对象存储（经典版）I 型

用户使用手册 V6

天翼云科技有限公司

目录

1 产品介绍.....1
2 主要概念.....2
2.1 OOS 的主要概念.....2
2.1.1 Account.....2
2.1.2 Service.....3
2.1.3 Bucket.....3
2.1.4 Object.....3
2.1.5 存储类型.....3
2.1.6 合规保留.....4
2.1.7 清单配置.....5
2.2 统计分析.....5
2.2.1 基本概念.....5
2.3 操作跟踪.....6
2.3.1 基本概念.....6
2.4 访问控制.....7
2.4.1 功能特性.....7
2.4.2 应用场景.....7
2.4.3 基本概念.....7
2.4.4 服务限制.....8
3 账户管理.....10
3.1 开通 OOS 服务.....10
3.2 进入对象存储控制台.....10
3.3 找回密码.....10
3.4 退出.....10
3.5 地域切换.....10
4 统计概览.....12

4.1 概览.....12
4.2 统计.....15
4.2.1 容量.....15
4.2.2 删除量.....17
4.2.3 流量.....18
4.2.4 请求次数.....21
4.2.5 并发连接数.....23
4.2.6 数据取回量.....24
5 存储桶列表.....27
5.1 存储桶管理.....27
5.1.1 创建存储桶（Bucket）.....28
5.1.2 存储桶列表.....31
5.1.3 删除存储桶.....31
5.1.4 清空存储桶.....32
5.1.5 查看/修改存储桶属性.....33
5.1.6 区域属性.....34
5.1.7 安全策略.....36
5.1.8 网站.....39
5.1.9 日志.....42
5.1.10 生命周期.....43
5.1.11 跨域设置.....47
5.1.12 合规保留.....48
5.1.13 清单配置.....52
5.2 文件管理.....59
5.2.1 查看文件详细信息.....60
5.2.2 上传文件.....61
5.2.3 下载文件.....64
5.2.4 管理文件元数据.....65

5.2.5 文件预览.....70
5.2.6 文件分享.....70
5.2.7 创建文件夹.....74
5.2.8 删除文件/文件夹.....74
5.2.9 复制文件.....75
5.2.10 移动文件.....76
5.2.11 修改存储类型.....77
5.2.12 搜索文件.....78
5.2.13 复制文件名称.....79
5.2.14 文件排序.....80
6 操作跟踪.....81
6.1 管理事件记录.....81
6.1.1 查看详细事件.....82
6.1.2 事件列表.....86
6.2 跟踪列表.....89
6.2.1 创建跟踪.....90
6.2.2 修改跟踪.....91
7 访问控制.....93
7.1 快速入门.....95
7.2 IAM 用户.....98
7.2.1 创建 IAM 用户.....98
7.2.2 查看和修改 IAM 用户信息.....103
7.2.3 删除用户.....108
7.2.4 IAM 用户登录.....109
7.3 IAM 用户组.....111
7.3.1 创建用户组.....111
7.3.2 查看和修改用户组信息.....113
7.3.3 删除用户组.....115

7.4 IAM 策略.....116
7.4.1 系统策略.....116
7.4.2 自定义策略.....118
7.4.3 查看策略基本信息.....132
7.4.4 授权用户/用户组.....133
7.5 安全设置.....134
7.5.1 密码安全设置.....134
7.5.2 登录安全设置.....136
7.6 安全凭证.....138
7.6.1 密钥.....138
7.6.2 密码.....139
7.6.3 MFA.....139
7.7 IAM 最佳实践.....142
7.7.1 安全管理.....142
7.7.2 用户管理示例.....143
8 资源包管理.....148
9 附录.....149
9.1 域名（Endpoint）列表.....149
9.1.1 对象存储网络.....149
9.1.2 对象存储网络 2.....150
9.1.3 香港节点.....150
9.2 操作权限与 API 对应关系.....151
9.3 IAM 策略编写规则.....158
9.3.1 Version.....158
9.3.2 Statement.....158

1 产品介绍

对象存储系统（Object-Oriented Storage，OOS）为客户提供一种海量、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。

用户可以根据需要，选择使用大陆的**对象存储网络**、**对象存储网络 2** 或**香港**节点。

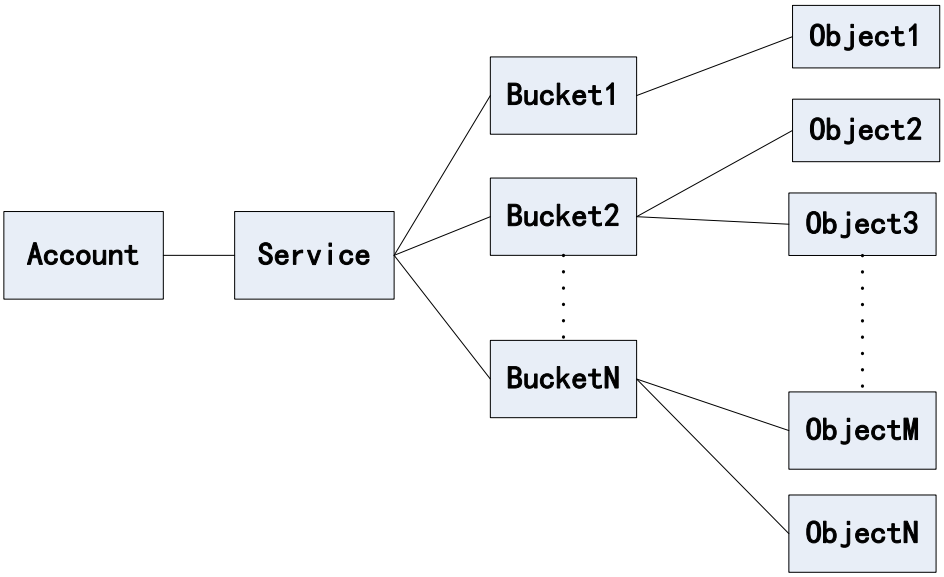
2 主要概念

2.1 OOS 的主要概念

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（文件）：用户存储在 OOS 上的每个文件都是一个 Object，也称为 OOS 的文件。
- Bucket（存储桶）：存储 Object 的存储桶。

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，联系天翼云客服工作人员开通 OOS 服务，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（存储桶），每个存储桶中可以存储不限数量的 Object（文件）。

2.1.1 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，联系天翼云客服人员（客服电话：400-810-9889）申请开通 OOS 服务。开通 OOS 服务成功之后，用户可以用该账户登录并使用 OOS 服务。

2.1.2 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 个的存储桶（Bucket）。

2.1.3 Bucket

存储桶（Bucket）是存储文件（Object）的容器。对象存储系统的每个文件（Object）都必须包含在一个存储桶中。对象存储提供的是基于桶和文件的扁平化存储方式，桶中的所有文件都处于同一逻辑层级，去除了文件系统中的多层级树形目录结构。

您可以设置存储桶的属性，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存储桶内的所有文件，因此您可以通过灵活的属性设置，来创建不同的存储桶，完成不同的管理功能。每个用户最多可以建立 10 个存储桶。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。

2.1.4 Object

对象（Object）是用户存储在 OOS 上的数据基本单元，也被称为 OOS 的文件。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、删除和共享文件。同时用户还可以对文件的组织形式进行管理，将文件移动或者复制到目标目录下。

2.1.5 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。如果上传文件时未指定存储类型，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：低频访问存储的文件有最短存储时间，存储时间短于 30 天的文件被提前删除或变更时，会产生一定费用。

- 最小计费大小：低频访问存储文件有最小计费大小，即如果文件大小低于 64KiB，会按照 64KiB 计算收费，文件大于等于 64KiB 按照实际存储收费。
- 数据取回：获取低频访问存储数据时产生的数据取回费用。

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	99.99%	99.9%
文件最小计费大小	按照文件实际大小计算	64KiB
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

文件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、修改文件的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：可以通过修改文件的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。

2.1.6 合规保留

OOS 提供合规保留功能，即启用 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文件进行修改和删除。

可以根据需求，对 Bucket 级别启用合规保留功能，以天（Days）或者以年（years）为单位设置合规保留时长，1year=365 days。

注意：

- 合规保留一旦启用，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，文件 A1 属于 Bucket A，A1 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文件。
- 处于合规保留期的文件，无法通过调用 API、控制台修改文件的存储类型，只能通过设置的生命周期规则修改存储类型。
- 文件处于合规保留期：如果生命周期规则为修改文件的存储类型，则生命周期规则可以生效。如果生命周期规则为到期删除文件，则文件必须过了合规保留期后，生命周期规则才能生效。

2.1.7 清单配置

通过 OOS 存储桶清单功能可以获取 Bucket 中指定文件（Object）的大小、存储类型等信息。相对于 GET Bucket (List Objects)接口，Bucket 清单可以按每天或者每周以 CSV 的形式输出指定文件的相关信息，且不会影响 Bucket 的请求速率。在需要列举海量文件的场景中，推荐使用 Bucket 清单功能。

2.2 统计分析

统计分析指用户可以查询指定 Bucket、指定数据位置的数据使用情况，根据统计分析数据，采取对应的措施。

2.2.1 基本概念

- **直接流量-互联网流量：**从互联网上传下载文件，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）上传下载文件，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**：从互联网上传下载文件，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）上传下载文件，并且经过对象存储网络内部调度产生的流量。
- **删除容量**：已删除文件的大小。

2.3 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 Bucket 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：用户通过操作跟踪功能可以查看近 6 个月内的管理事件，包括：登录，退出，查看、创建、修改和删除资源。
- 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 Bucket 中，即跟踪日志。

2.3.1 基本概念

2.3.1.1 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。

2.3.1.2 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。

2.3.1.3 写事件

写事件为可以修改资源的操作，包括创建、修改和删除操作。

2.4 访问控制

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。

2.4.1 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。

2.4.2 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文件的操作，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。

2.4.3 基本概念

2.4.3.1 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。

2.4.3.2 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。

2.4.3.3 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。

2.4.3.4 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 IAM 用户支持 MFA。

2.4.3.5 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。

2.4.3.6 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**：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。

2.4.4 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

3 账户管理

3.1 开通 OOS 服务

联系天翼云客服人员申请开通 OOS 服务。客服电话：400-810-9889。

3.2 进入对象存储控制台

用户可以按照下列方法进入对象存储 OOS 控制台：

- 登录天翼云官网后，进入 OOS 帮助中心，点击“管理控制台”，即进入对象存储经典版 I 型（OOS）控制台。
- 登录天翼云官网，点击右上角的“控制中心”，进入控制中心页面后点击“对象存储经典版 I 型”，即进入对象存储经典版 I 型（OOS）控制台。

3.3 找回密码

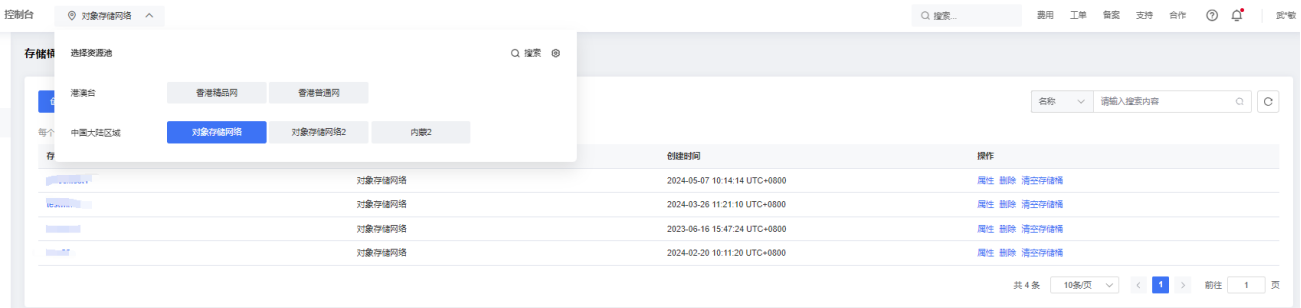
已注册用户在忘记密码的时候，可以在登录页面点击“忘记密码”，通过快捷通道找回密码。找回密码时，用户需要根据提示，按步骤输入相关信息找回密码。

3.4 退出

登录的账户，点击“退出”按钮，退出当前登录的账户。

3.5 地域切换

用户可以对 OOS 地域进行切换，根据选择跳转到不同的区域。



可以选择**中国大陆区域**的**对象存储网络**、**对象存储网络 2**，也可以选择**港澳台**的**香港**节点。

- **对象存储网络**：包含分布在全国多个省、市、自治区及直辖市的资源池，这些资源池间的存储桶（Bucket）、文件（Object）、访问密钥（**AccessKeyId** 和 **SecretAccessKey**）信息互通，可以实现全国数据的就近读取和写入。
- **对象存储网络 2**：包含分布在全国多个省、市、自治区及直辖市的资源池，这些资源池间的存储桶（Bucket）、文件（Object）、访问密钥（**AccessKeyId** 和 **SecretAccessKey**）信息互通，可以实现全国数据的就近读取和写入。
- **香港**：香港节点包括精品网和普通网。

