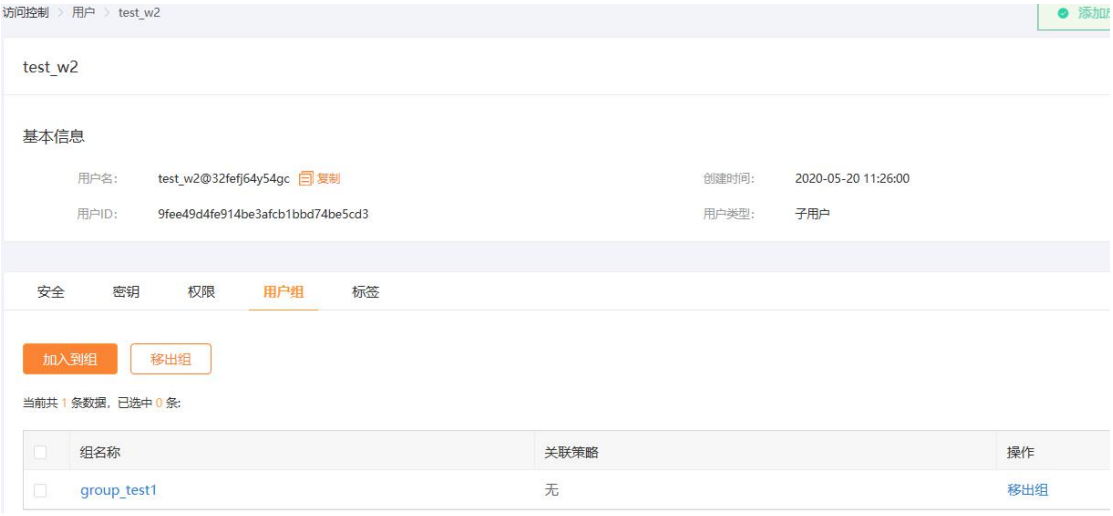
的策略表示用户已关联的策略；



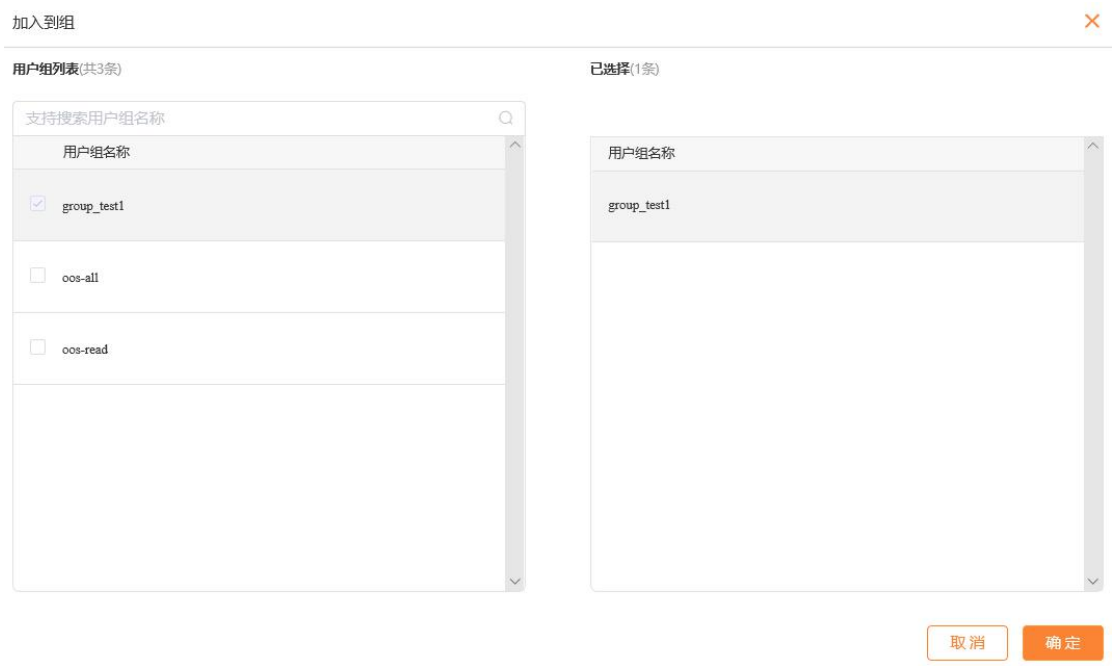
- 选择需要移除的策略，点击**移除权限**，可以为用户删除多条策略；点击对应策略的**移除权限**，可以解除已关联的策略；点击**从组移出**，该用户将移出对应的组，并解除随组关联的策略。

查看和修改用户组

点击**用户组**，可以查看用户所在的组，将用户**加入到组**或**移出组**。



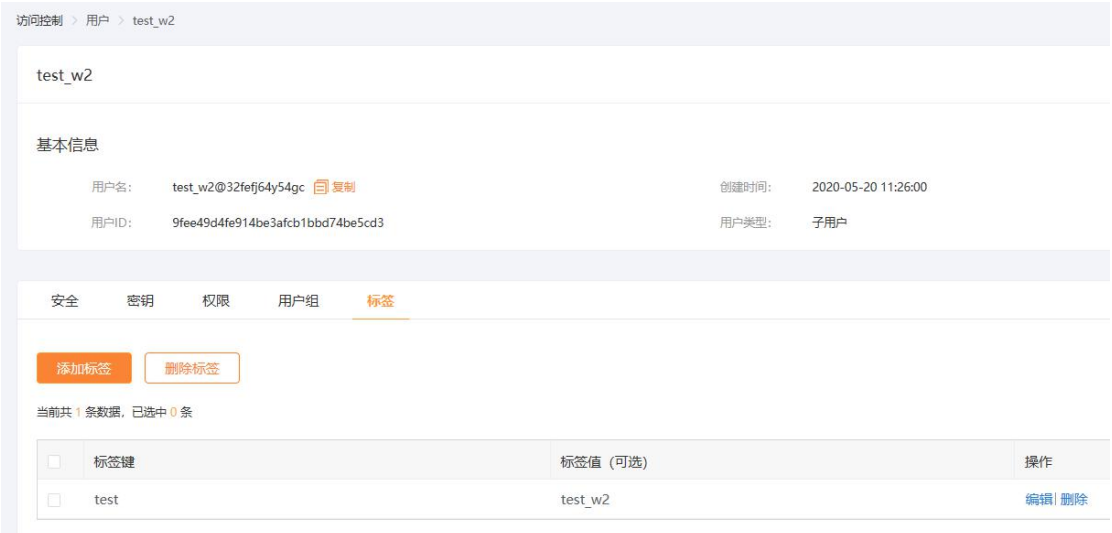
- 点击**加入到组**，弹出**加入到组**弹框，选择用户需要加入的组，点击**确定**。弹框中灰色的用户组表示用户已加入的用户组。



- 选择需要移出的组，点击**移出组**，可以将用户移出多个组；或者点击对应组后的**移出组**，可以将用户从该组移出。

查看和修改标签

点击**标签**，可以为查看用户标签信息、编辑标签信息、为用户**添加标签**或**删除标签**。



- **添加标签**：点击**添加标签**，填写**标签键**和**标签值**。标签值可为空，一个用户最多添加 10 个标签。
- **删除标签**：选择需要删除的标签，点击**删除标签**，可以将多个标签删除；或者点击对应标签的**删除**，可以将该标签删除。
- **编辑标签**：点击标签后的**编辑**，可以修改标签值。

删除用户

选择需要删除的用户，点击**删除**，可以删除多个用户；或者点击对应用户后面的**删除**，删除用户。

删除用户时，会弹出对话框，确认是否删除选中用户。

IAM 子用户登录

根用户或有管理用户权限的 IAM 子用户，通过**用户管理->用户**，进入具体用户页面，在用户详细信息页面，点击**安全**，复制**控制台登录链接**，即得到该子用户的登录链接。

输入用户名和登录密码，根据提示，进行登录。

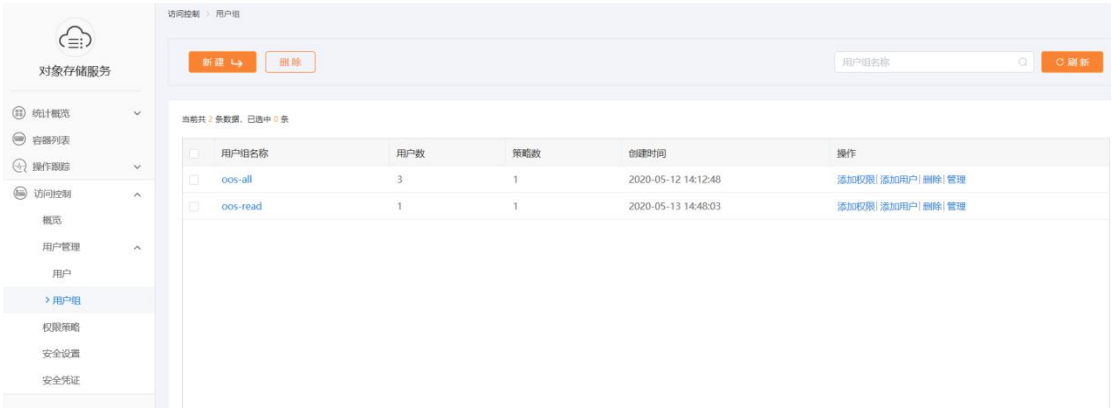
IAM 子用户与根用户的界面基本一致，子用户的功能根据授权而定。如果需要更多权限，可以向根用户进行申请。

IAM 用户组

管理员可以创建用户组，通过给用户组授权，组内的用户可以获得相同的权限策略，方便管理用户。

点击菜单栏中的**用户组列表**，可以：

- 新建用户组；
- 为已建立的用户组添加权限；
- 删除用户组；
- 为用户组添加用户；
- 管理用户组。



创建用户组

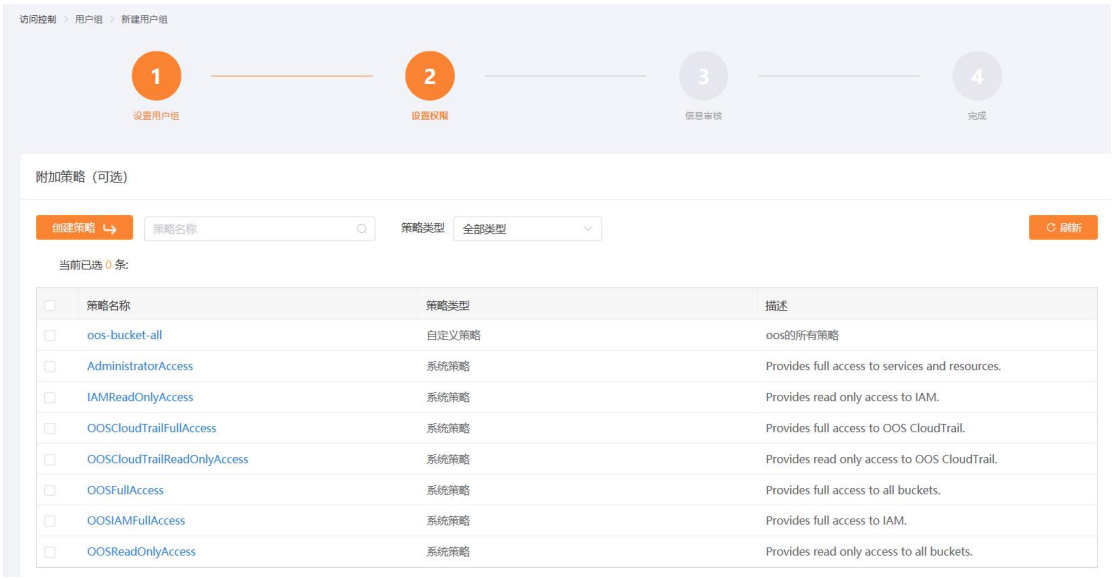
点击**访问控制->用户管理->用户组->新建**，进入**新建用户组**界面，创建用户组。