4 统计概览

在**统计概览**页，用户可以查询**容量**、**流量**、**请求次数**、**并发连接数**等相关信息。

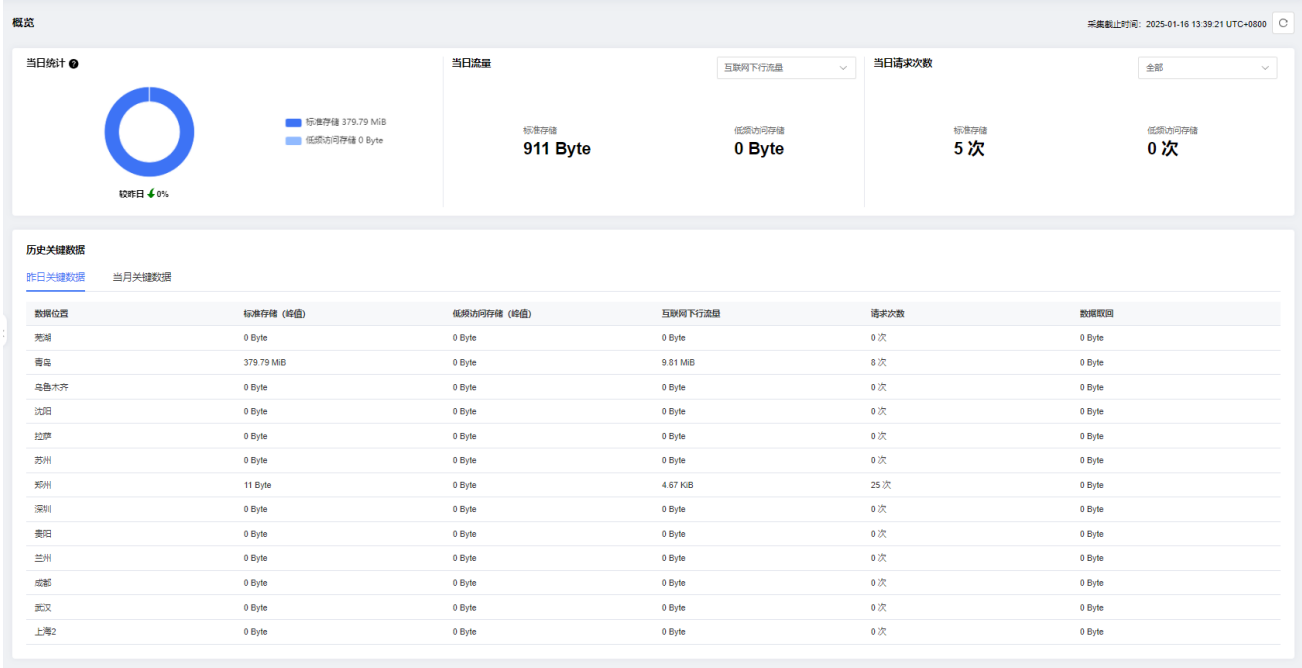
说明：对于 IAM 子用户，拥有相应的权限才可以查看统计相关信息，需要拥有的权限如下：

操作	需具备的权限
统计	statistics:GetAccountStatistcsSummary

4.1 概览

点击“统计概览”>“概览”，可用查看 Bucket 当日统计，包括：标准存储、低频访问存储、互联网下行流量、互联网上行流量、GET 类请求和 PUT 类请求。如果是香港节点，还可以选择网络类型：全部网络类型、精品网、普通网。

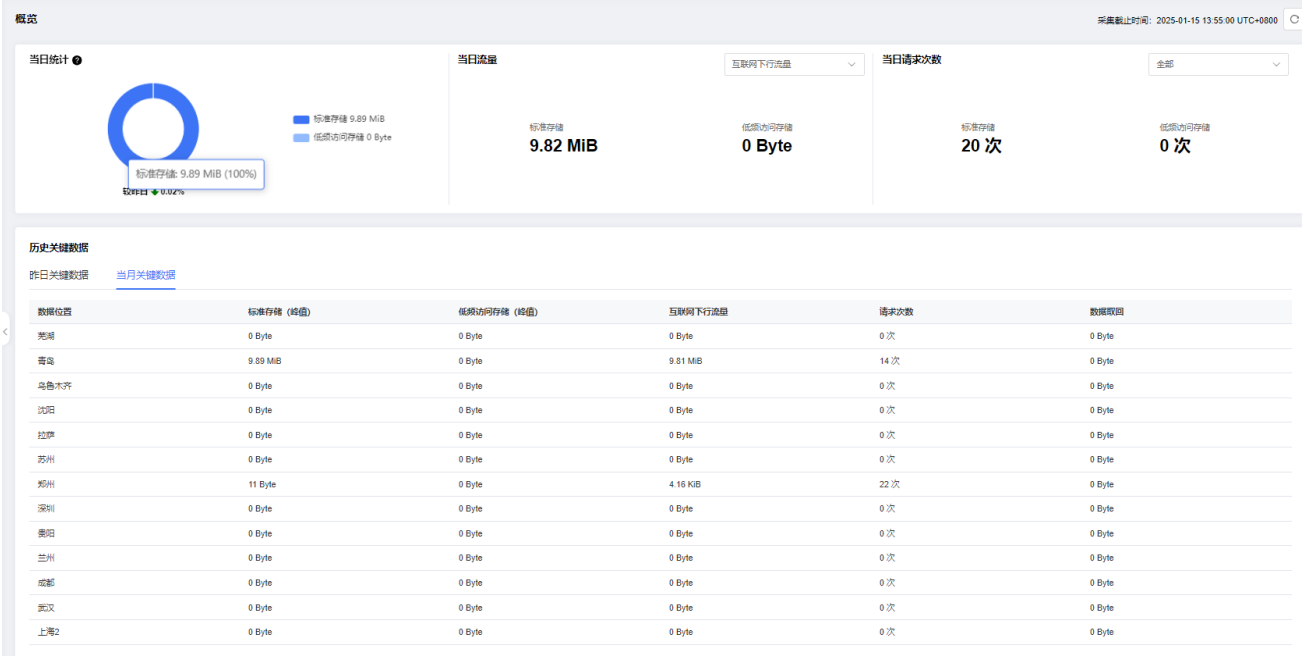
点击该页面的“昨日关键数据”（统计时间范围为北京时间当前时刻的前一天 00:00-24:00 的数据），可用查看各数据位置昨日的标准存储（峰值）、低频访问存储（峰值）、互联网下行流量、请求次数、数据取回。如果是香港节点，还会显示精品网下行流量、普通网下行流量。



项目	描述
当日统计	当日的存储容量，包括标准存储和低频访问存储。

当日流量	当日的流量统计，可以选择**互联网下行流量**（下载量）、**互联网上行流量**（上传量）。
当日请求次数	当日的请求次数，可以选择： ● 全部：包括所有的 Put 类请求和 Get 类请求。 ● Put 类请求。 ● GET 类请求。
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。
数据位置	存放文件（Object）的位置。
标准存储（峰值）	标准存储类型的数据的容量峰值。
低频访问存储（峰值）	低频访问存储类型的数据的容量峰值。
互联网下行流量	从互联网下载文件（Object）的数据流量。
请求次数	统计产生的 GET 请求、HEAD 请求、PUT 请求、POST 请求、DELETE 请求、OTHERS 的次数，以及所有请求的次数总和。统计产生返回码 200、204、206、403、404、4xx 的次数，以及所有返回码返回次数的总和。
数据取回	频访问存储类型的文件（Object）在查看和下载时产生的从 OOS 服务端读取数据的数据量。
精品网下行流量（香港）	通过精品网下载文件（Object）的数据流量。
普通网下行流量（香港）	通过普通网下载文件（Object）的数据流量。

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、请求次数、数据取回。如果是香港节点，还会显示精品网下行流量、普通网下行流量。



数据位置	标准存储（峰值）	低频访问存储（峰值）	互联网下行流量	请求次数	数据取回
芜湖	0 Byte	0 Byte	0 Byte	0 次	0 Byte
青岛	9.89 MiB	0 Byte	9.81 MiB	14 次	0 Byte
乌鲁木齐	0 Byte	0 Byte	0 Byte	0 次	0 Byte
沈阳	0 Byte	0 Byte	0 Byte	0 次	0 Byte
拉萨	0 Byte	0 Byte	0 Byte	0 次	0 Byte
苏州	0 Byte	0 Byte	0 Byte	0 次	0 Byte
郑州	11 Byte	0 Byte	4.16 KiB	22 次	0 Byte
深圳	0 Byte	0 Byte	0 Byte	0 次	0 Byte
贵阳	0 Byte	0 Byte	0 Byte	0 次	0 Byte
兰州	0 Byte	0 Byte	0 Byte	0 次	0 Byte
成都	0 Byte	0 Byte	0 Byte	0 次	0 Byte
武汉	0 Byte	0 Byte	0 Byte	0 次	0 Byte
上海2	0 Byte	0 Byte	0 Byte	0 次	0 Byte

4.2 统计

4.2.1 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	选择容量查询的数值类型： ● 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的容量 ● 标准类型：标准存储的容量。 ● 低频访问存储：低频访问存储的容量。

可以点击“下载”按钮，将统计信息下载到本地查看。

项目	描述
Date	统计时间。
StorageClass	存储类型： ● STANDARD：标准存储 ● STANDARD_IA：低频访问存储
BilledStorageUsage	计费容量，单位是 Byte。
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。

4.2.2 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。 ● 低频访问存储：低频访问存储的删除量。

可以点击“下载”按钮，将统计信息下载到本地查看。

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

4.2.3 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。
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：从互联网上传下载文件（Object）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：从互联网上传下载文件（Object），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）上传下载文件（Object）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）上传下载文件（Object），并且经过对象存储网络内部调度产生的流量。
网络类型	流量的网络类型（仅香港节点支持）： ● 全部网络类型：精品网和普通网流量和值。 ● 精品网：精品网的流量。 ● 普通网：普通网的流量。

可以点击“下载”按钮，将流量统计信息下载到本地查看。

项目	描述
Date	统计时间。
Region	数据位置。
Bucket	存储桶。
StorageClass	存储类型。
NetType	网络类型（仅香港节点支持）： ● highqualitynet：精品网。 ● normalqualitynet：普通网。
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。

4.2.4 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。
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	返回码 200 的次数。
Response204	返回码 204 的次数。
Response206	返回码 206 的次数。
Response403	返回码 403 的次数。
Response404	返回码为 404 的次数。
Response4XX	除返回码 403 和 404 外的其他返回码 4xx 的次数。

4.2.5 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：

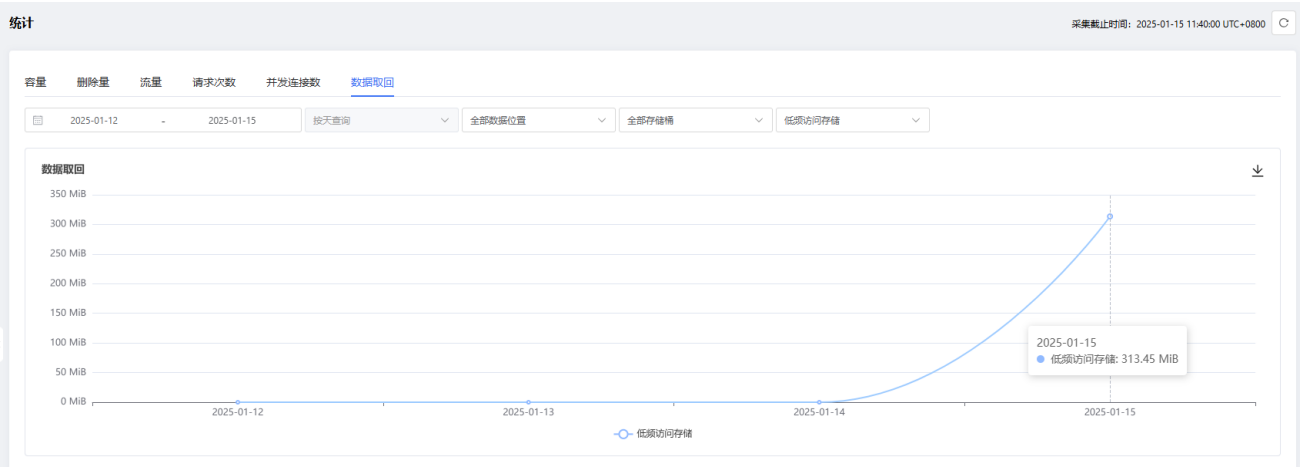
	● 全部数据位置：展示所有数据位置的并发连接数之和。 ● 具体数据位置：根据显示的数据位置进行选择，查看对应数据位置的并发连接数。
存储桶	并发连接数数查询的存储桶，可以选择： ● 全部存储桶：展示所有存储桶的并发连接数之和。 ● 具体存储桶：根据显示的存储桶，选择查看对应存储桶的并发连接数。
连接类型	选择并发连接数的连接类型： ● 全部连接类型：包含互联网连接数和非互联网连接数。 ● 互联网连接数。 ● 非互联网连接数。

可以点击“下载”按钮，将并发连接数的统计信息下载到本地查看。

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。

4.2.6 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数据取回量： ● 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。
RestoreStorageUsage(Bytes)	用户获取数据产生的数据取回量，标准存储类型文件（Object）产生的数据取回量为 0，单位是 Bytes。

5 存储桶列表

5.1 存储桶管理

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

操作	需具备的权限
创建存储桶	oos:PutBucket、oos:GetRegions 建议同时赋予的权限：oos:ListAllMyBucket
存储桶列表	oos:ListAllMyBucket
删除存储桶	oos:ListAllMyBucket、oos:DeleteBucket
清空存储桶	oos:ListAllMyBucket、oos:DeleteMultipleObjects
查看/修改存储桶属性	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
生命周期	oos:ListAllMyBucket、oos:GetLifecycleConfiguration、oos:PutLifecycleConfiguration
跨域设置	oos:ListAllMyBucket、oos:GetBucketCORS、oos:PutBucketCORS
合规保留	oos:ListAllMyBucket、oos:GetBucketObjectLockConfiguration、oos:PutBucketObjectLockConfiguration、oos:DeleteBucketObjectLockConfiguration
清单配置	oos:ListAllMyBucket、oos:PutBucketInventoryConfiguration、

	oos:GetBucketInventoryConfiguration

5.1.1 创建存储桶（Bucket）

点击“存储桶列表”>“创建存储桶（Bucket）”，输入存储桶名称，并设置其访问权限、索引位置、数据位置等信息。

1） 命名规范

存储桶（Bucket）的命名规范是：

- 存储桶名称必须全局唯一。
- 存储桶名称长度介于 3 到 63 字节之间。
- 存储桶名称只能由小写字母、数字、短横线（-）和点（.）组成。

- 存储桶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：
  - 只能包含小写字母、数字和短横线（-）。
  - 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。
- 存储桶名称不能是一组或多组“数字.数字”的组合（如 192.162.0.1）。
- 存储桶名称中不能包含双点（..）、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

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：私有、公共读、公共读写。各自的含义如下：

- 私有：只有根用户和具有相应权限的子用户可以对该存储桶内的文件进行读/写/删除操作（包括 Put、Delete 和 Get Object），其他人（包括匿名访问）只有通过 Bucket Policy 授权或分享链接才可访问该存储桶内的文件。
- 公共读：只有根用户和具有相应权限的子用户可以对该存储桶内的文件进行写/删除操作（包括 Put 和 Delete Object）。任何人（包括匿名访问）都可以对该存储桶内的文件进行读操作，这有可能造成您数据的外泄以及费用激增，请慎用该权限。
- 公共读写：任何人（包括匿名访问）都可以对该存储桶内的文件进行读/写/删除操作（包括 Get、Put 和 Delete Object）。这有可能造成您数据的外泄以及费用激增，若被人恶意写入违法信息还可能会侵害您的合法权益，除特殊场景外，不建议您配置公共读写权限。

  注意：如果想使用访问权限为公共读写的存储桶，请联系天翼云客服评估审核后开通此功能。

3) 索引位置

索引位置是指存放文件数据索引信息的位置，在创建存储桶时指定索引位置，创建成功后不能再对存储桶的索引位置进行更改。

4) 数据位置

数据位置是指存放文件数据的位置。

- 如果用户选择“就近写入”，那么文件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文件数据，OOS 将按用户指定的位置顺序存储文件。

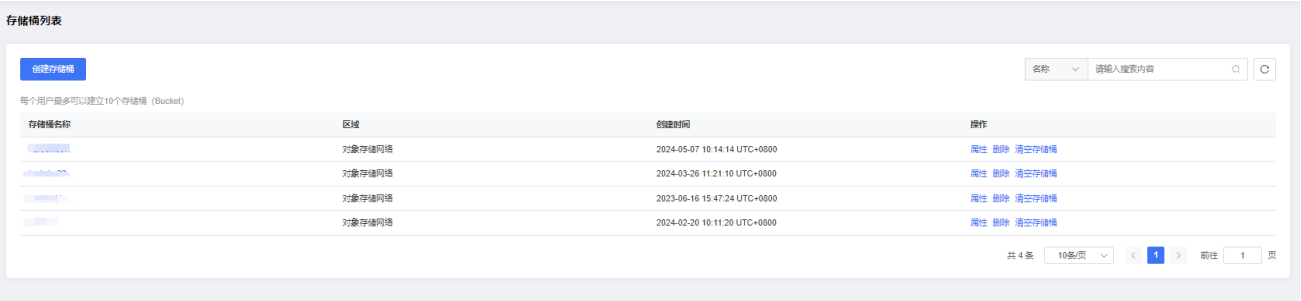
5） 数据调度策略

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。

5.1.2 存储桶列表

在存储桶列表页可以查看存储桶信息，包括存储桶名称、区域、创建时间。

用户可以根据需求，在右上角的搜索框内输入需要查询的存储桶名称进行查询，支持模糊查询。

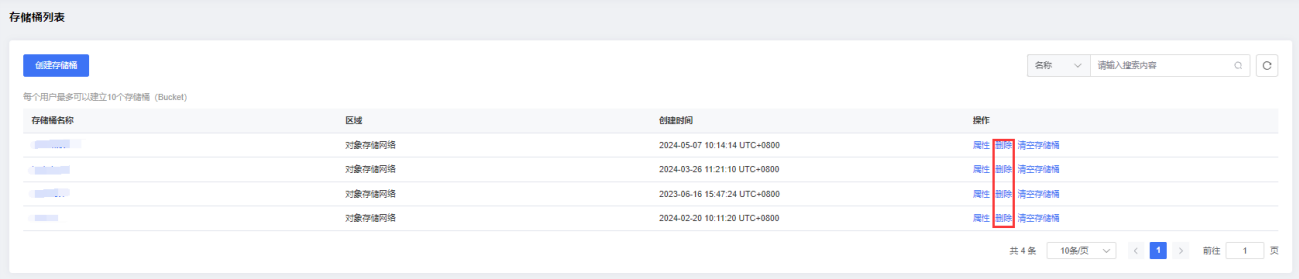


项目	描述
存储桶名称	存储桶的名称。
区域	存储桶所属的区域，包括对象存储网络、对象存储网络 2、其他区域、香港，详见**地域切换**。
创建时间	存储桶创建的时间。
操作	可以查看修改存储桶的属性、删除存储桶、清空存储桶。存储桶的属性包括：存储桶属性、区域属性、安全策略、网站、日志、生命周期、跨域设置、合规保留。

5.1.3 删除存储桶

在“存储桶列表”页，点击要删除存储桶“操作”列的“删除”按钮，可以删除该存储桶。

说明：只有存储桶中不包含任何文件夹和文件时，用户才可以删除该存储桶。



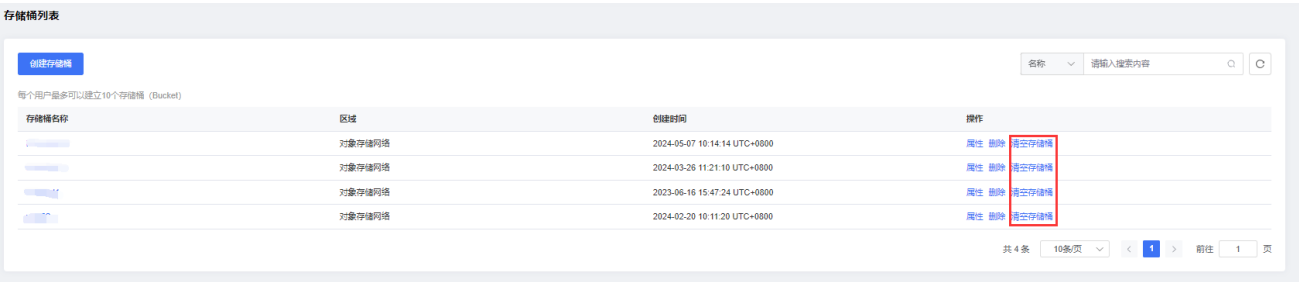
当用户点击“删除”后，需要在弹窗进行二次确认后，才可以删除存储桶。

5.1.4 清空存储桶

在“存储桶列表”页，点击存储桶“操作”列的“清空存储桶”按钮，可以清空该存储桶数据。

注意：

- 清空存储桶将永久删除存储桶中的所有文件，已删除的文件无法恢复。在执行清空存储桶过程中，可通过关闭任务方式进行终止，但是已经发送的任务无法终止。
- 执行清空存储桶时添加到存储桶的文件可能会被删除。
- 为了防止在执行清空存储桶时将新文件添加到此存储桶，建议您更新存储桶策略，禁止将文件添加到存储桶。
- 如果存储桶包含大量文件，建议您创建生命周期规则来删除存储桶中的文件。



当点击“清空存储桶”后，弹出“清空存储桶确认”弹窗，填入存储桶名称后，才可以清空存储桶数据。

清空过程中，刷新或者关闭页面可能导致无法完全清空存储桶。

5.1.5 查看/修改存储桶属性

对象存储系统提供存储桶（Bucket）级别的权限控制，用户可以根据需求，设置存储桶的访问权限。

在“存储桶列表”页面点击“属性”>“存储桶属性”，可查看所选存储桶的属性信息，并对存储桶的访问权限进行修改。

存储桶（Bucket）目前有 3 种访问权限：私有、公共读、公共读写。各自的含义如下：

- 私有：只有根用户和具有相应权限的子用户可以对该存储桶内的文件进行读/写/删除操作（包括 Put、Delete 和 Get Object），其他人（包括匿名访问）只有通过 Bucket Policy 授权或分享链接才可访问该存储桶内的文件。
- 公共读：只有根用户和具有相应权限的子用户可以对该存储桶内的文件进行写/删除操作（包括 Put 和 Delete Object）。任何人（包括匿名访问）都可以对该存储桶内的文件进行读操作，这有可能造成您数据的外泄以及费用激增，请慎用该权限。
- 公共读写：任何人（包括匿名访问）都可以对该存储桶内的文件进行读/写/删除操作（包括 Get、Put 和 Delete Object）。这有可能造成您数据的外泄以及费用激增，若被人恶意写入违法信息还可能会侵害您的合法权益，除特殊场景外，不建议您配置公共读写权限。

  注意：如果想使用访问权限为公共读写的存储桶，请联系天翼云客服评估审核后开通此功能。

5.1.6 区域属性

在“存储桶列表”页面点击“属性”>“区域属性”，进入“区域属性”页面，用户可以通过该页更改存储桶（Bucket）的数据位置和数据调度策略，但不能修改索引位置。

说明：香港节点仅显示 Endpoint。

项目	描述
索引位置	存放文件索引信息的位置，在创建存储桶时指定索引位置，创建成功后不能再对存储桶的索引位置进行更改。
数据位置	存放文件数据的位置，用户可以根据自身需求进行修改： ● 就近写入：文件数据将被存储在距离写入点最近的数据位置。 ● 指定位置：可以指定多个数据位置存放文件数据，OOS 将按用户指定的位置顺序存储文件。
数据调度策略	数据调度的策略： ● 允许自动调度：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。 ● 不允许自动调度：OOS 不会自动调度用户数据存储位置的调度。
Endpoint	域名地址。

5.1.7 安全策略

安全策略定义 OOS 资源的访问权限，作用于所配置的存储桶及存储桶内文件。OOS 存储桶拥有者通过安全策略可为 IAM 用户或其他帐号授权存储桶及存储桶内文件的操作权限，具体包括：

- 允许/拒绝 Bucket 级别的权限。
- 允许/拒绝 Object 级别的权限。

在安全策略中，用户可以设置 Bucket policy，用于定义 OOS 资源的访问权限，存储桶的安全策略是由效果、被授权用户、资源、动作和条件 5 个桶策略基本元素共同决定，详细的 Bucket Policy 格式请参见《开发者文档》。

说明：如果 Bucket 的属性为私有或者公共读，配置允许任何用户可以向该 Bucket 写文件的策略时，需要联系天翼云客服进行备案。

在“存储桶列表”页面点击“属性”>“安全策略”，进入“安全策略”页面，在该页面点击“编辑策略”，可以添加 Bucket Policy。

Policy 示例如下：

- Referer 设置

  例如要配置名称为"example-bucket"的 Bucket 的访问策略，只允许 Referer 头为以“https://www.ctyun.cn/”或“https://ctyun.cn/”开头的 https 请求访问此 Bucket，那么可以采用如下的配置方式。

```
{
  "Version":"2012-10-17",
  "Id":"*",
  "Statement":[
    {
      "Sid":"*",
      "Effect":"Allow",
```

```
      "Principal":{ "CTYUN": ["*"] },
      "Action":"oos:GetObject",
      "Resource":"arn:ctyun:oos:::example-bucket/*",
      "Condition":{
        "StringLike":{
          "ctyun:Referer":[
            "https://www.ctyun.cn/*",
            "https://ctyun.cn/*"
          ]
        }
      }
    }
  ]
}
```

- **IP 设置**

  如果只允许 IP 地址在 192.168.143.0/24 范围内的 IP 访问存储桶 example-bucket，不允许 IP 地址 192.168.143.188/32 访问，那么可以采用如下的配置方式。

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

```
}
```

5.1.8 网站

在“存储桶列表”页面点击“属性”>“网站”，进入“网站”页面。在该页面，用户可以配置存储桶（Bucket）的网站托管属性，配置完成后，可以使用已经备案的静态网站域名访问存放在存储桶内的数据。

注意：

- 如果配置静态网站托管后，当匿名用户直接访问存储桶的域名，会将静态网站文件下载到本地。如果要实现访问静态网站时是预览网站内容，而非下载静态网站文件，静态网站域名须是存储桶绑定的已备案自定义域名，为存储桶绑定自定义域名请联系天翼云客服申请。
- OOS 自有网站托管域名不支持 HTTPS 访问，用户自定义域名支持 HTTPS 访问。如果需要支持 HTTPS 访问，请联系天翼云客服，提供域名证书，证书支持格式：crt+key 或者 PEM，请确保提供的证书在有效期内，建议证书有效期至少 1 年及以上，避免使用免费证书。
- 尽量避免目标存储桶名中带有“.”，否则通过 HTTPS 访问时可能出现客户端校验证书出错。

网站托管配置步骤如下：

1）创建一个公共读属性的存储桶（Bucket）。

2）向天翼云客服提交工单，评估审核申请客户自定义域名添加白名单。

3）在域名管理中添加别名。

- 如果不使用 CDN 加速，将存储桶的 CNAME Record Value（*bucketname*.oos-website-cn.oos-*xx*.ctyunapi.cn）作为别名添加到域名管理系统中。
- 如果使用 CDN 加速，将 CDN 厂商提供的别名添加到域名管理系统中，然后在 CDN 回源地址中配置 OOS 侧的 CNAME Record Value，并将回源 host 配置为您的自定义域名（如 your***domain.com）。

说明：创建存储桶时显示的 Endpoint 为 oos-cn.ctyunapi.cn，该 Endpoint 是针对整个对象存储网络的域名，该域名在解析时，会根据用户地理位置的不同解析到不同的资源池地址。如果创建 Bucket 时有多个数据位置，系统默认选取创建时第一个有效数据位置作为 CNAME Record Value（*bucketname*.oos-website-cn.oos-*xx*.ctyunapi.cn）。如