1. 设置用户组

设置用户组名：用户组名创建成功后，不可进行修改。用户组命名需遵守以下规则：

- 用户组名必须唯一。
- 1~128 位字符串组成，字符只能包含字母、数字或特殊字符，不包含空格。字母不区分大小写，特殊字符只能是：下划线（_）、中划线（-）、逗号（,）、句点（.）、加号（+）、等号（=）和 at 符号（@）。

2. 设置权限



可以在搜索框中搜索匹配策略，搜索出的匹配策略以列表的形式展现出来，可以通过勾选对应策略，为用户组附加策略。

说明：可以创建用户组时为用户组添加策略，也可以用户组创建完成后，再为其添加策略。

注意：每个用户组最多添加 10 条策略。

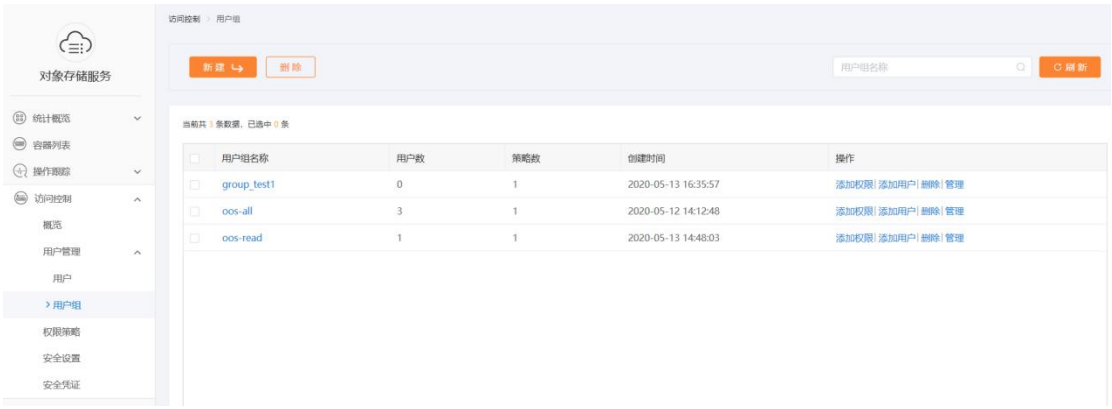
3. 信息审核

对于新建用户组的信息，可以进行审核。如果有需要修改的地方，可以点击编辑图标 进行修改。

4. 完成

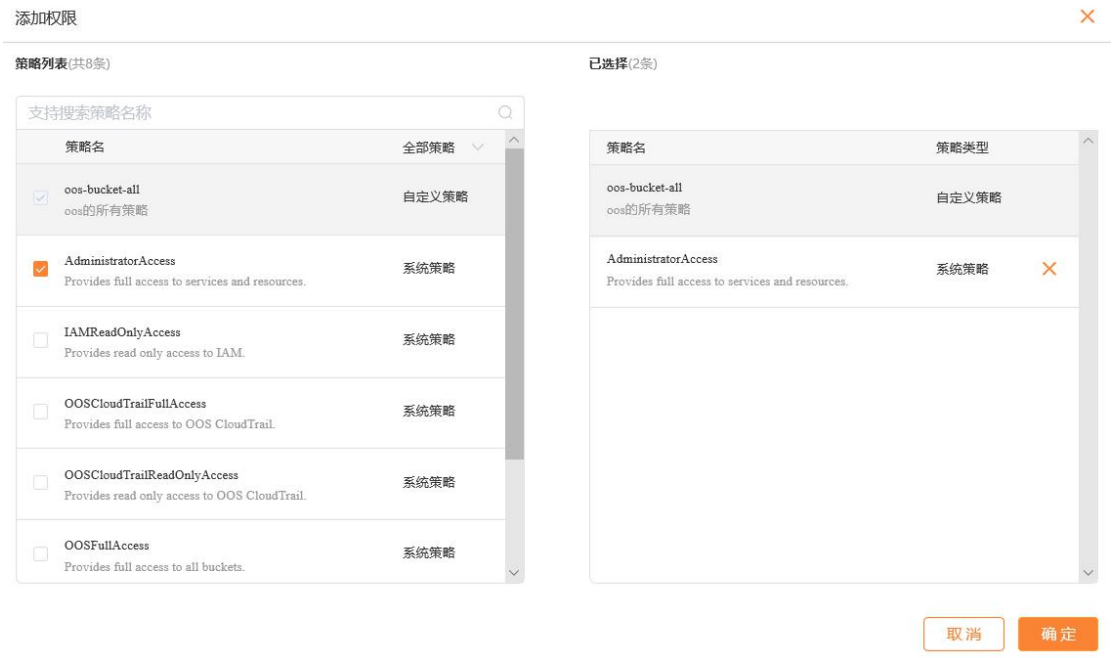
查看和修改用户组信息

点击导航栏中**访问控制->用户管理->用户组**，可以查看和维护用户组信息。

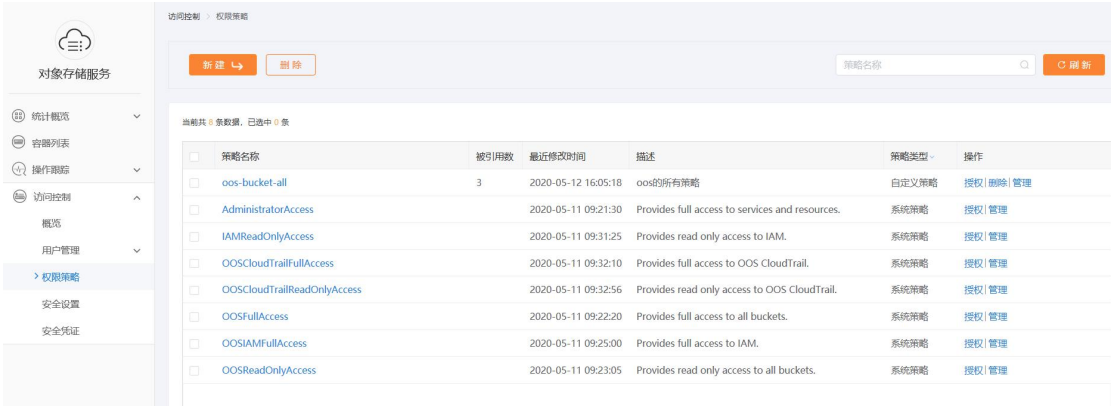


为用户组设置权限

- **添加权限**
  - 在**用户组**界面，点击对应用户组操作中的**添加权限**，弹出**添加权限**界面，为用户组添加策略。弹框中灰色的策略表示用户组已关联的策略。



- 点击对应的用户组名，进入用户组详细信息页，点击**权限->添加权限**，为用户组添加策略。

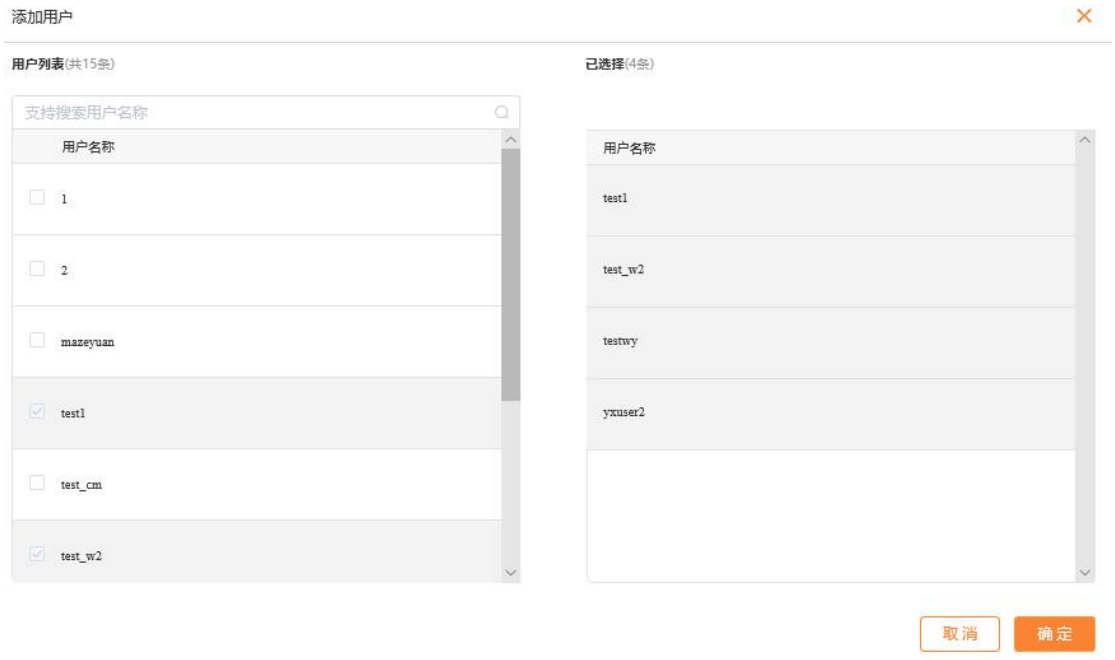


- **移除权限**

在用户组详细信息页，点击**权限**，选择需要移除的策略，点击**移除权限**，可以为用户组删除多条策略；或者点击对应策略后面的**移除权限**，可以为用户组删除对应的策略。

为用户组添加或移出用户

- **添加用户**
  - 在**用户组**界面，点击对应用户组操作中的**添加用户**，弹出**添加用户**界面，为用户组添加用户。



  - 点击对应的用户组名或者**管理**，进入用户组详细信息页，点击**用户->添加用户**，为用户组添加用户。
- **移出用户**

点击对应的用户组名或者**管理**，进入用户组详细信息页，点击**用户**，选择需要移出的用户，点击**移出用户**，可以为用户组删除多个用户；或者点击对应用户后面的**移出用户**，为用户组移出对应用户。