果创建存储桶时，只有一个数据位置可用，则在存储桶区域中展示的 CNAME Record Value 为 *bucketname*.oos-website-cn.oos-cn.ctyunapi.cn。所以如果使用静态网站托管，建议您根据存储桶区域属性中的数据位置，选择您想使用的数据位置的 CNAME Record Value 作为域名管理系统中的别名。例如您创建存储桶时有效数据位置为沈阳、兰州、成都、贵阳，则存储桶中展示的 CNAME Record Value 为 *bucketname*.oos-website-cn.oos-lnsy.ctyunapi.cn，您可以将 *bucketname*.oos-website-cn.oos-lnsy.ctyunapi.cn 作为别名，也可以将兰州、成都或者贵阳为域名的 CNAME Record Value 作为您的别名。

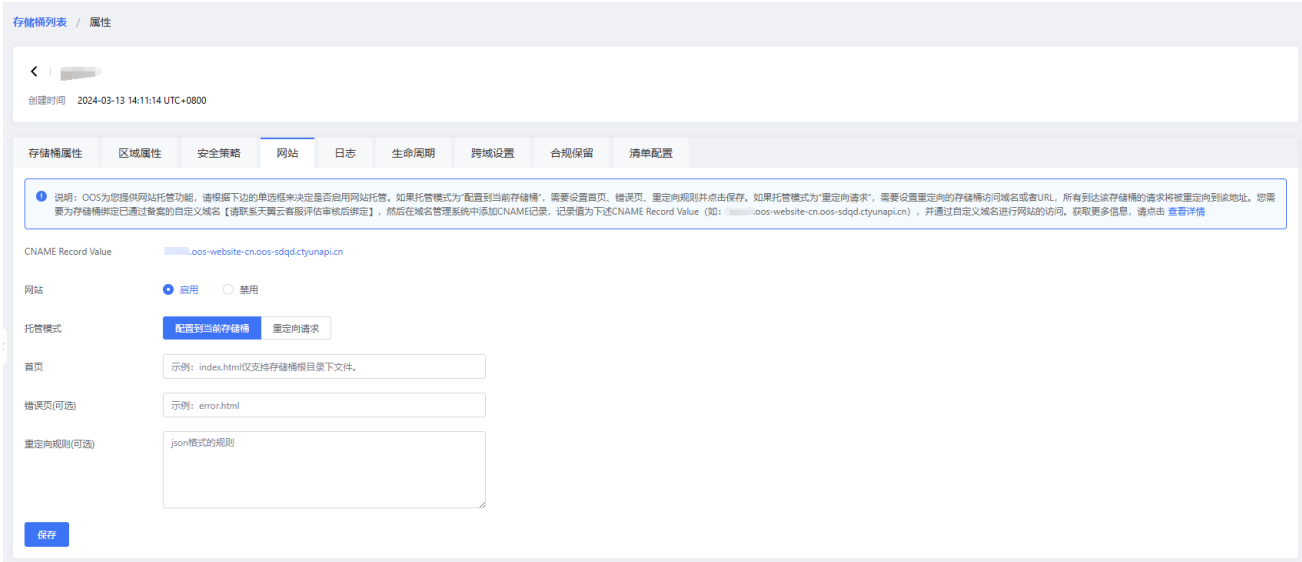
4) 上传文件

将网站的所有文件（html、CSS、js、图片等）上传到之前创建的存储桶中，注意保持文件之间的相对路径。

5) 配置存储桶网站属性

进入**网站**属性，选择**启用**网站托管：

- 托管模式为配置到当前存储桶：



  - 配置首页：首页指访问网站时跳转到的页面。例如将 http://your***domain.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://your***domain.com/index.html 页面。

- 配置错误页（可选）：错误页指当访问网站时，出现错误跳转到的页面。例如将 `http://your***domain.com` 出错页设置为 `error.html`，那么当访问网站出错时，将跳转到 `http://your***domain.com /error.html`。
- 重定向规则（可选）：可以通过制定重定向规则，将满足条件的请求重定向到指定主机或页面。控制台支持配置 JSON 格式的重定向规则。可以配置多条重定向规则，每条重定向规则一个 Condition 和一个 Redirect。例如：

```
[
   {
     "Condition": {
          "HttpErrorCodeReturnedEquals": "string",
          "KeyPrefixEquals": "string"
           },
     "Redirect": {
          "HostName": "string",
          "Protocol": "Protocol",
          "ReplaceKeyPrefixWith": "string"
           }
      }
]
```

重定向规则描述

项目	描述
Condition	Condition 元素可以不配置，若配置，则包含元素不能为空。 Condition 中可包含的元素：KeyPrefixEquals（重定向请求时匹配的文件名前缀）、HttpErrorCodeReturnedEquals（重定向请求时匹配的 HTTP 错误码）。 ● 当某一元素存在多条值时以最后一条为准。 ● 当 KeyPrefixEquals 和 HttpErrorCodeReturnedEquals 存在时，需要同时匹配时才生效。 ● 如果 Condition 未配置，相当于匹配所有规则。
Redirect	Redirect 必须配置。Redirect 可以为空，可以包含元素。 Redirect 中可包含的元素：Protocol（重定向请求时使用的协议，取值 *http* 或 `https`）、HostName（重定向请求时使用的站点名）、ReplaceKeyPrefixWith（描

	述重定向请求时使用的文件名前缀）、ReplaceKeyWith（重定向请求时使用的文件名）。 ● 当某一元素存在多条值时，以最后一条为准。 ● ReplaceKeyPrefixWith 和 ReplaceKeyWith 不能同时存在。

- 托管模式为重定向请求：需要设置重定向的存储桶访问域名或者 URL，所有到达该存储桶的请求将被重定向到该地址。例如，你将重定向页面配置为 www.ctyun.cn，所有到您域名（如 http://your***domain.com）的请求，都会重定向到 www.ctyun.cn。

5.1.9 日志

在“存储桶列表”页面点击“属性”>“日志”，进入“日志”页面。在该页面，用户可以为存储桶配置日志功能。

日志功能可以帮助您记录所有操作记录，您可以选择“启用”或“禁用”用户日志功能，同时还可以通过设置目标存储桶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》。

项目	描述
日志类型	日志类型为本地日志。
状态	是否启用日志功能记录对该 Bucket 的所有操作： ● 启用 ● 禁用
前缀	日志的前缀名称。
目标存储桶	日志存储的目标存储桶，可以根据下拉框进行选择目标存储桶。

5.1.10 生命周期

在“存储桶列表”页面点击“属性”>“生命周期”，进入“生命周期”页面。在该页面，用户可以配置生命周期规则。

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文件。当文件的生命周期到期时，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。文件到期被删除后，用户将不需要为到期的文件付费。OOS 删除到期文件后，会在 Bucket log 中记录一条日志，操作项是"OOS.EXPIRE.OBJECT"。

  注意：如果文件的生命周期规则设置的是到期后删除，文件到期后将被永久删除，无法恢复。

- 将与生命周期规则匹配的文件由标准存储转换为低频访问存储，可以根据需要设置生命周期规则从文件最后一次修改生效，还是从文件最后一次访问时间生效。OOS 转换存储类型为低频访问存储后，会在 Bucket log 中记录一条日志，操作项是"OOS.TRANSITION_SIA.OBJECT"。

项目	描述
规则名称	生命周期规则名称。
适用范围	生命规则适用的范围。
规则	生命周期规则详情。
状态	生命周期规则的状态： ● 启用 ● 禁用
操作	可以启用/禁用、修改、删除指定的生命周期规则。

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文件最后一次修改时间或最后一次访问时间多少天后生效。 ● 日期：生命周期规则生效日期，对于最后一次修改时间在此日期之前的文件执行生命周期规则。
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，符合该前缀的文件执行生命周期规则。不符合的不执行生命周期规则。 ● 整个存储桶：创建的生命周期规则适用该存储桶内的所有文件。
转换到低频访问文件	匹配生命周期规则的文件，到期后转换成低频访问文件。 ● 如果“文件转换策略”为“天数”，可以选择文件： ■ 最后一次修改时间：指定在文件最后一次修改后多少天，根据生命周期规则，文件转为低频访问存储。 ■ 最后一次访问时间：指定在文件最后一次访问后多少天，根据生命周期规则，文件转为低频访问存储。 ● 如果“文件转换策略”为“日期”，则在此日期之前修改的文件，将在此日期转换为低频访问存储。
删除文件	匹配生命周期规则的文件，到期后删除。 ● 如果“文件转换策略”为“天数”，指定在文件最后一次修改后多少天，文件被删除。 ● 如果“文件转换策略”为“日期”，则在此日期之前修改的文件，将在此日期被删除。

注意：

- 如果存储桶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。

- 如果存储桶内的生命周期规则正在执行时被修改配置，则修改后的配置并不立即生效，需等原生命周期规则执行完成后才能生效。
- 每个存储桶最多创建 1000 条生命周期规则。
- 同一存储桶，同一类型（到期删除或者到期转成低频访问存储）的生命周期规则不能存在叠加前缀，例如已创建到期删除文件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 的到期删除文件的生命周期规则。
- 当用户为存储桶设置了生命周期规则，这些规则将同时应用于已有文件和后续新创建的文件。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 天前的文件都加入到待删除队列中。

OOS 通过将文件的最后一次修改时间或者最后一次访问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，一个文件的最后修改时间为 GMT 2016 年 1 月 15 日 10:30，生命周期为 3 天，那么文件的到期时间是 GMT 2016 年 1 月 19 日 00:00。如果文件在上传之后没有修改过，则最后修改时间为该文件的上传时间。

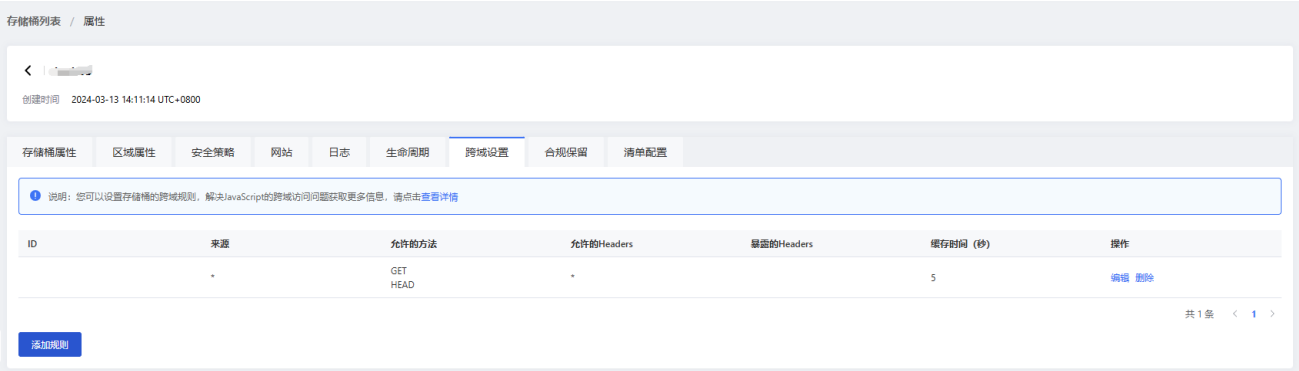
5.1.11 跨域设置

在“存储桶列表”页面点击“属性”>“跨域设置”，进入“跨域设置”页面。在该页面，用户可以设置存储桶的跨域规则。

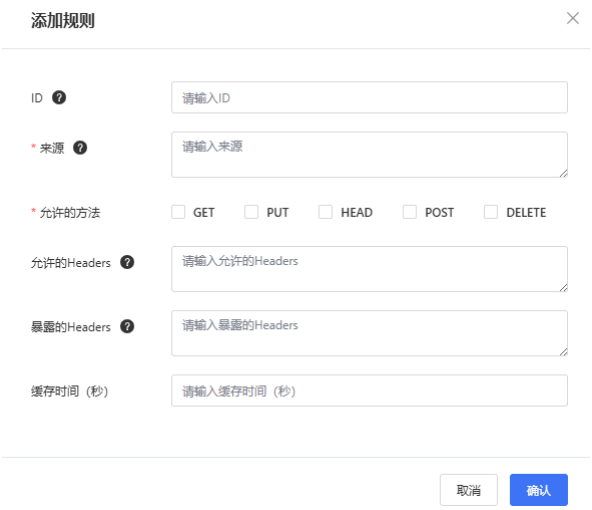
浏览器限制脚本内发起跨源 HTTP 请求，即同源策略。例如，当来自于 A 网站的页面中的 JavaScript 代码希望访问 B 网站的时候，浏览器会拒绝该访问，因为 A、B 两个网站是属于不同的域。通过配置 CORS，可以解决不同域相互访问的问题，CORS 定义了客户端 Web 应用程序在一个域中与另一个域中的资源进行交互的方式。

以下是有关使用 CORS 的示例场景：

- 场景 1：比如用户的网站 www.exam***ple.com，后端使用了 OOS。在 web 应用中提供了使用 JavaScript 实现的上传文件功能，但是在该 web 应用中，只能向 www.exam***ple.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.exam***ple.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.exam***ple.com 中转。
- 场景 2：假设用户在名为 website 的存储桶中托管网站，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 (存储在此存储桶中)，通过 OOS API endpoint oos-xx.ctyunapi.cn 向存储桶发送 GET 和 PUT 请求。浏览器通常会阻止 JavaScript 发送这些请求，但借助 CORS，用户可以配置存储桶支持来自 website.oos-website-cn.oos-xx.ctyunapi.cn 的跨域请求。