删除用户组

选择需要删除的用户组，点击**删除**，可以删除多个用户组；或者点击对应用户组后面的**删除**，删除用户组。

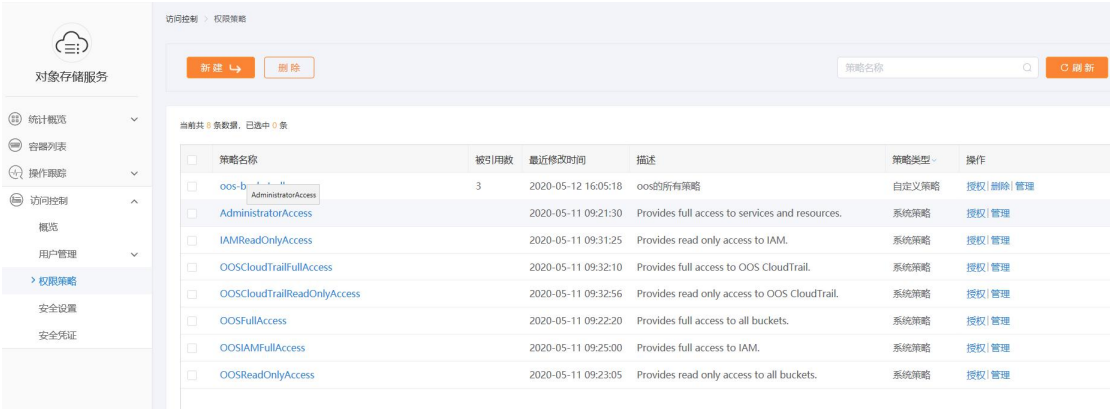
IAM 策略

策略是以 JSON 格式描述权限的信息。管理员创建的 IAM 用户在没有授权策略前是没有任何权限的。只有将策略授权给用户组或者用户，用户才拥有对应的权限。

IAM 支持系统策略和自定义策略：

- 系统策略：天翼云 OOS 预先创建好的策略，用户可以根据自身需求，直接引用。对于系统策略，用户只能使用，不能修改。
- 自定义策略：用户自己创建的策略，用户可以对该类型策略进行修改和删除。

点击菜单栏中的**访问控制->权限策略**，进入权限策略，可以查看策略列表、创建自定义策略、删除自定义策略、对策略进行管理等。



系统策略

目前支持的系统策略有以下几种：

策略名	描述
AdministratorAccess	所有权限，与根用户的权限一样多。
IAMReadOnlyAccess	IAM 相关的 get 和 list 权限。
OOSCloudTrailFullAccess	操作跟踪需要的相关权限，包括： ● OOS：CreateBucket、DeleteBucket、GetBucket、HeadBucket、GetService、GetObject； ● ClouldTrail：所有操作。
OOSCloudTrailReadOnlyAccess	操作跟踪读相关的权限，包括：GetTrailStatus、DescribeTrails、LookupEvents、GetEventSelectors、GetObject、GetService。

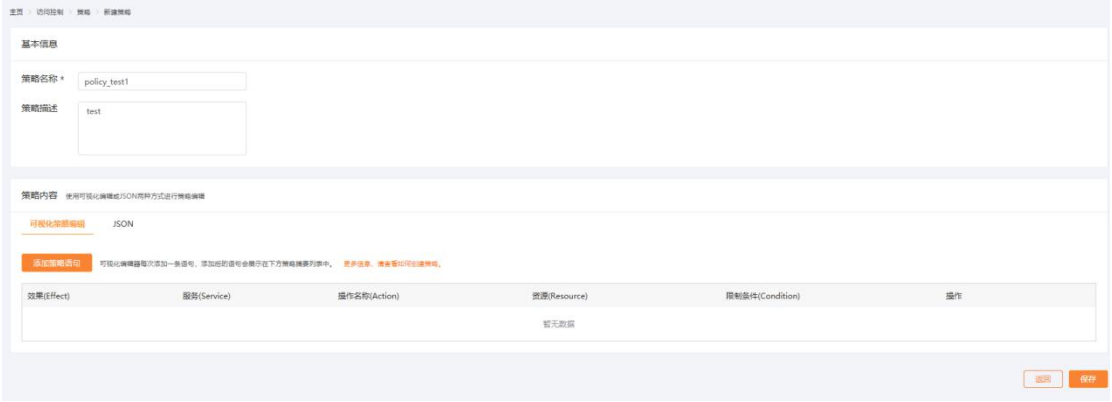
OOSFullAccess	OOS 的所有权限，包括 Bucket 和 Object 的所有操作。
OOSIAMFullAccess	IAM 只读权限，包括 IAM 的 GET、List 相关操作。
OOSReadOnlyAccess	OOS 只读权限，包括 Bucket 和 Object 的 GET、List 相关操作。

自定义策略

新建自定义策略

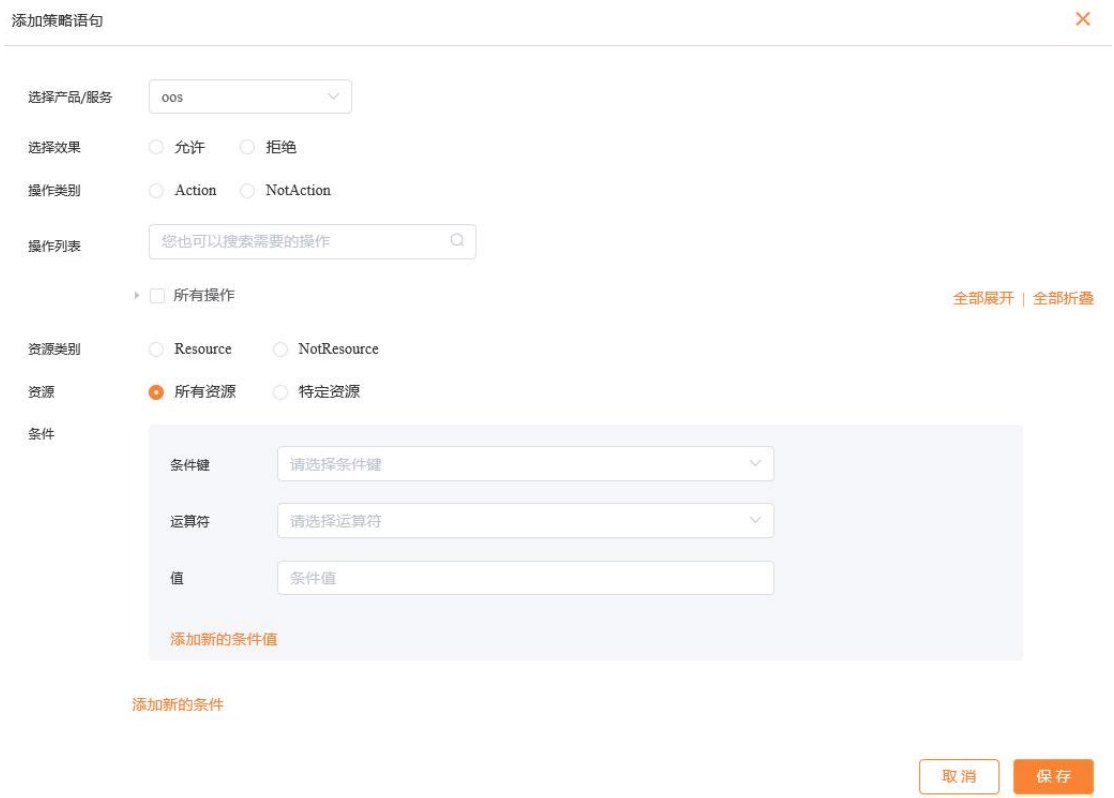
点击**访问控制->权限策略->新建**，进入**新建策略**界面，可以按照下列步骤进行新建策略。

1. **输入策略名称**。策略名需遵循下列规则：
   - 1~128 位字符串组成，字符只能包含字母、数字或特殊字符，不包含空格。字母不区分大小写，特殊字符只能是：下划线（_）、中划线（-）、逗号（,）、句点（.）、加号（+）、等号（=）和 at 符号（@）。
   - 策略名必须唯一。
2. 添加描述（可选）：可以对策略进行概要描述。
3. 添加策略内容，可以通过**可视化策略编辑**或 **JSON** 编程实现。



- **可视化策略编辑**

  点击**添加策略语句**，弹出添加授权语句对话框，可以根据需要，对该策略进行权限配置。



项目	描述
选择产品/服务	可以定义选择服务产品的类型： ➢ oos：对象存储； ➢ cloudtrail：操作跟踪； ➢ statistics：统计； ➢ iam：用户身份管理与访问控制服务。
选择效果	对选择操作的效果： ● **允许**：根据选择的操作类别，对选择的操作效果表现为允许； ● **拒绝**：根据选择的操作类别，对选择的操作效果表现为拒绝。
操作类别	**选择操作的类别。**可以在**搜索框**中模糊搜索或者精准搜索，搜索出的操作会在操作列表中显示。 **操作类别：** ➢ **Action**：对指定的操作匹配； ➢ **NotAction**：与指定的操作之外的其他操作匹配的策略元素。使用 **NotAction** 时： ■ 如果使用**允许**效果，则允许未列出的所有适用操作或服务； ■ 如果使用**拒绝**效果，则拒绝此类未列出的操作或服务。
操作列表	可以在操作列表中选择需要对操作实行的策略。各服务包含的策略见**操作列表**。

资源类别	**资源**是策略生效的实体： ● **Resource**：策略生效的资源。 ● **NotResource**：除指定资源外的其他资源，策略生效。
资源	可以指定**所有资源**，也可以指定**特定资源**。选特定资源时，必须添加具体的资源 ARN。 对于 statistics，无法选择资源，默认**所有资源**。
条件（可选）	用户策略生效的条件。 **注意**：如果条件值输入的是时间，将需要设置的时间转换为 UTC+0 时间。

操作列表

产品/服务	**描述**
OOS	列表： ● ListBucket ● ListAllMyBucket ● GetRegions
	读： ● ListBucketMultipartUploads ● GetBucketAcl ● GetBucketAccelerate ● GetBucketLocation ● GetBucketPolicy ● GetLifecycleConfiguration ● GetBucketWebsite ● GetBucketCORS ● GetBucketLogging ● GetObject ● ListMultipartUploadParts
	写： ● DeleteBucket ● PutLifecycleConfiguration ● PutBucketWebsite ● DeleteBucketWebsite ● PutBucketCORS ● PutBucketLogging ● PutAccelerateConfiguration ● PutObject ● DeleteObject

	● DeleteMultipleObjects ● AbortMultipartUpload ● PutBucket
	权限管理： ● PutBucketPolicy ● DeleteBucketPolicy
cloudtrail	列表： ● DescribeTrails ● LookupEvents
	读： ● GetEventSelectors ● GetTrailStatus
	写： ● PutEventSelectors ● StopLogging ● CreateTrail ● UpdateTrail ● DeleteTrail ● StartLogging
statistics	GetAccountStatistcsSummary
iam	列表： ● GetAccountSummary ● GetLoginProfile ● ListAccessKeys ● ListUsers ● ListUserTags ● ListGroups ● ListGroupsForUser ● ListPolicies ● ListAttachedGroupPolicies ● ListAttachedUserPolicies ● ListEntitiesForPolicy ● ListVirtualMFADevices ● ListMFADevices
	读： ● GetUser ● GetGroup ● GetPolicy

	● GetAccountPasswordPolicy
	写： ● CreateAccessKey ● DeleteAccessKey ● UpdateAccessKey ● CreateUser ● DeleteUser ● TagUser ● UntagUser ● CreateGroup ● DeleteGroup ● AddUserToGroup ● RemoveUserFromGroup ● ChangePassword ● UpdateAccountPasswordPolicy ● DeleteAccountPasswordPolicy ● CreateVirtualMFADevice ● DeleteVirtualMFADevice ● EnableMFADevice ● DeactivateMFADevice ● CreateLoginProfile ● DeleteLoginProfile ● UpdateLoginProfile
	权限： ● CreatePolicy ● DeletePolicy ● AttachUserPolicy ● DetachUserPolicy ● AttachGroupPolicy ● DetachGroupPolicy