点击**添加规则**可以增加新的跨域访问规则：



项目	描述
ID	规则的唯一标识，最长 255 个字符，选填。
来源	允许跨域的源。 可以指定多个，每行一个，每行最多有一个使用通配符（*）。
允许的方法	允许跨域的请求：GET、PUT、HEAD、POST、DELETE。
允许的 Header	通过 Access-Control-Request-Headers 请求头，指定预检 OPTIONS 请求中允许的请求头。 可以指定多个，每行一个，每行最多有一个使用通配符（*）。
暴露的 Header	指定客户应用程序(例如，JavaScript XMLHttpRequest 文件)能够访问的响应头。 可以指定多个，每行一个，不能使用通配符（*）。
缓存时间（秒）	指定浏览器对特定资源的预检（OPTIONS）请求返回结果的缓存时间，单位为秒。

5.1.12 合规保留

在“存储桶列表”页面点击“属性”>“合规保留”，进入“合规保留”页面。在该页面，可以添加合规保留规则，为存储桶启用合规保留功能。合规保留启用后，对存储桶内的所有文件生效。

项目	描述
规则类型	项目类型为合规保留。
适用范围	合规保留规则的适用范围，目前为整个存储桶。
规则	合规保留的天数。
状态	合规保留规则的启用状态： ● 启用 ● 禁用
操作	可以对合规保留规则进行操作。未启用前，可以对规则进行启用、编辑和删除。启用后只能对规则进行编辑，设置合规保留时长大于或等于上次设置的时长，才能生效。

注意：启用存储桶合规保留功能后，任何用户（包括根用户）都不能对此存储桶内处于合规保留期的文件进行修改和删除。

可以按照下列步骤启用合规保留规则：

1. 点击“添加规则”，添加合规保留。如果已经添加了合规保留且未启用，可以点击“操作”列的“编辑”，进行修改，如果不修改，直接跳到步骤 3 启用合规保留。

2. 输入保留周期，点击“确认”后，会进行二次确认，是否要创建合规保留。

3. 点击“确认”后，合规保留规则创建成功。

说明：合规保留创建后，默认是禁用状态，需要用户启用后，才能生效。合规保留未启用时，可以对合规保留时长进行编辑。

4. 点击“启用”后，输入启用合规保留的存储桶名称，为该存储桶启用合规保留。

5. 点击“确认”后，合规保留启用成功。

注意：

- 合规保留一旦启用，不能关闭，不能缩短合规保留时长，但可以通过编辑延长合规保留时长。
- 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，文件 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文件。
- 处于合规保留期的文件，无法通过调用 API、控制台修改文件的存储类型，只能通过生命周期修改存储类型。
- 处于合规保留期的文件，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需过了合规保留期后才能生效。

5.1.13 清单配置

在“存储桶列表”页面点击“属性”>“清单配置”，进入“清单配置”页面。在该页面，用户可以配置存储清单功能。

通过 OOS 存储桶清单功能可以获取存储桶中指定文件（Object）的大小、存储类型等信息。相对于 GET Bucket (List Objects)接口，存储桶清单可以按每天或者每周以 CSV 的形式输出指定文件的相关信息，且不会影响存储桶的请求速率。在需要列举海量文件的场景中，推荐使用存储桶清单功能。

说明：每个存储桶最多配置 10 条清单规则。配置清单的存储桶和存储清单结果文件的存储桶可以不同。

项目	描述
规则名称	清单名称。
文件前缀	清单规则匹配的文件前缀。
存储清单的存储桶	目标存储桶，导出的清单结果存放在此存储桶。
清单报告存储路径	清单结果文件的存储路径前缀。
导出频率	清单结果导出的周期。
上次导出	上次导出清单结果的时间。
操作	可以对清单规则进行停用/启用、编辑、删除。

点击“添加规则”，可以添加 Bucket 清单规则。

说明：*表示必填字段，不带*表示可选字段。

名称	描述
规则名称	清单名称。清单名称在当前存储桶下必须唯一。 取值：只允许使用小写字母、数字、短横线（-）和下划线（_），且不能以短横线（-）或下划线（_）开头或结尾，1~64 个字符。
文件前缀	清单规则匹配的文件前缀。 取值：0~1024 个字符。
存储清单的存储桶	目标存储桶，导出的清单结果存放在此存储桶。 配置清单的存储桶和存储清单结果文件的存储桶可以相同，也可以不同。
清单报告存储路径	清单结果文件的存储路径前缀。 ● 如果将清单结果文件直接保存在存储桶根目录下，这项不填写。 ● 如果将清单结果文件保存在存储桶非根目录下，需要填写不包括 Bucket 名

	字在内的完整路径。 例如将清单结果文件保存在存储桶 example 的 dir 目录下，该字段填写 dir；如果保存在存储桶 example 的 dir/dir1 目录下，则该字段填写 dir/dir1。 取值：0~512 个字符。
导出频率	清单结果导出的周期。 ● 每天：按天导出清单文件。 ● 每周：按周导出清单文件。清单规则开启当天会根据清单规则启动一次清单导出任务，第二天启动周期性清单导出任务。例如周一开启清单规则，周一当天会启动清单导出任务，后期会按每周二启动清单导出任务。 **说明**：当前的清单结果文件导出完成后，才会创建新的清单任务。如果文件较多时（数量大于 10 亿），建议按周导出清单结果文件。
清单内容可选信息	设置清单结果中包含配置项，可以设置多个配置项： ● 文件大小：文件的大小。 ● 存储类型：文件的存储类型。 ● 最后更新日期：文件的最后一次修改时间。 ● ETag：文件的 ETag 值，用于标识文件的内容。 ● 分片上传状态：是否为通过分片上传方式上传的文件。 **说明**：如果未设置配置项，清单默认输出源存储桶和 Key（文件名称）。

存储桶清单配置后，清单结果文件会按指定的周期输出，按下列目录结构输出：

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

名称	描述
dest_bucket	该目录为清单的目标存储桶，清单结果将存储在此存储桶。
destination-prefix	该目录为清单结果的存储路径前缀。如果清单规则配置的时候未指定该前缀，则省略该目录。
src_bucket	该目录为源存储桶，即配置清单的存储桶。
inventory_id	该目录为清单名称。
YYYY-MM-DDTHH-MMZ	该目录为开始扫描源存储桶的时间，格林威治时间戳，如 2023-08-24T16-00Z。该目录下包含了 manifest.json 和 manifest.checksum 文件。
manifest.json	提供了有关清单的元数据和其他基本信息，其中包含清单结果压缩文件的 MD5 值，待清单结果文件生成后，才会生成汇总清单结果文件的 manifest 文件。
manifest.checksum	包含 manifest.json 文件 MD5 值的文件。
data	该目录下存放了清单结果文件，清单结果文件格式为使用 GZIP 压缩的 CSV 文件。 **注意**：当源存储桶中文件数量较多时，为方便用户下载和处理数据，程序会自动将清单文件切分成多个 CSV 压缩文件。CSV 压缩文件按照 *uuid*.csv.gz、*uuid*-1.csv.gz、*uuid*-2.csv.gz 的顺序依次递增。您可以从 manifest.json 文件中获取 CSV 文件列表，然后按照以上顺序依次解压 CSV 文件并读取清单数据。每个文件只会出现在一个清单结果文件中。
UUID.csv.gz	清单结果文件，存储在 data 文件夹中，包含清单功能导出的文件信息。报告以.csv.gz 的格式进行存储，可能存在多个清单结果文件，每生成一个，就在 data 目录下新增一个文件。

manifest.json：提供了有关清单的元数据和其他基本信息。示例如下：

```
{
    "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"
}
```

manifest.json 描述

名称	描述
destinationBucket	存放清单结果的目标存储桶。
fileSchema	清单结果包含的字段： ● Bucket：清单文件所在的存储桶。 ● Key：清单文件名称。 ● Size：文件大小。 ● StorageClass：文件的存储类型。 ● LastModifiedDate：文件最后一次修改日期。 ● ETag：文件的 ETag 值。 ● IsMultipartUploaded：文件是否通过分片上传生成。如果是，则该字段值为 TRUE，否则为 FALSE。 **说明**：用户在“清单内容可选信息”配置了 Size、StorageClass、LastModifiedDate、ETag、IsMultipartUploaded，fileSchema 中才会出现对应字段。
creationTimestamp	扫描源存储桶的时间，UNIX 时间戳，精确到毫秒。
files	清单结果文件的内容： ● MD5checksum：清单结果文件的 MD5。

	● size：清单结果文件的大小，单位字节。 ● key：清单结果文件的名称，格式为：*destination-prefix*/*src_bucket*/*inventory_id*/data/*文件名*，用户配置了 *destination-prefix*，*destination-prefix* 才会出现在路径中。
sourceBucket	源存储桶，即配置清单规则的存储桶。
version	清单版本号，值为 2023-08-30。
fileFormat	清单结果文件格式。

清单结果输出内容如下例所示，该例为“清单内容可选信息”中选择了所有可选信息输出的示例：

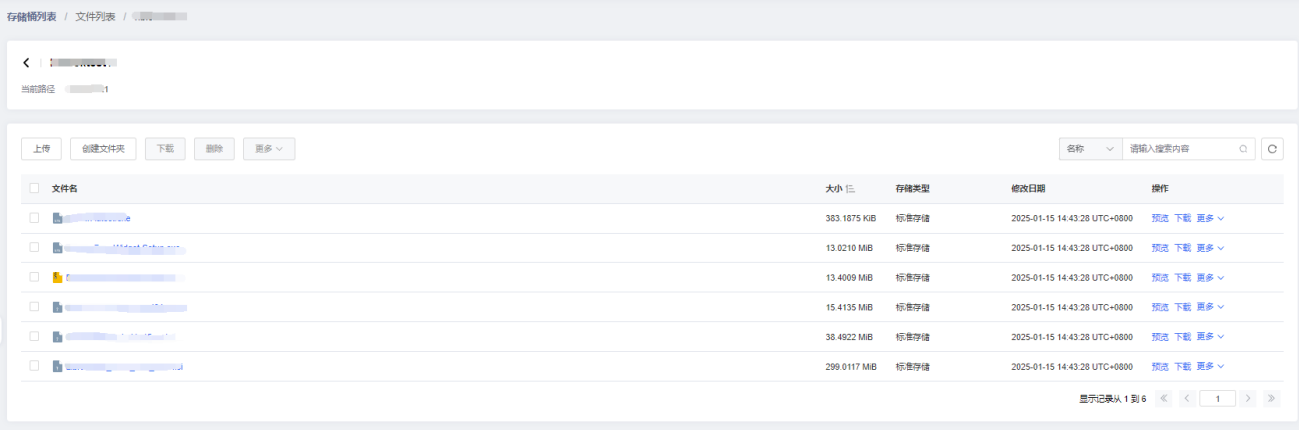
	A	B	C	D	E	F	G
1		1.txt	6060576	Standard	2023-05-2	6F7A30A13	TRUE
2		1%2F	0	Standard	2023-05-2	D41D8CD98	FALSE
3		1%2F1.txt	5	Standard	2023-05-2	D5397F149	FALSE
4		1%2F2.txt	3	Standard	2023-05-2	202CB962A	FALSE
5		1%2F3.txt	3	Standard	2023-05-2	202CB962A	FALSE
6		1%2F4.txt	3	Standard	2023-05-2	202CB962A	FALSE
7		1%2F5.txt	3	Standard	2023-05-2	202CB962A	FALSE
8		2%2F	0	Standard	2023-05-2	D41D8CD98	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

清单结果从左到右字段分别是：

字段名称	描述
Bucket	清单文件所在的存储桶。
Key	清单文件名称。 文件名称使用 URL 编码，需要用户自行解码查看。
Size	文件大小。
StorageClass	文件的存储类型： ● Standard：标准存储。 ● Standard_IA：低频访问存储。
LastModifiedDate	文件最后一次修改日期。

ETag	文件的 ETag 值。 文件创建的时会生成一个 ETag 值，用于标识文件的内容。
IsMultipartUploaded	文件是否通过分片上传生成： ● TRUE：通过分片上传。 ● FALSE：不是通过分片上传。

5.2 文件管理

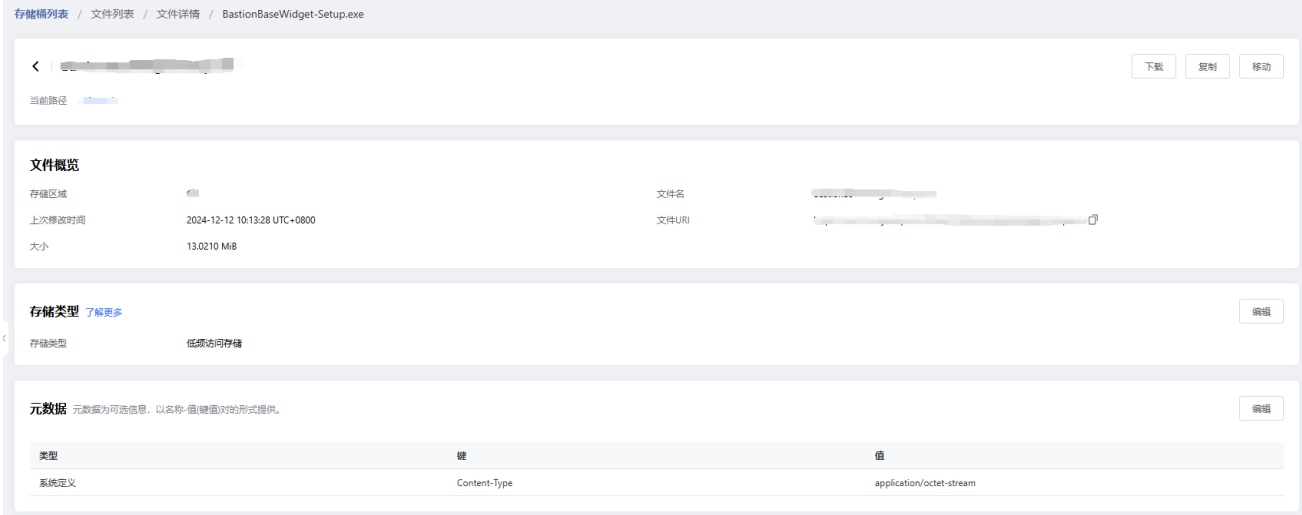


对于 IAM 子用户，拥有相应的权限才可以在控制台对文件进行操作，操作和需要拥有的权限如下：

操作	需具备的权限
上传文件	oos:ListAllMyBucket、oos:ListBucket、oos:PutObject
文件下载	oos:ListAllMyBucket、oos:ListBucket、oos:GetObject
管理文件元数据	oos:ListAllMyBucket、oos:ListBucket、oos:GetObject、oos:PutObject
文件预览	oos:ListAllMyBucket、oos:ListBucket、oos:GetObject
文件分享	oos:ListAllMyBucket、oos:ListBucket、oos:GetObject
创建文件夹	oos:ListAllMyBucket、oos:ListBucket、oos:PutObject
删除文件	oos:ListAllMyBucket、oos:ListBucket、oos:DeleteObject
删除文件夹	oos:ListAllMyBucket、oos:ListBucket、oos:DeleteMultipleObjects
移动文件	源和目的都需要的权限：oos:ListAllMyBucket、oos:ListBucket 对于源文件需要具有的权限：oos:GetObject、oos:DeleteObject 对于目的端需要的权限：oos:PutObject
修改存储类型	oos:ListAllMyBucket、oos:ListBucket、oos:GetObject、oos:PutObject
复制文件	源和目的都需要的权限 oos:ListAllMyBucket、oos:ListBucket 对于源文件需要具有的权限：oos:GetObject 对于目的端需要的权限：oos:PutObject
搜索文件	oos:ListAllMyBucket、oos:ListBucket
文件排序	oos:ListAllMyBucket、oos:ListBucket