条件描述

条件键	运算符	值
ctyun:CurrentTime	● **DateEquals**：匹配指定日期； ● **DateNotEquals**：不等于指定日期； ● **DateLessThan**：早于指定日期；	格式为：yyyy-MM-dd’T’HH:mm:ss’Z’。例如：2019-12-18T09:00:00Z。

	● **DateLessThanEquals**：早于或等于指定日期； ● **DateGreaterThan**：晚于指定日期； ● **DateGreaterThanEquals**：晚于或等于指定日期。	**DateEquals** 和 **DateNotEquals** 精确到天，其他精确到秒。 **注意**：将需要设置的时间转换为 UTC+0 时间。
ctyun:SourceIp	● **IpAddress**：与指定 IP 地址或范围匹配； ● **NotIpAddress**：除指定 IP 地址或范围外的所有 IP 地址匹配。	IPv4：点分十进制格式。 IPv6：32 位 16 进制数，格式为 X:X:X:X:X:X:X:X。 如果指定地址范围，IP 地址后加掩码表示，如 192.163.1.5/3。
ctyun:userid	● **StringEquals**：精准匹配指定的值，区分大小写； ● **StringNotEquals**：与指定的值不匹配，区分大小写； ● **StringEqualsIgnoreCase**：与指定的值精准匹配，不区分大小写。 ● **StringNotEqualsIgnoreCase**：与指定的值不匹配，不区分大小写； ● **StringLike**：与指定的值精准匹配；或通过填充通配符，与指定的值相似，可以包括多字符匹配的通配符 (*) 或单字符匹配的通配符 (?)。区分大小写； ● **StringNotLike**：与指定的值不能进行模糊匹配，区分大小写。	包含数字和小写字母的 32 位字符串。 运算符为 **StringLike** 和 **StringNotLike**，可以包含通配符。
ctyun:username	● **StringEquals**：精准匹配指定的值，区分大小写；	1~64 位字符串组成，字符只能包含

	● **StringNotEquals**：与指定的值不匹配，区分大小写； ● **StringEqualsIgnoreCase**：与指定的值精准匹配，不区分大小写。 ● **StringNotEqualsIgnoreCase**：与指定的值不匹配，不区分大小写； ● **StringLike**：与指定的值精准匹配；或通过填充通配符，与指定的值相似，可以包括多字符匹配的通配符 (*) 或单字符匹配的通配符 (?)。区分大小写； ● **StringNotLike**：与指定的值不匹配，区分大小写。值可以在字符串中的任何位置包括多字符匹配的通配符 (*) 或单字符匹配的通配符 (?)。	字母、数字或特殊字符，字母不区分大小写，特殊字符只能是：下划线（_）、中划线（-）、逗号（,）、句点（.）、加号（+）、等号（=）和 at 符号（@）。 **说明**：运算符为 **StringLike** 和 **StringNotLike**，可以包含通配符。
ctyun:UserAgent	● **StringEquals**：精准匹配指定的值，区分大小写； ● **StringNotEquals**：与指定的值不匹配，区分大小写； ● **StringEqualsIgnoreCase**：与指定的值精准匹配，不区分大小写。 ● **StringNotEqualsIgnoreCase**：与指定的值不匹配，不区分大小写； ● **StringLike**：与指定的值精准匹配；或通过填充通配符，与指定的值相似，可以包括多字符匹配的通配符 (*) 或单字符匹配的通配符 (?)。区分大小写； ● **StringNotLike**：与指定的值不匹配，区分大小写的无效匹配。或通过填充通配符，	字符串，可以包含特殊字符。

	与指定的值也不匹配。	
ctyun:Referer	● **StringEquals**：精准匹配指定的值，区分大小写； ● **StringNotEquals**：与指定的值不匹配，区分大小写； ● **StringEqualsIgnoreCase**：与指定的值精准匹配，不区分大小写。 ● **StringNotEqualsIgnoreCase**：与指定的值不匹配，不区分大小写； ● **StringLike**：与指定的值精准匹配；或通过填充通配符，与指定的值相似，可以包括多字符匹配的通配符 (*) 或单字符匹配的通配符 (?)。区分大小写； ● **StringNotLike**：与指定的值不匹配，区分大小写的无效匹配。或通过填充通配符，与指定的值也不匹配。	字符串，可以包含特殊字符。
ctyun:SecureTransport	**Bool**：布尔匹配。	● **true** ● **false**
ctyun:MultiFactorAuthPresent	**Bool**：布尔匹配。 **说明**：只有 IAM 服务支持此条件键。	● **true** ● **false**
ctyun:MultiFactorAuthAge	● **NumericEquals**：与指定的值相同； ● **NumericNotEquals**：与指定的值不同，否定匹配； ● **NumericLessThan**：小于指定的值； ● **NumericLessThanEquals**：小于等于指定的值； ● **NumericGreaterThan**：大于指定的值； ● **NumericGreaterThanEquals**：大于等于指定的值。	整数形式。

	说明：只有 IAM 服务支持此条件键。	
oos:prefix	● **StringEquals：**精准匹配指定的值，区分大小写； ● **StringNotEquals**：与指定的值不匹配，区分大小写； ● **StringEqualsIgnoreCase：**与指定的值精准匹配，不区分大小写。 ● **StringNotEqualsIgnoreCase**：与指定的值不匹配，不区分大小写； ● **StringLike：**与指定的值精准匹配；或通过填充通配符，与指定的值相似，可以包括多字符匹配的通配符 (*) 或单字符匹配的通配符 (?)。区分大小写； ● **StringNotLike**：与指定的值不匹配，区分大小写。值可以在字符串中的任何位置包括多字符匹配的通配符 (*) 或单字符匹配的通配符 (?)。	字符串形式。 说明：本条件键仅对 ListBucket 生效。
oos:x-amz-acl	● **StringEquals：**精准匹配指定的值，区分大小写； ● **StringNotEquals**：与指定的值不匹配，区分大小写； ● **StringEqualsIgnoreCase：**与指定的值精准匹配，不区分大小写。 ● **StringNotEqualsIgnoreCase**：与指定的值不匹配，不区分大小写； ● **StringLike：**与指定的值精准匹配；或通过填充通配符，与指定的值相似，可以包括多字符匹配的通配符 (*) 或单字符匹配的通配符 (?)。区分大小写；	字符串形式。 取值为： ● private：私有 ● public-read：只读 ● public-read-write：公有 说明：创建 Bucket 时，通过使用此条件键可以控制存储桶 ACL 的类型，本条件键仅对 PutBucket 生效。