5.2.1 查看文件详细信息

在“存储桶列表”页面，点击对应的存储桶，进入“文件列表”。点击具体的文件，可以查看文件的详细信息。



名称	描述
文件概览	可以查看下列信息： ● 存储区域：文件存储的数据位置 ● 文件名。 ● 上次修改时间：文件最近一次的修改时间。 ● 文件 URI：文件具体的 URI。 ● 大小：文件的大小。
存储类型	文件的存储类型： ● 标准存储 ● 低频访问存储
元数据	文件的具体元数据信息。详细参见**管理文件元数据**。

5.2.2 上传文件

说明：

- 通过控制台上传的文件大小有限制，单个文件不能超过 5GiB。若用户需要上传大于 5GiB 的文件时，可以通过 API 访问 OOS 服务进行上传。
- 通过控制台上传文件，最多支持 500 个文件同时上传。
- 上传文件时，遇到同名文件，新上传的文件会覆盖原来的文件。

在“存储桶列表”页面，点击对应的存储桶，进入“文件列表”，在该页面，可以上传文件。点击“上传”，弹出“上传文件”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。

项目	描述
当前位置	文件上传的位置。
存储类型	文件的存储类型： ● 标准存储：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。如果上传文件时未指定存储类型，OOS 默认使用标准存储。 ● 低频访问存储：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：低频访问存储的文件有最短存储时间，存储时间短于 30 天的文件被提前删除或变更时，会产生一定费用。 ■ 最小计费大小：低频访问存储文件有最小计费大小，即如果文件大小低于 64KiB，会按照 64KiB 计算收费，文件大于等于 64KiB 按照实际存储收费。 ■ 数据取回：获取低频访问存储数据时会产生数据取回费用。
选择文件	可以通过将目录或文件拖到浮窗上传文件，也可以点击**添加文件**、**添加文件夹**按钮上传文件。 上传的文件中如果想移除的，可以勾选对应的文件，点击**移除**按钮，进行文件移除。 **说明**：在查找框中可以模糊匹配查找上传的文件。
元数据	用户可以编辑上传文件的文件元数据信息，具体元数据信息详见**管理文件元数据**。

可以按照下列方式上传文件：

- 将本地目录或多个文件拖到浮窗中，控制台将您拖进浮窗的文件自动上传至 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

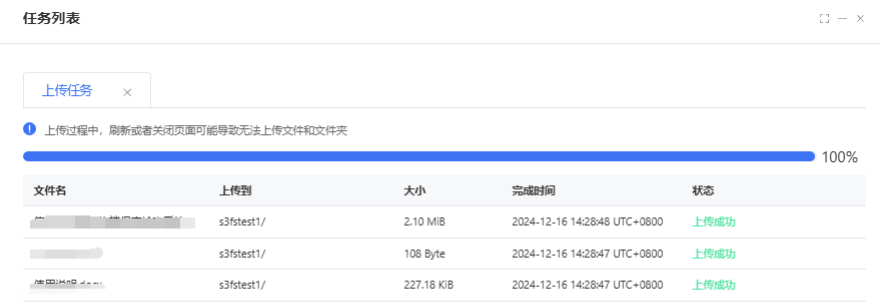
  Photo/20190102/2.jpg

- 点击“添加文件”按钮，弹出上传文件的对话框，可以选择一个或多个文件进行上传。

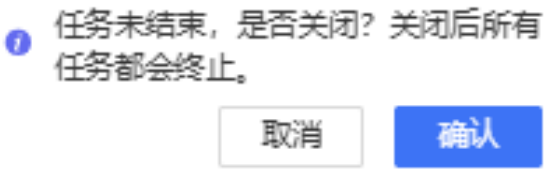
- 点击“添加文件夹”按钮，弹出上传文件的对话框，可以选择需要上传的文件夹。

文件上传过程中，可以查看各文件上传状态：

- 上传中，状态为文件上传的进度。
- 还未进行上传，状态为“等待中”。
- 上传成功，状态为“上传成功”。
- 上传失败，状态位“上传失败”。



上传过程中，如果关闭上传的对话框，弹出提示信息框。

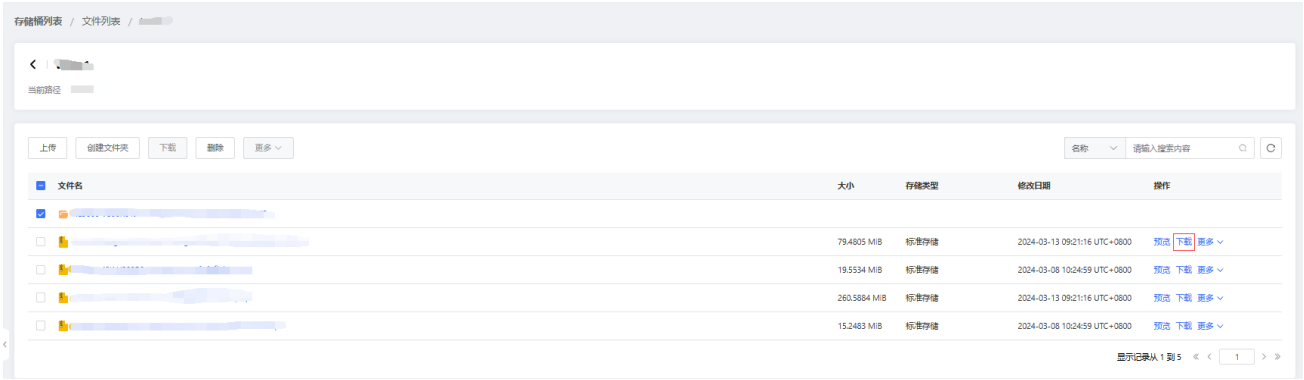


- 确认：关闭，结束上传。
- 取消：继续上传文件。

5.2.3 下载文件

在“存储桶列表”页面，点击对应的存储桶，进入“文件列表”，在该页面，可以下载文件。点击操作列的“**下载**”，可以下载单个文件。选中一个或者多个文件，点击上方导航的“**下载**”，可以批量下载文件。

注意：基于安全合规要求，禁止通过 OOS 默认域名以匿名或者 URL 签名方式下载后缀为 apk、ipa 的文件，在 Header 中包含签名或者通过自定义域名方式下载此类文件不受影响。



5.2.4 管理文件元数据

元数据是对文件的属性描述，包括系统定义元数据（System Meta）和用户自定义元数据（User Meta）两种。您可以通过编辑元数据来管理文件的属性。

用户可以修改的系统定义元数据

注意：系统定义元数据取值请按照 HTTP 标准进行填写。

字段	描述
Cache-Control	指定文件的缓存行为。 取值： ● no-cache：不直接使用缓存，而是先去服务端验证文件是否已更新。如果文件已更新，说明本地缓存已过期，需从服务端重新下载文件；如果文件未更新，表明本地缓存未过期，此时使用本地缓存。 ● no-store：文件不会被缓存。 ● public：文件允许被任何中间者（可能是代理服务器、类似于 cdn 网络）缓存。 ● private：文件只能被获取它的终端缓存。它不允许任何中间者（intermediate）缓存响应的资源。 ● max-age=<seconds>：缓存文件的相对过期时间，单位为秒。此选项仅在 HTTP 1.1 中可用。
Content-Disposition	指定文件的展示形式。 取值：

	● Content-Disposition:inline：直接预览文件内容。 ● Content-Disposition:attachment：以原文件名的形式下载到浏览器指定路径。 ● Content-Disposition:attachment; filename="*FileName*"：以自定义文件名的形式下载到浏览器指定路径。 *FileName*：用于自定义下载后的文件名称，例如 example.jpg。 将文件下载到浏览器指定路径时： ● 如果文件名称包含星号（*）、正斜线（/）等特殊字符时，可能会出现特殊字符转义的情况。例如，下载 test*.jpg" 到本地时，test*.jpg"可能会转义为 test .jpg"。 ● 若需确保下载名称中包含中文字符的文件到本地指定路径后，文件名称不出现乱码的现象，您需要将名称中包含的中文字符进行 URL 编码。例如，将“中文.txt”从 OOS 下载到本地后，需要保留文件名为“中文.txt”，需按照 "attachment;filename="+URLEncoder.encode("中文","UTF-8")+".txt;filename*=UTF-8""+URLEncoder.encode("中文","UTF-8")+".txt")的格式设置 Content-Disposition，即 attachment;filename=%E4%B8%AD%E6%96%87.txt;filename*=%E4%B8%AD%E6%96%87.txt。
Content-Encoding	指定文件的编码方式。需要按照文件的实际编码类型填写，否则可能造成客户端（浏览器）解析编码失败或文件下载失败。若文件未编码，不增加此项。 取值： ● identity：表示文件未经过压缩或编码。 ● gzip：表示文件采用 Lempel-Ziv（LZ77）压缩算法以及 32 位 CRC 校验的编码方式。 ● compress：表示文件采用 Lempel-Ziv-Welch（LZW）压缩算法

	的编码方式。 ● deflate：表示文件采用 zlib 结构和 deflate 压缩算法的编码方式。 ● br：表示文件采用 Brotli 算法的编码方式。 默认值为 identity。 关于 Content-Encoding 的更多信息参见 RFC2616。
Content-Type	指定文件的内容类型。 用于定义文件的类型和网页的编码。如果没有指定文件类型，则根据文件的扩展名生成。如果文件没有扩展名，则文件类型的默认值 application/octet-stream。
Content-Language	声明文件内容使用的语言。例如某个文件使用简体中文编写，则此项可设置为 zh-CN。
Expires	缓存内容的绝对过期时间，格式是格林威治时间（GMT）。 例如 Wed, 22 Nov 2023 14:18:58 +0800。如果 Cache-Control 设置了 max-age=<seconds>，以 max-age=<seconds>为准。
x-amz-website-redirect-location	将相关联文件的请求重定向到同一存储桶中的其他文件或外部 URL。此值对于每个单独文件都是唯一的，原定设置情况下不会复制该值。更多信息请参考的 POST Object。

可以修改的用户定义元数据

字段	描述
x-amz-meta-*	用户自定义元数据。键（key）必须为 ASCII 中可打印字符的部分值，不支持的字符详见下表。值（Value）为除（space）外的 ISO 8859-1 以内的字符。

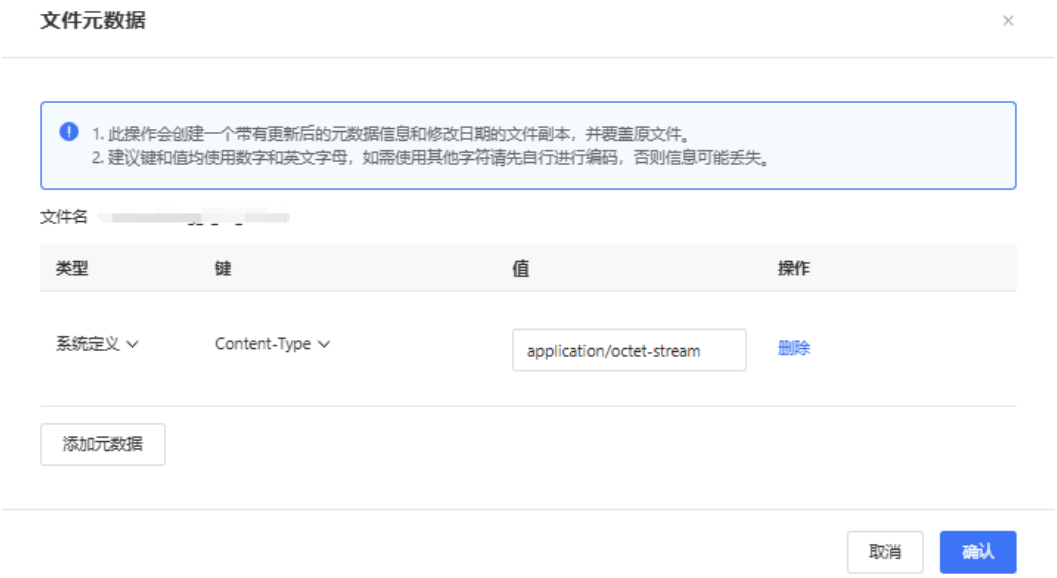
用户定义元数据取值：95 个可打印字符中不可取的值

ASCII 十进制	图形	ASCII 十进制	图形
32	（space）	61	=
34	"	62	>
40	(	63	?

41	)	64	@
44	,	91	[
47	/	92	\
58	:	93	]
59	;	123	{
60	<	125	}

点击文件列表中的“更多”>“编辑元数据”或“更多操作”>“编辑元数据”，可以进行对文件的元数据进行编辑。

说明：如果同时选择多个文件编辑元数据，则不会显示文件的原有元数据信息。如果文件存在已有元数据的键（key）与本次添加元数据的键（key）相同，则其值（value）会更新为最新的值，该文件其他历史元数据均会保留。



点击“添加元数据”，可以修改文件的系统定义元数据或用户定义元数据。

名称	描述
类型	元数据的类型： ● 系统定义 ● 用户定义

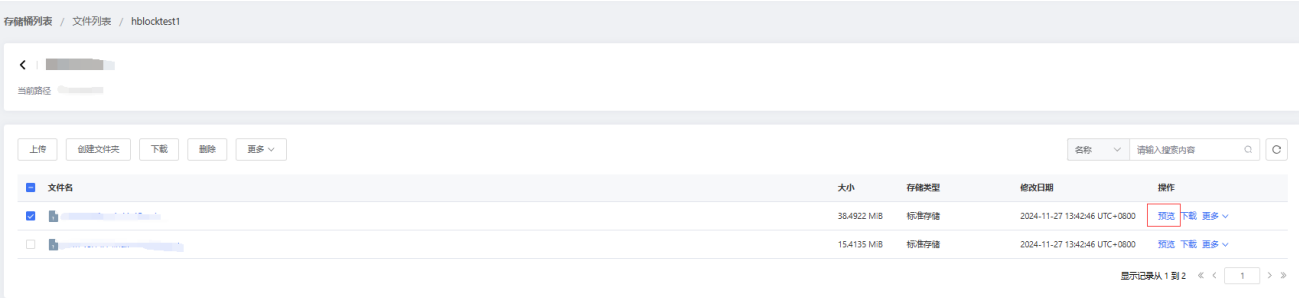
键	具体元数据名称。 元数据为系统定义时，取值： ● Cache-Control ● Content-Disposition ● Content-Encoding ● Content-Type ● Content-Language ● Expires ● x-amz-website-redirect-location 元数据为用户定义时，取值：x-amz-meta-*。
值	对应元数据的具体取值。
操作	点击“删除”按钮，可以删除该元数据。

5.2.5 文件预览

在“存储桶列”表页面，点击对应的存储桶，进入“文件列表”，在该页面，可以预览文件。点击文件“操作”列的“预览”按钮，可以预览文件。

注意：

- 基于安全合规要求，禁止通过 OOS 默认域名预览后缀为 apk、ipa 的文件，在 Header 中包含签名或者通过自定义域名方式下载此类文件不受影响。
- 预览的文件为图片或网页时，会以附件的形式下载到本地。



5.2.6 文件分享

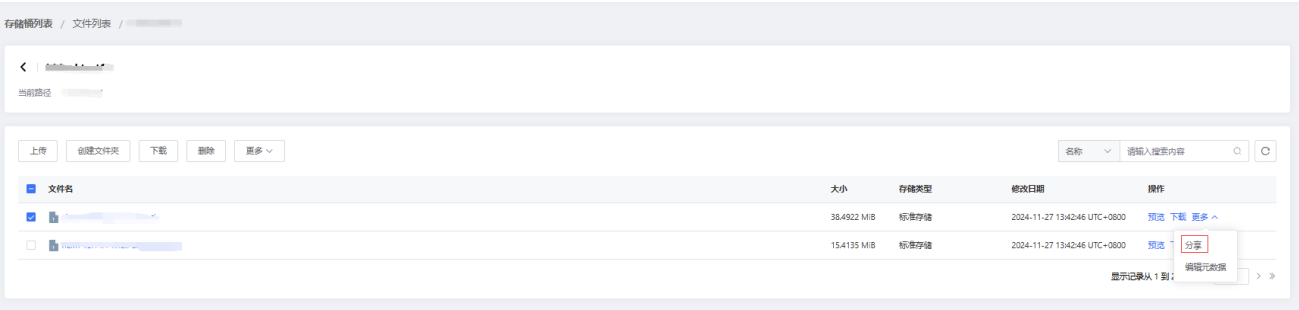
在“存储桶列表”页面，点击对应的存储桶，进入“文件列表”，在该页面，可以分享文件。通过文件分享，可以分享单个文件或者多个文件。

注意：基于安全合规要求，禁止通过 OOS 默认域名以匿名或者 URL 签名方式下载后缀为 apk、ipa 的文件，在 Header 中包含签名或者通过自定义域名方式下载此类文件不受影响。

5.2.6.1 单个文件分享

分享单个文件，选择需要分享的文件，点击对应文件后的“操作”>“更多”>“分享”，或者点击“更多操作”>“分享”，即可对该文件进行分享。

注意：在分享图片或者网页时，访问者会下载到本地查看。



点击“分享”按钮，弹出“文件分享”对话框。

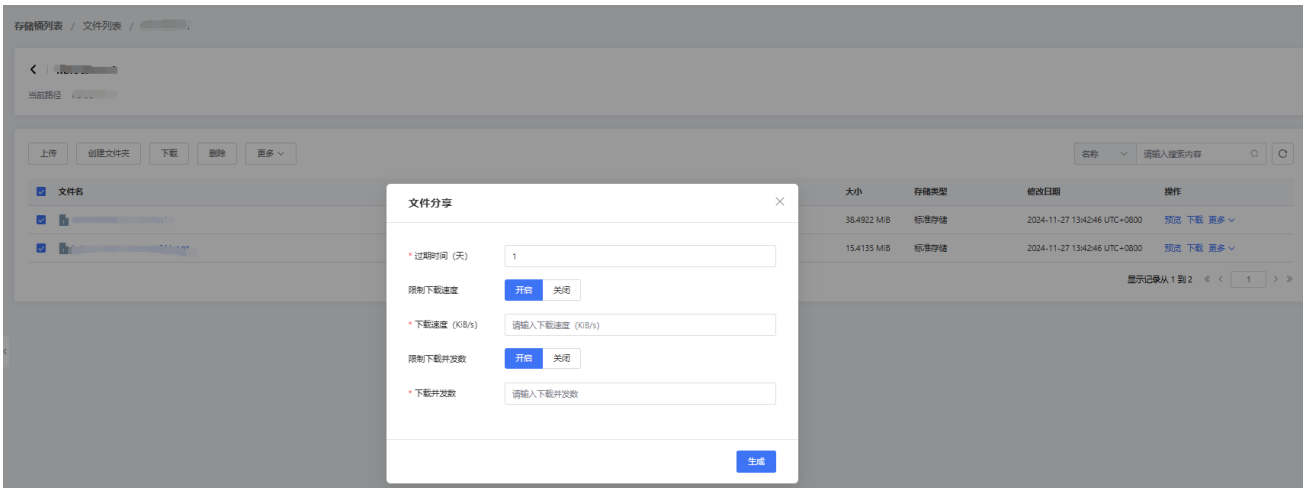
名称	描述
文件名称	要分享的文件名称。
过期时间（天）	设置的过期时间。 取值[1, 9999999]，单位是天。 **说明：**如果不填写，默认分享链接 15 分钟过期。
限制下载速度	是否开启下载速度限制： ● 开启 ● 关闭
下载速度（KiB/s）	下载速度限制。 取值[1, 2147483647]，单位是 KiB/s。

限制下载并发数	是否开启下载并发数限制。
下载并发数	下载并发数。 取值[1，2147483647]。
链接	文件的分享链接。

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 可以访问此文件。

5.2.6.2 批量文件分享

分享多个文件时，选择需要分享的多个文件，点击“更多操作”>“分享”，即弹出“文件分享”对话框。



名称	描述
过期时间（天）	设置的过期时间。 取值[1, 9999999]，单位是天。
限制下载速度	是否开启下载速度限制： ● 开启 ● 关闭
下载速度（KiB/s）	下载速度限制。 取值[1, 2147483647]，单位是 KiB/s。

限制下载并发数	是否开启下载并发数限制。
下载并发数	下载并发数。 取值[1，2147483647]。

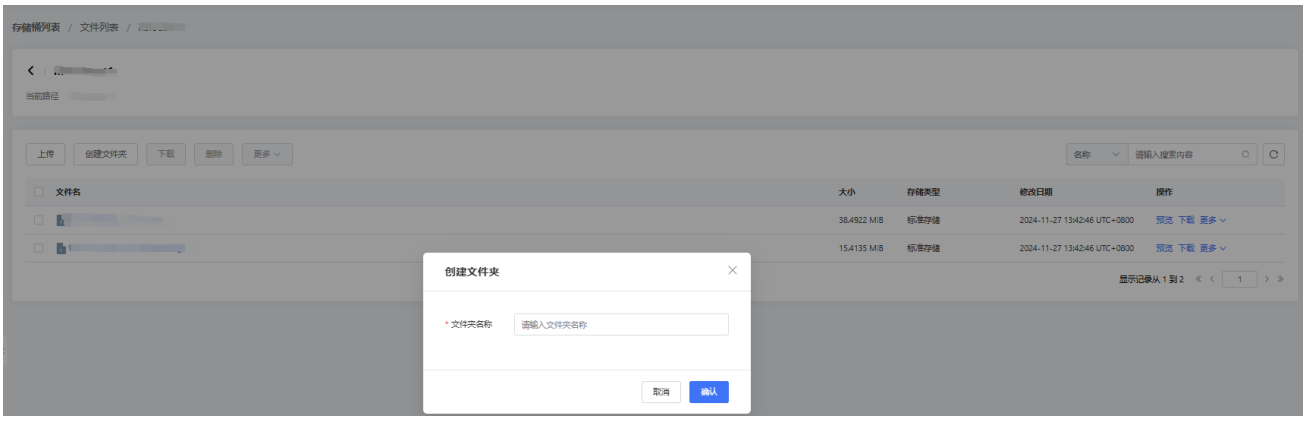
点击**生成**按钮，会生成一个 csv 文件，在 csv 文件中，用户可以查看每个文件的具体分享链接。

5.2.7 创建文件夹

在“存储桶列表”页面，点击对应的存储桶，进入“文件列表”，在该页面，可以创建文件夹。点击“创建文件夹”,在弹窗中设置要创建的文件夹名称，创建后的文件夹可以包含文件（Object）。这里的文件夹并不是文件系统中文件夹的概念。为了方便用户进行数据管理，OOS 提供了一种方式模拟文件夹。实际上 OOS 内部是通过在文件名称中增加“/”，将该文件在管理控制台上模拟成一个文件夹的形式展现。通过 API 列举文件，获取到的文件名以“/”分隔的，最后一个“/”后的内容就是文件名。如果最后一个“/”后没有内容，则表示一个文件夹路径。文件夹的层级结构深度不会影响访问文件的性能。

其中文件夹名称：

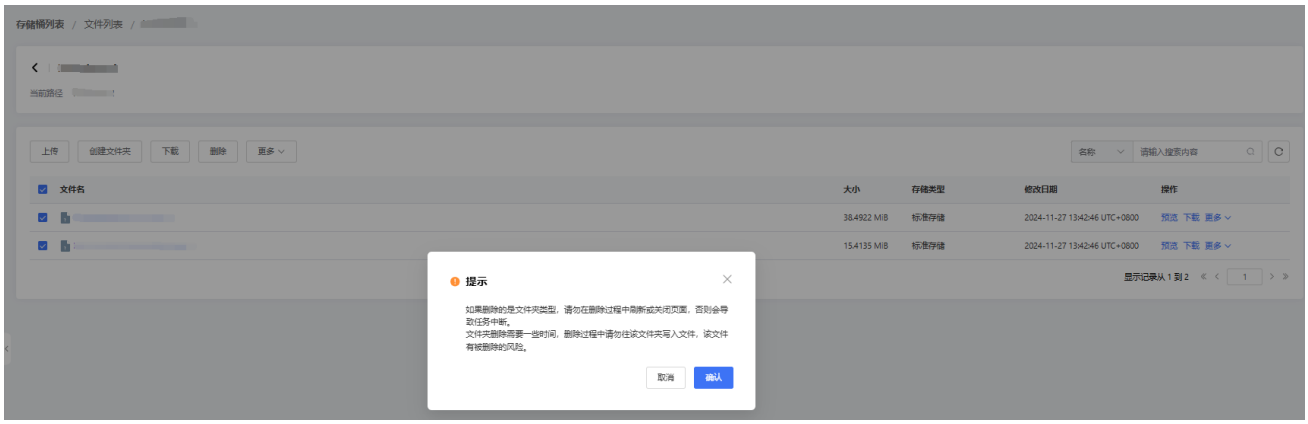
- 不为空 。
- 不包含 ？ " : / ' \ 。
- 不能以 | 开头并且不能以|结尾。
- 不能为：.或者+。



5.2.8 删除文件/文件夹

通过控制台删除文件/文件夹有两种方式：

- 通过控制台手动删除：在“存储桶列表”页面，点击对应的存储桶，进入“文件列表”，在该页面选择需要删除的文件或文件夹，点击“删除”。删除文件或文件夹时，需要用户的二次确认，防止误删。