	● **StringNotLike**：与指定的值不匹配，区分大小写。值可以在字符串中的任何位置包括多字符匹配的通配符 (*) 或单字符匹配的通配符 (?)。	

- JSON 编程授权

可以使用 JSON 语言对策略内容进行添加。以下列策略为例，说明 JSON 编程策略的语法结构。

```
{
  "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 编程参数表

参数	含义	值
Version	策略的版本	2012-10-17

Statement：策略的授权语句。 Statement 可以有多个，表示不同的授权结构。	**Effect**：效果	定义操作的选择效果	● **Allow**：允许执行； ● **Deny**：拒绝执行。 **说明**：当同一个 Action 中的 Effect 同时包含 Allow 和 Deny 时，遵循 Deny 优先的原则。
	● **Action**：对操作的类别显性匹配； ● **NotAction**：与指定的操作之外的其他操作显性匹配。 **说明**：对于一个 Statement，Action 和 NotAction 二选一	定义操作的类别	**格式为**： ● **服务名**： ➢ **oos**：对象存储； ➢ **cloudtrail**：操作跟踪； ➢ **statistics**：管理 API； ➢ **iam**：访问控制。 ● **操作列表**：见**操作列表**。
	● **Resource**：策略生效的资源； ● **NotResource**：除指定资源外，策略生效。	资源类别	**格式可以为**： ● arn:ctyun:*service*::*accountid*:*resource* ● arn:ctyun:*service*::*accountid*:*resourcetype/resource* **其中**： ● service：服务名； ● accountid：账户 ID； ● resource：具体资源。在指定资源时，可以使用通配符，其中*表示字符的任意组合，？表示任何单个字符；例如 oos 可以表示为：arn:ctyun:oos::accountID:bucket/object，其中 bucket 和 object 为用户实际的资源名称。 ● resourcetype：资源类型。可以使用*表示所有资源类型。根据服务不同，对应的 resourcetype 不同： ■ iam 的 resourcetype 可以为：user、

			group、policy、mfa 或*； ■ cloudtrail 的 resourcetype 可以为：trail 或*； ■ statistics 的 resourcetype 可以为：*。
	Condition：条件	策略生效的条件	**格式为：** 条件运算符:{条件名:[条件值 1,条件值 2]} **说明：一个 Condition 可以包含多个条件运算符，一个条件运算符又可以包含一个条件名和多个条件值。**

- **…IfExists 条件运算符**

IfExists：如果请求的内容中存在关键字，则依照策略所述的条件来处理关键字。如果该关键字不存在，则条件元素的计算结果将为 true。

目前仅 Bool 型和数字类型的运算符支持使用 IfExists 条件运算符，表达形式：*运算符* IfExists，例如 BoolIfExists、NumericEqualsIfExists。对于…IfExists 的使用见示例 1 和示例 2。

示例 1

- 拒绝没有使用 MFA 认证的控制台请求，不拒绝使用 MFA 认证的控制台请求和使用密钥的 API 请求。但如果允许使用 MFA 认证的控制台请求和使用密钥的 API 请求，需要再写显性允许语句。

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

- 拒绝没有使用 MFA 认证的控制台请求及使用密钥的 API 请求，不拒绝 MFA 认证的控制台请求。但如果允许 MFA 认证的控制台请求，需要再写显性允许语句。

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

示例 2

- 允许使用 MFA 认证在 1800 秒内的请求及使用密钥的 API 请求。

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

- 允许使用 MFA 认证在 1800 秒内的请求，但不允许 MFA 认证超过 1800 秒以上及没有使用 MFA 的请求（包括 API 请求）。

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

修改自定义策略

- **策略内容**

点击**权限策略->*策略名称*->策略内容->编辑策略**，弹出编辑策略界面，可以通过**可视化策略编辑器**或 **JSON** 对策略进行编辑，具体编辑方法见**新建策略**和**策略语法结构**。

删除自定义策略

点击导航栏的**权限策略**，进入权限策略页面。选择需要删除的策略进行勾选，点击**删除策略**，可以删除未关联用户和用户组的策略。

点击**操作**中的**删除**，可以删除该策略。

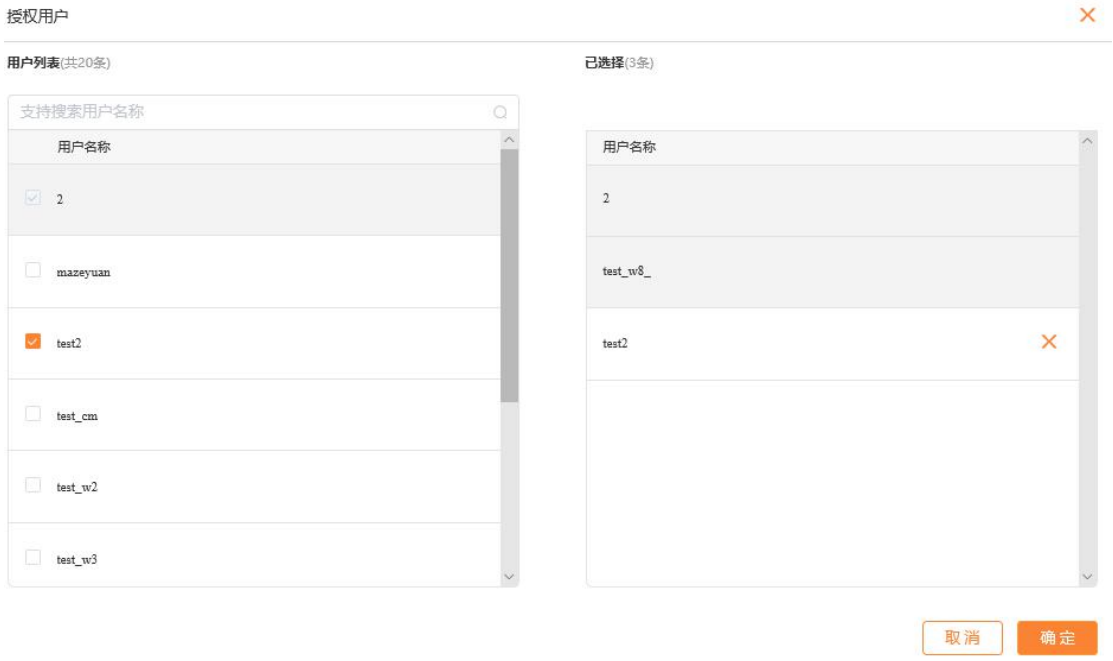
查看策略基本信息

在**权限策略**页面，点击***策略名***或者**管理**，可以进入具体策略页面，在该页面可以查看策略的基本信息和修改策略。

策略基本信息包含：策略名称、策略类型、创建时间、最近修改时间、描述。

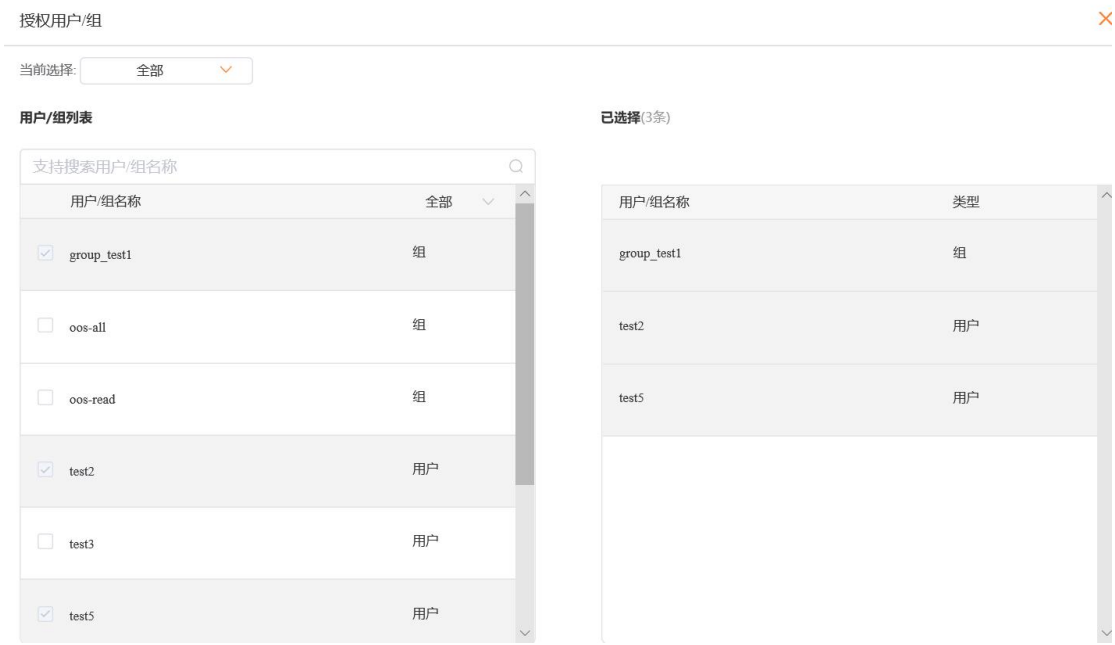
授权用户

在**权限策略**页面，点击**授权用户**，弹出**授权用户**页面。选择需要授权的用户，可以为用户进行授权。弹框中灰色的用户表示已关联该策略的用户。



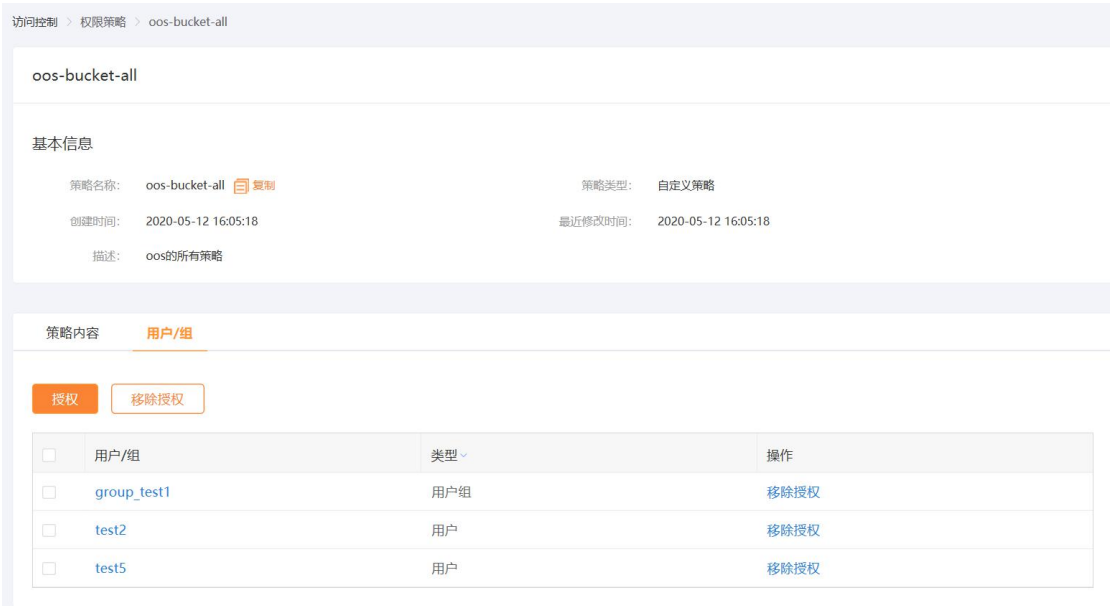
- **授权用户/组**

在**权限策略**页面，点击**授权**，弹出**授权用户/组**页面。选择需要授权的用户或用户组，可以为其进行授权。弹框中灰色的用户组表示已关联该策略的用户或用户组。



- **查看授权用户/组**

在权限策略页，点击对应策略或者策略后的**管理**，进入对应策略详情页，可以在**用户/组**，查看当前策略已关联的用户和用户组，同时可以为用户或用户组进行**授权**和**移除授权**。



安全设置

点击导航栏中的**安全设置**，可以进行**密码安全设置**。

编辑密码规则

点击编辑密码规则，可以对密码规则进行重新设置。

项目	描述
密码长度	可以设置用户的密码长度，取值范围是 8~128 的整数。
密码中必须包含元素	用户可以选择下列的任意一项或者多项： ●大写字母：A~Z；

	●小写字母：a~z； ●数字：0~9； ●非字母数字字符，包括：!@#$%^&*()_+-=[]{}|' 如果不选，使用默认规则，即密码中必须包含小写字母和数字。
密码有效期	密码有效天数，整数形式，取值范围为 0~1095，0 表示永不过期。
自主管理密码	● 如果勾选用户自主管理密码，允许 IAM 用户自主修改密码； ● 如果未勾选用户自主管理密码，只能管理员来修改密码。
密码过期后	● 限制用户登录，允许用户重置密码：密码过期后，用户可以自行修改密码； ● 限制用户登录，须由管理员重置密码：密码过期后，用户不能执行修改密码。
历史密码检验策略	在重置密码时对历史密码进行检查，禁止使用设置次数前的密码。整数形式，取值范围为 0~24，0 表示不启用历史密码检验策略，但当前密码不属于历史密码，故新设置的密码不能与当前密码相同。 历史密码为除当前密码外，历史使用过的密码。例如设置**历史检验策略**为 1，当前密码为 Password1，前一次的密码为 Password0，用户希望设置的新密码为 Password2，则 Password2 不能与前一次密码 Password0 和当前密码 Password1 相同。

自主管理密码和密码过期后之间的关系如下表所示：

项目	**勾选用户自主管理密码**	**不勾选用户自主管理密码**
限制用户登录，允许用户重置密码	任何时候，IAM 用户都可以自己修改密码。	只能密码过期后，允许 IAM 修改一次密码。
限制用户登录，不允许用户重置密码	任何时候，控制台用户无法修改密码，可以通过 API 进行修改。	IAM 用户任何时候都不能自行修改密码。

清除密码规则

点击**清除密码规则**，将改为默认密码规则，默认密码规则为：

- 密码长度：8-128 位；
- 密码中必须包含元素：小写字母、数字；
- 密码有效期：永久；
- 自主管理密码：允许用户自主管理密码；
- 密码过期后：不需要管理员重置；
- 历史密码检查策略：不启用历史密码检查策略，但用户更改密码时，新

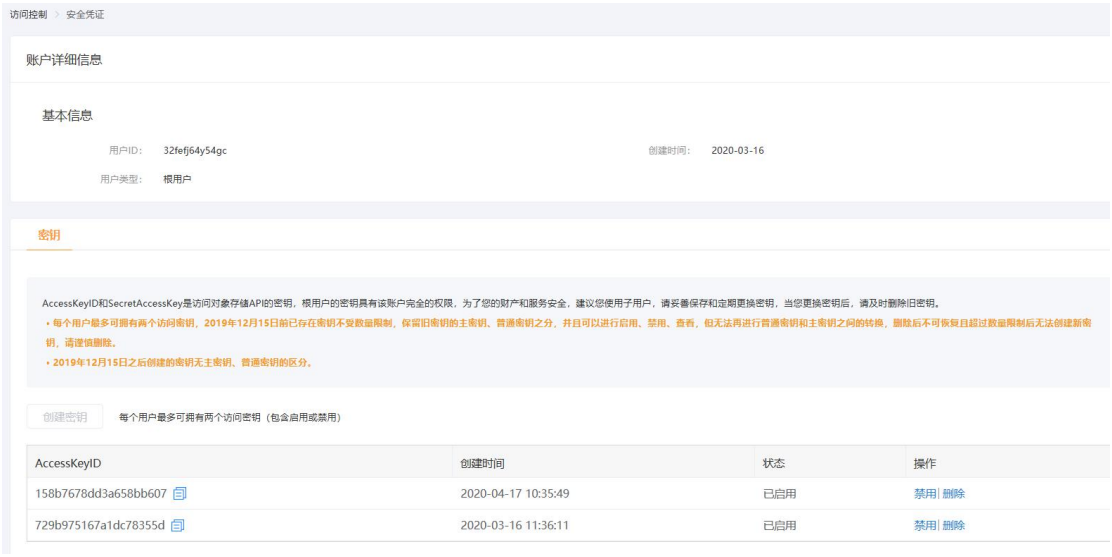
密码不能与当前密码相同，因为当前密码不属于历史密码。

安全凭证

密钥

在菜单栏，点击**安全凭证**，可以查看账户详细信息的安全凭证信息，包括：用户 ID、创建时间、用户类型、密钥。

注意：一个用户最多拥有 2 个访问密钥，如果将访问密钥全部删除，则该用户不能使用删除的 AK/SK 进行签名。



密钥描述

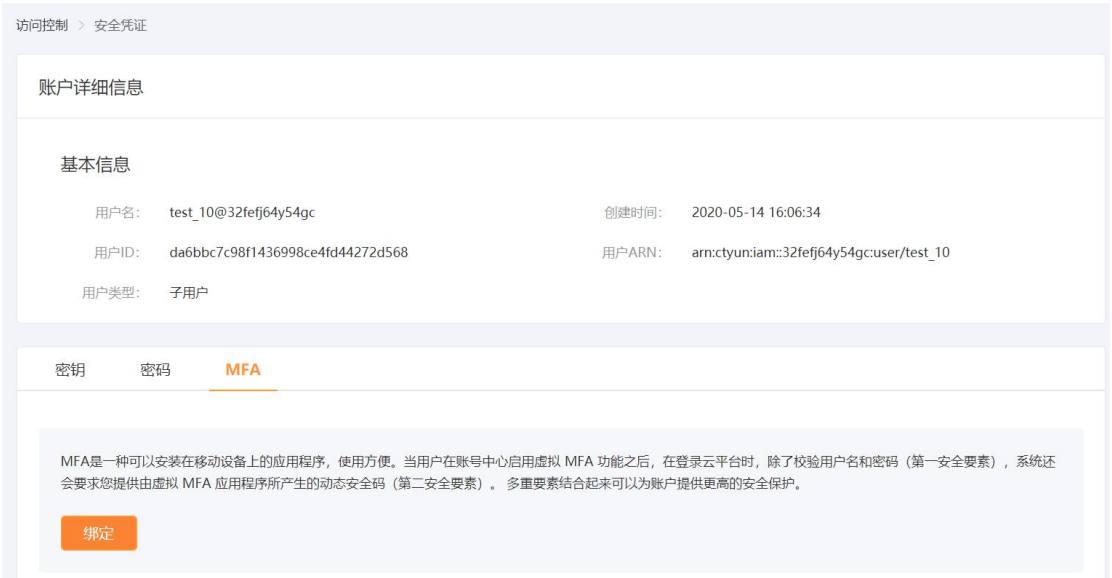
项目	描述
AccessKeyID	密钥 ID。点击，可以对密钥 ID 进行复制。
SecretAccessKey	密钥值，点击，可以查看密钥值的明文形式。 **说明**：在 IAM 上线之前创建的密钥有此项。
创建时间	密钥创建时间。 **无**：表示该密钥是在 IAM 功能上线前创建的。
密钥类型	● **主密钥** ● **普通密钥** **说明**：在 IAM 上线之前创建的密钥有此项。
状态	密钥启用状态： ● **已启用** ● **已禁用**
操作	可以对密钥进行操作： ● **禁用** ● **删除**

密码

只有具有更改密码权限用户的子用户才能进行更改密码。根用户的密码通过天翼云页面修改。

MFA

MFA 认证仅子用户支持，但是如果没有授权使用 MFA 认证，则子用户无法进行 MFA 认证。具有 MFA 授权的用户，可以在**安全凭证->MFA** 页面，进行 MFA 绑定。



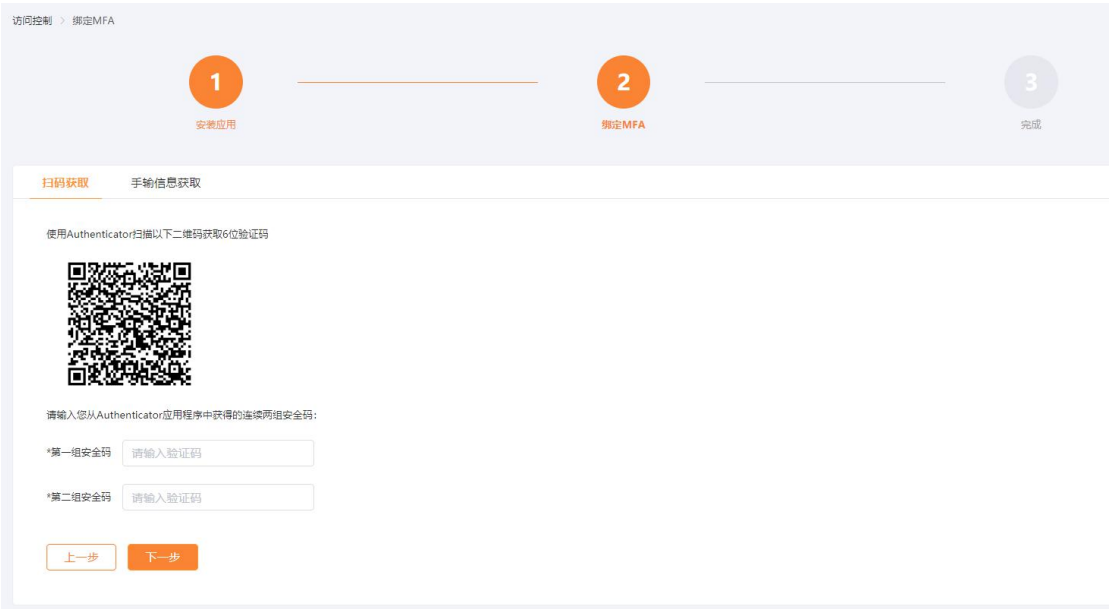
MFA 绑定步骤如下：

1. 点击**绑定**，进入 **MFA 绑定**页面。

说明：您需要在手机端安装基于时间的一次性密码（TOTP）口令认证工具。

2. 绑定 MFA：可以使用**扫码获取**，和**手动信息获取**。

   注意：输入的**第一组安全码**和**第二组安全码**必须是连续的。



3. 绑定完成。

   注意：如果您后续不再使用 MFA，并希望卸载已安装的动态口令工具，请先解绑已绑定的 MFA 设备。如果您再未解绑 MFA 的情况下卸载动态口令工具，可能会造成相关用户不可用，请慎重操作。


访问控制 > 绑定MFA
1
安装应用
2
绑定MFA
3
完成
绑定完成
您已成功绑定MFA设备
请注意，如您后续不再使用MFA，并希望卸载已安装的动态口令工具，请先解绑已绑定的MFA设备。如您在未解绑MFA的情况下，卸载动态口令工具，可能会造成相关用户不可用，请谨慎操作！
返回

IAM 最佳实践

安全管理

- **创建独立的 IAM 子用户**

  一个账户可以建立多个子用户，您可以通过 IAM 为不同的操作人员创建独立的 IAM 子用户。根据操作人员的职能范围，授予相应的管理权限。同时建议您也为根用户创建子用户，并授予该子用户管理权限，使用该用户进行日常管理工作，保护账户安全。

- **控制台登录用户与编程用户分离**

  建议通过控制台登录用户与编程用户分离，以便更好的分配权限：

  - 控制台登录用户：通过控制台登录的用户，只需设置控制台登录密码。
  - 编程用户：通过 API 访问的用户，只需创建访问密钥。

- **分组进行授权**

  账户有多个用户时，通过用户组将用户进行分类，同类权限的用户分到一组。通过为用户组授权，使组内用户获取用户组具有的权限。

- **授予最小权限**

  建议您为 IAM 用户授予最小权限，您可以使用 IAM 用户制定策略，给 IAM 用户仅授予完成工作所需的权限，通过授予最小权限，可以帮您安全的控制 IAM 用户对 OOS 的管理。

- **为 IAM 用户配置强密码策略**

  通过 IAM 可以为控制台登录的用户设置强密码策略。例如密码最小长度、密码中必须包含元素、密码不与历史密码相同、强制定期更换密码等，确保用户使用复杂度高的强密码。

- **开启 MFA 认证**

  为 IAM 用户开启多因素认证（Multi-factor authentication，MFA），提高账号的安全性，在用户名和密码之外再增加一层安全保护。

- **使用策略限制条件**

  您可以在 IAM 策略中设置用户在特定时间、特定请求 IP 的条件下才能操作指定的 OOS 资源，而其他情况下不能操作。

- **根账户不使用访问密钥**

  由于根账户对名下资源有完全的控制权，为了避免因访问密钥泄露带来的风险，不建议根用户使用访问密钥。

  建议您创建子用户，并授予该子用户管理权限，使用该用户进行日常管理工作，保护账户安全。

- **开启操作跟踪功能**

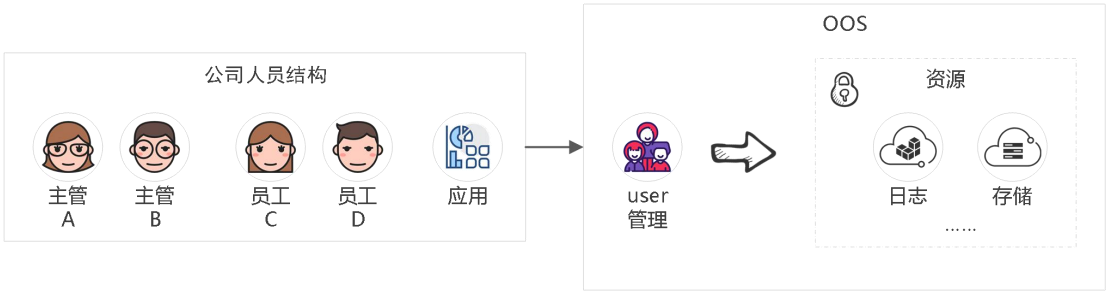
  开启 OOS 的操作跟踪功能，记录用户在账户中做了哪些操作、使用了哪些资源。操作跟踪日志会记录操作的类型、时间、操作的源 IP、操作人员等，并且可以长久的保存在 OOS 存储桶中。

将 IAM 与操作跟踪功能结合使用，您可以从控制和监控两个层面进行账户管理。

用户管理示例

某公司有多个员工需要访问、操作存储资源，由于每个员工的工作职责不同，需要的权限也不同：

- 将控制台登录用户和编程用户区分；
- 可以根据不同的职能为用户分配权限；
- 只有管理员可以进行较为敏感的日常操作；
- 不同的管理人员可以查看不同方面的保密数据。



目前该公司希望：

- 主管 A 和主管 B 均有保密数据的查看权限；
- 主管 A 可以在 MFA 认证的情况下对 IAM 用户进行管理和变更；
- 主管 B 可以进行操作跟踪管理，查看账户的操作记录；
- 员工 C 和员工 D 可以查看存储桶对象；
- 编程用户可以对存储桶上传对象。

创建用户组并关联策略

IAM 用户组	**包含用户**	**策略说明**
保密数据权限组	主管 A 和主管 B	查看 secretBucket 内的保密数据，但不可以更改。
IAM 管理组	主管 A	可以进行 IAM 的相关管理操作。
操作跟踪管理组	主管 B	可以进行操作跟踪的相关管理操作，查看操作跟踪 Bucket 中的数据。
查看存储对象组	员工 C 和员工 D	查看上传对象权限。
上传对象组	编程用户	通过 API 可以向指定的 Bucket 内写入数据。

保密数据组权限策略示例：

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowGroupToSeeBucket",
      "Action": [
        "oos:ListBuckets",
        "oos:Get*"
      ],
      "Effect": "Allow",
      "Resource": [
//secretBucket 的存储桶资源
        "arn:ctyun:oos::10rc2arpn6306:secretBucket",
//存储桶 secretBucket 下所有对象
        "arn:ctyun:oos::10rc2arpn6306:secretBucket/*"
          ]
        }
      ]
    }
```

IAM 管理组策略示例

```
    {
        "Version": "2012-10-17",
        "Statement": [
            {
                "Sid": "AllowGroupToManageIAM",
                "Effect": "Allow",
                "Action": "iam:*",
                "Resource": "*",
                "Condition": {
                    "Bool": {
                        "ctyun:MultiFactorAuthPresent": "true"
                    }
                }
            }
        ]
}
```

操作跟踪管理组策略示例

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

查看对象组策略示例

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

```
    }
```

上传对象组策略示例

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

附录

域名（Endpoint）列表

OOS 对象存储网络中的各个地区，使用统一的 OOS API、统计、操作跟踪和 IAM API 的 Endpoint。用户也可以指定使用某个资源池的 Endpoint，这样可以直接定位到该资源池。Endpoint 列表如下：

OOS API Endpoint: oos-cn.ctyunapi.cn，支持 HTTP 和 HTTPS。

统计 API Endpoint: oos-cn-mg.ctyunapi.cn，支持 HTTP 和 HTTPS。

操作跟踪 API Endpoint：oos-cn-cloudtrail.ctyunapi.cn，支持 HTTPS。

IAM Endpoint: oos-cn-iam.ctyunapi.cn，支持 HTTPS。

OOS 对象存储具体资源池 Endpoint 如下：

地区	OOS API Endpoint
郑州	oos-hazz.ctyunapi.cn
沈阳	oos-lnsy.ctyunapi.cn
四川成都	oos-sccd.ctyunapi.cn
乌鲁木齐	oos-xjwlmq.ctyunapi.cn
甘肃兰州	oos-gslz.ctyunapi.cn
山东青岛	oos-sdqd.ctyunapi.cn
贵州贵阳	oos-gzgy.ctyunapi.cn
湖北武汉	oos-hbwh.ctyunapi.cn
西藏拉萨	oos-xzls.ctyunapi.cn
安徽芜湖	oos-ahwh.ctyunapi.cn
广东深圳	oos-gdsz.ctyunapi.cn
江苏苏州	oos-jssz.ctyunapi.cn
上海 2	oos-sh2.ctyunapi.cn

除对象存储网络外，其他地域的 Endpoint 列表如下。

地区	OOS API Endpoint
北京 2	oos-bj2.ctyunapi.cn

内蒙	oos-nm2.ctyunapi.cn
长沙	oos-hncs.ctyunapi.cn
西安	oos-snxa.ctyunapi.cn
杭州	oos-hz.ctyunapi.cn
江苏	oos-js.ctyunapi.cn
广州	oos-gz.ctyunapi.cn
北京	oos-hq-bj.ctyunapi.cn
上海	oos-hq-sh.ctyunapi.cn

操作权限与 API 对应关系

表 1　OOS 的操作权限与 API 对应关系

操作权限		API
Bucket 列表	ListBucket	GET Bucket（List Object）、HEAD Bucket
	ListAllMyBucket	GET Service
	GetRegions	GET Regions
Bucket 读取	ListBucketMultipartUploads	List Multipart Uploads
	GetBucketAcl	GET Bucket acl
	GetBucketAccelerate	GET Bucket accelerate
	GetBucketLocation	GET Bucket location
	GetBucketPolicy	GET Bucket policy
	GetLifecycleConfiguration	GET Bucket lifecycle
	GetBucketWebsite	GET Bucket website
	GetBucketCORS	GET Bucket cors
	GetBucketLogging	GET Bucket logging
	GetBucketObjectLockConfiguration	GetBucketObjectLockConfiguration
Bucket 写入	PutBucket	PUT Bucket
	DeleteBucket	DELETE Bucket
	DeleteMultipleObjects	DELETE Multiple Objects
	PutLifecycleConfiguration	PUT Bucket lifecycle、DELETE Bucket lifecycle
	PutBucketWebsite	PUT Bucket website
	DeleteBucketWebsite	DELETE Bucket website
	PutBucketCORS	PUT Bucket cors、DELETE Bucket cors
	PutBucketLogging	PUT Bucket logging
	PutAccelerateConfiguration	PUT Bucket accelerate
	PutBucketObjectLockConfiguration	PutBucketObjectLockConfiguration
	DeleteBucketObjectLockConfiguration	DeleteBucketObjectLockConfiguration
Bucket 权限	PutBucketPolicy	PUT Bucket policy
	DeleteBucketPolicy	DELETE Bucket policy
Object 读取	ListMultipartUploadParts	List Parts
	GetObject	GET Object、HEAD Object
Object 写入	PutObject	PUT Object、PUT Object-Copy、POST Object、Initiate Mulitipart Upload、Upload Part、Compelete Multipart Upload、Upload Part – Copy
	DeleteObject	DELETE Object

	AbortMultipartUpload	Abort Multipart Upload

表 2　统计的操作权限与 API 对应关系

操作权限	API
GetAccountStatistcsSummary	GET Capacity、GET DeleteCapacity、GET Traffics、GET AvailableBandwidth、GET Requests、GET RetarnCode、GET ConcurrentConnection、GET Usage、GET AvailBW、GET Bandwidth、Get Connection

表 3　操作跟踪的操作权限与 API 对应关系

操作权限		API
列表	DescribeTrails	DescribeTrails
	LookupEvents	LookupEvents
读取	GetEventSelectors	GetEventSelectors
	GetTrailStatus	GetTrailStatus
写入	PutEventSelectors	PutEventSelectors
	StopLogging	StopLogging
	CreateTrail	CreateTrail
	UpdateTrail	UpdateTrail
	DeleteTrail	DeleteTrail
	StartLogging	StartLogging

表 4　IAM 的操作权限与 API 对应关系

操作权限		API
列表	GetAccountSummary	GetAccountSummary
	GetLoginProfile	GetLoginProfile
	ListAccessKeys	ListAccessKeys
	ListUsers	ListUsers
	ListUserTags	ListUserTags
	ListGroups	ListGroups
	ListGroupsForUser	ListGroupsForUser
	ListPolicies	ListPolicies
	ListAttachedGroupPolicies	ListAttachedGroupPolicies
	ListAttachedUserPolicies	ListAttachedUserPolicies
	ListEntitiesForPolicy	ListEntitiesForPolicy
	ListMFADevices	ListMFADevices
	ListVirtualMFADevices	ListVirtualMFADevices
读取	GetUser	GetUser
	GetGroup	GetGroup
	GetPolicy	GetPolicy
	GetAccountPasswordPolicy	GetAccountPasswordPolicy

写入	CreateAccessKey	CreateAccessKey
	DeleteAccessKey	DeleteAccessKey
	UpdateAccessKey	UpdateAccessKey
	CreateUser	CreateUser
	DeleteUser	DeleteUser
	TagUser	TagUser
	UntagUser	UntagUser
	CreateGroup	CreateGroup
	DeleteGroup	DeleteGroup
	AddUserToGroup	AddUserToGroup
	RemoveUserFromGroup	RemoveUserFromGroup
	ChangePassword	ChangePassword
	UpdateAccountPasswordPolicy	UpdateAccountPasswordPolicy
	DeleteAccountPasswordPolicy	DeleteAccountPasswordPolicy
	CreateVirtualMFADevice	CreateVirtualMFADevice
	DeactivateMFADevice	DeactivateMFADevice
	DeleteVirtualMFADevice	DeleteVirtualMFADevice
	EnableMFADevice	EnableMFADevice
	CreateLoginProfile	CreateLoginProfile
	DeleteLoginProfile	DeleteLoginProfile
	UpdateLoginProfile	UpdateLoginProfile
权限	CreatePolicy	CreatePolicy
	DeletePolicy	DeletePolicy
	AttachUserPolicy	AttachUserPolicy
	DetachUserPolicy	DetachUserPolicy
	AttachGroupPolicy	AttachGroupPolicy
	DetachGroupPolicy	DetachGroupPolicy

IAM 策略编写规则

Version

Version 策略元素用在策略之中，用于定义策略语言的版本，包含在所有策略中的 Statement 元素之前。

目前 OOS IAM 在用的策略版本为：2012-10-17，兼容 AWS 最新策略版本。

如果未包含 Version 元素，则此值默认为 2012-10-17。

Statement

Statement 为策略的主要元素，该元素为必填项。Statement 中可含一条单独的 JSON 语句，也可包含由多条语句组成的 JSON 语句块。每条单独的语句块必须使用大括号{}括起来。每个 JSON 语句块中包括下列元素：Sid（非必填）、Effect（必填）、Action 或 NotAction（二选一）、Resource 或 NotResource（二选一）、Condition（非必填）。

Statement 语句的结构如下：

```
“Statement”: [ {…}, {…}, {…}, …]
```

例如下例为多个 JSON 语句块组成的示例：

```
{
    "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/*"
```

```
            ]
        }
    ]
}
```

Sid

Sid 是针对策略语句提供的可选标识符，用户可以为声明数组中的每份声明指定 Sid 值，Sid 值是策略文件 ID 的子 ID。在 IAM 中，Sid 值在 JSON 策略中必须唯一。

Effect

Effect 元素是必需具备的元素，用于指定声明所产生的结果是“允许”还是“显式拒绝”。Effect 的有效值为 Allow 和 Deny。在默认情况下，将拒绝访问资源。如要允许访问资源，必须将 Effect 元素设置为 Allow。

Action

Action 元素描述将允许或拒绝的指定操作。每个服务有对应的任务操作，用户可以使用相应服务来执行所描述的任务。目前提供的服务有：oos（对象存储）、cloudtrail（操作跟踪）、statistics（统计）和 iam。具体每种服务包括的操作详见**操作列表**。

Action 元素的语法结构为：”Action”: “服务:具体操作”。其中具体操作也可以用通配符（*）表示某类操作。

- 示例 1：OOS：获取对象操作。

```
"Action": "oos:GetObject"
```

- 示例 2：IAM：创建 IAM 用户。

```
"Action": "iam:CreateUser"
```

- 示例 3：使用通配符（*）表示执行 OOS 的所有服务。

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

- 示例 4：使用通配符（*）表示执行 IAM 服务中包含 AccessKey 的操作。

```
"Action": "iam:*AccessKey*"
```

NotAction

NotAction 元素描述与指定操作列表之外的所有内容显式匹配。使用 NotAction 时只列出不应匹配的一些操作。使用 NotAction 时：

- 如果使用 Allow 效果，则允许未列出的所有适用操作或服务。
- 如果使用 Deny 效果，则拒绝此类未列出的操作或服务。如果想允许某个已列出的操作，则必须显式允许此操作。

- 示例 1：除删除存储桶操作外，允许用户执行 OOS 其他所有操作。

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

- 示例 2：允许用户执行除 IAM 服务外的所有操作。

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

- 示例 3：拒绝除 oos、cloudtrail 和 statistics 之外的服务。但并不是允许 oos、cloudtrail 和 statistics 服务的操作，如果允许 oos、cloudtrail 和 statistics 中的某个操作，需要再写新的策略进行显式允许。

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

```
        "NotAction": [
            "oos:*",
            "cloudtrail:*",
            "statistics:*",
        ],
        "Resource": "*",
    }]
}
```

Resource

Resource 元素指定执行策略的资源，可以指定一个或多个对象。

格式可以为：

- “Resource”: “arn:ctyun:*service*::*accountid*:*resource”*
- “Resource”: “arn:ctyun:*service*::*accountid*:*resourcetype*/*resource”*

其中：

- *service*：服务名；
- *accountid*：账户 ID；
- *resource*：具体资源。在指定资源时，可以使用通配符，其中*表示字符的任意组合，？表示任何单个字符。

说明：在 resource 最后部分添加**策略变量“${ctyun:username}”**指定占位符。当策略执行时，策略变量将被替换为请求本身的用户名。

如下列举例，将含有策略变量的策略附加给多个用户，当用户 A 发起请求时，username 将替换为 A 的用户名；当用户 B 发起请求时，username 将替换为 B 的用户名。

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

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

- *resourcetype*：资源类型。

NotResource

NotResource 元素指除指定资源列表之外的所有内容显式匹配的策略元素。使用 NotResource 时，只列出不应匹配的一些资源，而不是包括将匹配的资源列表。使用 NotResource 时应注意，在此元素中指定的资源是受限的资源，即：

- 如果使用 Allow，则将允许未列出的所有资源，包括所有其他服务中的资源；

- 如果使用 Deny，则拒绝所有未列出资源。

Condition

Condition 元素描述允许用户指定策略生效的条件。在 Condition 元素中，用户可构建表达式，并使用条件运算符将策略中的条件与请求值相匹配。

Condition 元素可以由多个条件组成。条件包括：条件运算符、条件键和条件值组成，一个条件键可以对应多个条件值。

Condition 的语法结构如下：

“Condition”: {“条件运算符 A”: {“条件键 A”:[“条件值 A1”, “条件值 A2”，…]}, “条件运算符 B”: {“条件键 B”:[“条件值 B1”, “条件值 B2”，…] } }

说明：条件键不区分大小写。如果条件值是时间，将需要设置的时间转换为 UTC+0 时区的时间。

若存在多个条件，各个条件之间的约束如下：

- 存在多个条件运算符，采用逻辑 AND 评估这些条件；
- 若一个条件键对应多个条件值，采用逻辑 OR 评估这些条件值；
- 必须满足所有条件运算符才能做出允许或者拒绝。如果多个条件中的任何一个不满足，那么策略不生效。

条件键、运算符、条件值见下表：

条件键	运算符	条件值
ctyun:CurrentTime	● **DateEquals**：匹配指定日期； ● **DateNotEquals**：不等于指定日期； ● **DateLessThan**：早于指定日期； ● **DateLessThanEquals**：早于或等于指定日期； ● **DateGreaterThan**：晚于指定日期； ● **DateGreaterThanEquals**：晚于或等于指定日期。	格式为：yyyy-MM-dd'T'HH:mm:ss'Z'。例如：2019-12-18T09:00:00Z。 **DateEquals** 和 **DateNotEquals** 精确到天，其他精确到秒。 **注意**：将需要设置的时间转换为 UTC+0 时间。
ctyun:SourceIp	● **IpAddress**：与指定 IP 地址	● IPv4：点分十进

	或范围匹配； ● **NotIpAddress**：除指定 IP 地址或范围外的所有 IP 地址匹配。	制格式 ● IPv6：32 位 16 进制数，格式为 X:X:X:X:X:X:X:X。 如果指定地址范围，IP 地址后加掩码表示，如 192.163.1.5/3。
ctyun:userid	● **StringEquals**：精准匹配指定的值，区分大小写； ● **StringNotEquals**：与指定的值不匹配，区分大小写； ● **StringEqualsIgnoreCase**：与指定的值精准匹配，不区分大小写。 ● **StringNotEqualsIgnoreCase**：与指定的值不匹配，不区分大小写； ● **StringLike**：与指定的值精准匹配；或通过填充通配符，与指定的值相似，可以包括多字符匹配的通配符 (*) 或单字符匹配的通配符 (?)。区分大小写； ● **StringNotLike**：与指定的值不匹配，区分大小写的无效匹配。或通过填充通配符，与指定的值也不匹配。	包含数字和小写字母的 32 位字符串。运算符为 **StringLike** 和 **StringNotLike**，可以包含通配符。
ctyun:username	● **StringEquals**：精准匹配指定的值，区分大小写； ● **StringNotEquals**：与指定的值不匹配，区分大小写； ● **StringEqualsIgnoreCase**：与指定的值精准匹配，不区分大小写。 ● **StringNotEqualsIgnoreCase**	1~64 位字符串组成，字符只能包含字母、数字或特殊字符，特殊字符只能是：下划线（_）、中划线（-）、逗号（,）、句点（.）、加号（+）、等号（=）

	：与指定的值不匹配，不区分大小写； ● **StringLike**：与指定的值精准匹配；或通过填充通配符，与指定的值相似，可以包括多字符匹配的通配符 (*)或单字符匹配的通配符 (?)。区分大小写； ● **StringNotLike**：与指定的值不匹配，区分大小写的无效匹配。或通过填充通配符，与指定的值也不匹配。	和 at 符号（@）。 **说明**：运算符为 **StringLike** 和 **StringNotLike**，可以包含通配符。
ctyun:UserAgent	● **StringEquals**：精准匹配指定的值，区分大小写； ● **StringNotEquals**：与指定的值不匹配，区分大小写； ● **StringEqualsIgnoreCase**：与指定的值精准匹配，不区分大小写。 ● **StringNotEqualsIgnoreCase**：与指定的值不匹配，不区分大小写； ● **StringLike**：与指定的值精准匹配；或通过填充通配符，与指定的值相似，可以包括多字符匹配的通配符 (*) 或单字符匹配的通配符 (?)。区分大小写； ● **StringNotLike**：与指定的值不匹配，区分大小写的无效匹配。或通过填充通配符，与指定的值也不匹配。	字符串，可以包含特殊字符。
ctyun:Referer	● **StringEquals**：精准匹配指定的值，区分大小写； ● **StringNotEquals**：与指定的值不匹配，区分大小写； ● **StringEqualsIgnoreCase**：与指定的值精准匹配，不区分	字符串，可以包含特殊字符。

	大小写。 ● **StringNotEqualsIgnoreCase**：与指定的值不匹配，不区分大小写； ● **StringLike**：与指定的值精准匹配；或通过填充通配符，与指定的值相似，可以包括多字符匹配的通配符 (*)或单字符匹配的通配符 (?)。区分大小写； ● **StringNotLike**：与指定的值不匹配，区分大小写的无效匹配。或通过填充通配符，与指定的值也不匹配。	
ctyun:SecureTransport	**Bool**：布尔匹配。	● **true** ● **false**
ctyun:MultiFactorAuthPresent	**Bool**：布尔匹配。 **说明**：只有 IAM 服务支持此条件键。	● **true** ● **false**
ctyun:MultiFactorAuthAge	● **NumericEquals**：与指定的值相同； ● **NumericNotEquals**：与指定的值不同，否定匹配； ● **NumericLessThan**：小于指定的值； ● **NumericLessThanEquals**：小于等于指定的值； ● **NumericGreaterThan**：大于指定的值； ● **NumericGreaterThanEquals**：大于等于指定的值。 **说明**：只有 IAM 服务支持此条件键。	整数形式。
oos:prefix	● **StringEquals**：精准匹配指定的值，区分大小写； ● **StringNotEquals**：与指定的值不匹配，区分大小写； ● **StringEqualsIgnoreCase**：与	字符串形式。 说明：本条件键仅对 ListBucket 生效。

	指定的值精准匹配，不区分大小写。 ● **StringNotEqualsIgnoreCase**：与指定的值不匹配，不区分大小写； ● **StringLike**：与指定的值精准匹配；或通过填充通配符，与指定的值相似，可以包括多字符匹配的通配符 (*) 或单字符匹配的通配符 (?)。区分大小写； ● **StringNotLike**：与指定的值不匹配，区分大小写。值可以在字符串中的任何位置包括多字符匹配的通配符 (*) 或单字符匹配的通配符 (?)。	
oos:x-amz-acl	● **StringEquals**：精准匹配指定的值，区分大小写； ● **StringNotEquals**：与指定的值不匹配，区分大小写； ● **StringEqualsIgnoreCase**：与指定的值精准匹配，不区分大小写。 ● **StringNotEqualsIgnoreCase**：与指定的值不匹配，不区分大小写； ● **StringLike**：与指定的值精准匹配；或通过填充通配符，与指定的值相似，可以包括多字符匹配的通配符 (*) 或单字符匹配的通配符 (?)。区分大小写； ● **StringNotLike**：与指定的值不匹配，区分大小写。值可以在字符串中的任何位置包括多字符匹配的通配符 (*) 或单字符匹配的通配符 (?)。	字符串形式。 取值为： ● private：私有 ● public-read：只读 ● public-read-write：公有 **说明**：创建 Bucket 时，通过使用此条件键可以控制存储桶 ACL 的类型，本条件键仅对 PutBucket 生效。

说明：在 Condition 元素中添加**策略变量“${ctyun:username}”**指定占位符。当策略执行时，策略变量将被替换为请求本身的用户名。

示例：将含有策略变量的策略附加给多个用户，当用户 A 发起请求时，条件键 oos:prefix 将根据用户 A 的 username 进行判断；当用户 B 发起请求时，条件键 oos:prefix 将根据用户 B 的 username 进行判断。

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

- **…IfExists 条件运算符**

IfExists：如果请求的内容中存在关键字，则依照策略所述的条件来处理关键字。如果该关键字不存在，则条件元素的计算结果将为 true。

目前仅 Bool 型和数字类型的运算符支持使用 IfExists 条件运算符，表达形式：*运算符* IfExists，例如 BoolIfExists、NumericEqualsIfExists。对于…IfExists 的使用见示例 1 和示例 2。

示例 1

- 拒绝没有使用 MFA 认证的控制台请求，不拒绝使用 MFA 认证的控制台请求和使用密钥的 API 请求。但如果允许使用 MFA 认证的控制台请求和使用密钥的 API 请求，需要再写显性允许语句。

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

- 拒绝没有使用 MFA 认证的控制台请求及使用密钥的 API 请求，不拒绝 MFA 认证的控制台请求。但如果允许 MFA 认证的控制台请求，需要再写显性允许语句。

```
"Effect" : "Deny",
```

```
"Condition" : { "BoolIfExists" : { "ctyun:MultiFactorAuthPresent" : false } }
```

示例 2

- 允许使用 MFA 认证在 1800 秒内的请求及使用密钥的 API 请求。

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

- 允许使用 MFA 认证在 1800 秒内的请求，但不允许 MFA 认证在 1800 秒以上及没有使用 MFA 的请求（包括 API 请求）。

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

策略变量

在编写策略时，如果不能确定 Resource、NotResource 或 Condition 元素中的精确值，可以使用策略变量作为占位符。目前仅支持变量“**${ctyun:username}**”。当策略执行时，策略变量将被替换为请求本身的用户名。

示例 1：将含有策略变量的策略附加给多个用户，当用户 A 发起请求时，username 将替换为 A 的用户名；当用户 B 发起请求时，username 将替换为 B 的用户名。

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

```
}
```

示例 2：将含有策略变量的策略附加给多个用户，当用户 A 发起请求时，条件键 oos:prefix 将根据用户 A 的 username 进行判断；当用户 B 发起请求时，条件键 oos:prefix 将根据用户 B 的 username 进行判断。

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