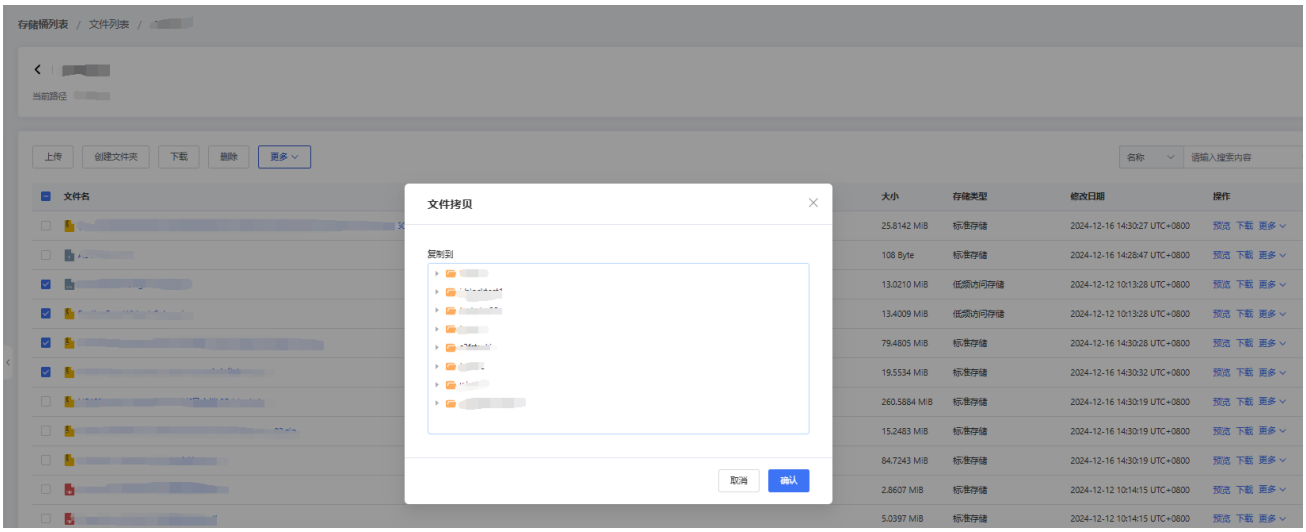
说明：删除文件夹时，会弹出文件夹的删除状态。如果删除失败，会给出失败原因。

- 通过配置生命周期规则进行删除文件或文件夹，详见**生命周期**。

5.2.9 复制文件

在“存储桶列表”页面，点击对应的存储桶，进入“文件列表”，在该页面，可以复制文件。选择需要复制的文件，点击“更多操作”>“复制”，弹出“文件拷贝”窗口，用户可以通过文件拷贝功能将文件复制到其他存储桶（Bucket）中。

注意：使用控制台操作，复制的单个文件不能大于 5 GiB。如果大于 5 GiB，请调用 API 的 PUT Object -Copy 或 Copy Part 接口进行操作。

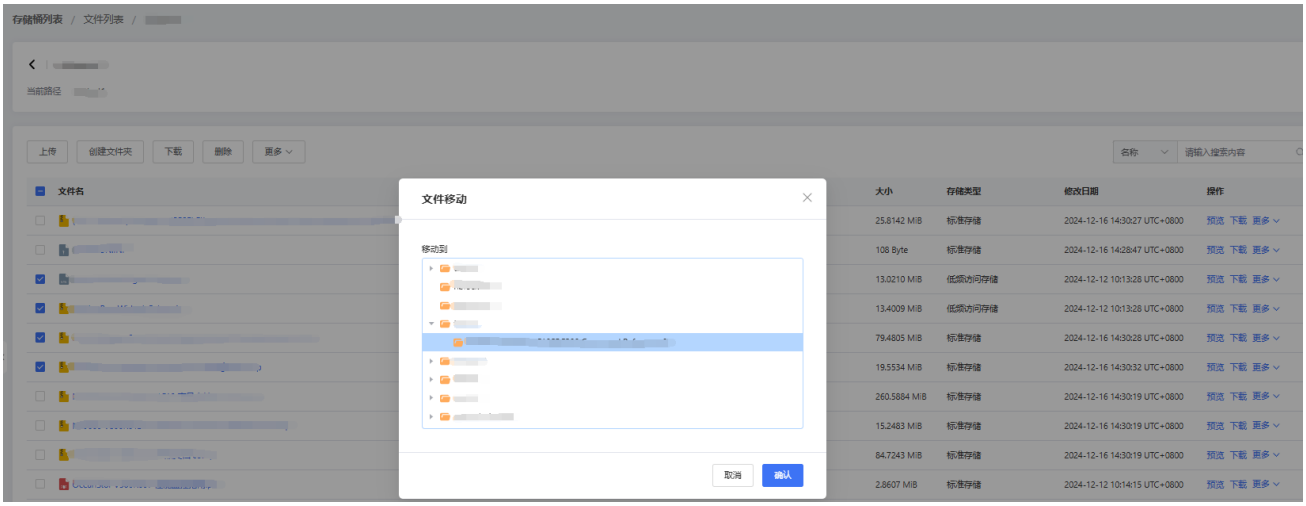


5.2.10 移动文件

在“存储桶列表”页面，点击对应的存储桶，进入“文件列表”，在该页面，可以移动文件到其他存储桶。

选择需要移动的文件，点击“更多操作”>“移动”，弹出“文件移动”窗口，用户可以通过文件移动功能将文件移动到其他存储桶（Bucket）中。

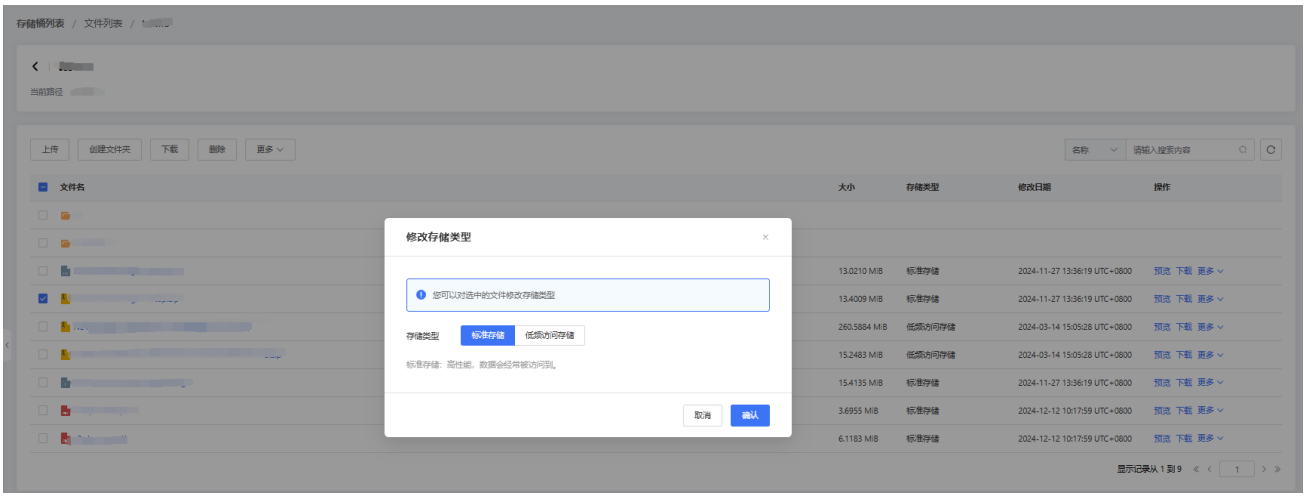
注意：使用控制台操作，移动的单个文件不大于 5 GiB。如果超过 5 GiB，请调用 API 的 PUT Object -Copy 或 Copy Part、DELETE Object 接口进行操作。



5.2.11 修改存储类型

在“存储桶列表”页面，点击对应的存储桶，进入“文件列表”，在该页面，可以修改文件类型。

选择需要修改的文件，点击“更多操作”>“修改存储类型”，弹出“修改存储类型”窗口，对文件的存储类型进行修改。

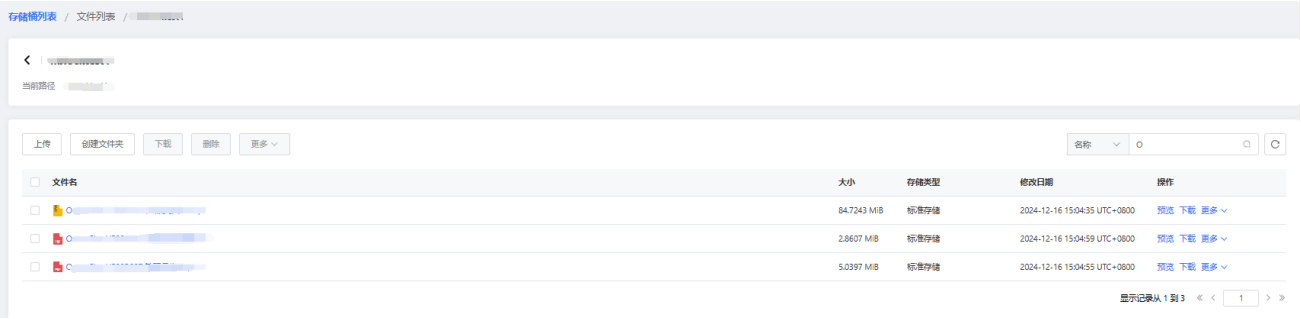


- **标准存储（STANDARD）**：访问时延低、吞吐量高，能够有效支持各种热点类型数据频繁访问。适用于各种音视频服务、图片服务、大型网站、大数据分析等应用的数据存储。标准存储是默认的存储类型。如果上传文件时未指定存储类型，OOS 默认使用标准存储。
- **低频访问存储（STANDARD_IA）**：适合长期保存不经常访问的数据。对于不经常访问但仍需要实时访问的数据，可以采用低频访问存储，例如各类移动应用、智能设备、企业数据的长期备份。
  - 最短存储时间：低频访问存储的文件有最短存储时间，存储时间短于 30 天的文件被提前删除或变更时，会产生一定费用。
  - 最小计费大小：低频访问存储文件有最小计费大小，即如果文件大小低于 64KiB，会按照 64KiB 计算收费，文件大于等于 64KiB 按照实际存储收费。
  - 数据取回：获取低频访问存储数据时会产生数据取回费用。

5.2.12 搜索文件

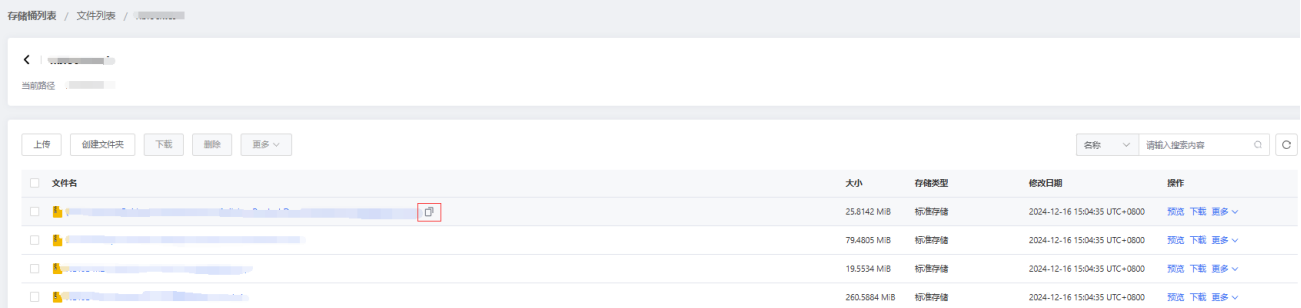
在“存储桶列表”页面，点击对应的存储桶，进入“文件列表”，在该页面，可以通过搜索文件前缀来查找文件或者文件夹。

当用户存储的文件较多时，可以通过搜索文件前缀来查找符合条件的文件和文件夹。



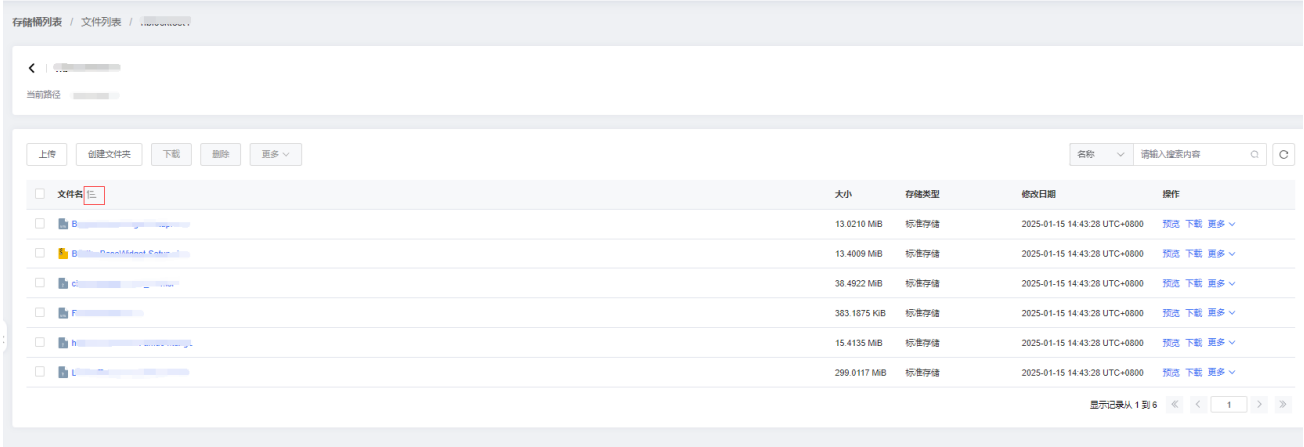
5.2.13 复制文件名称

在“存储桶列表”页面，点击对应的存储桶，进入“文件列表”，在该页面，可以复制文件名。当需要复制文件名称时，可以将鼠标放到需要复制的文件上，文件名称旁会出现一个复制按钮 ，点击该按钮，即可复制该文件名称名。



5.2.14 文件排序

在“存储桶列表”页面，点击对应的存储桶，进入“文件列表”，在该页面，将鼠标放在“文件名”、“大小”或者“修改日期”上，可以对存储桶内已经列举出的文件根据文件名、文件大小或修改日期进行排序，每次只能选择一种排序方式。



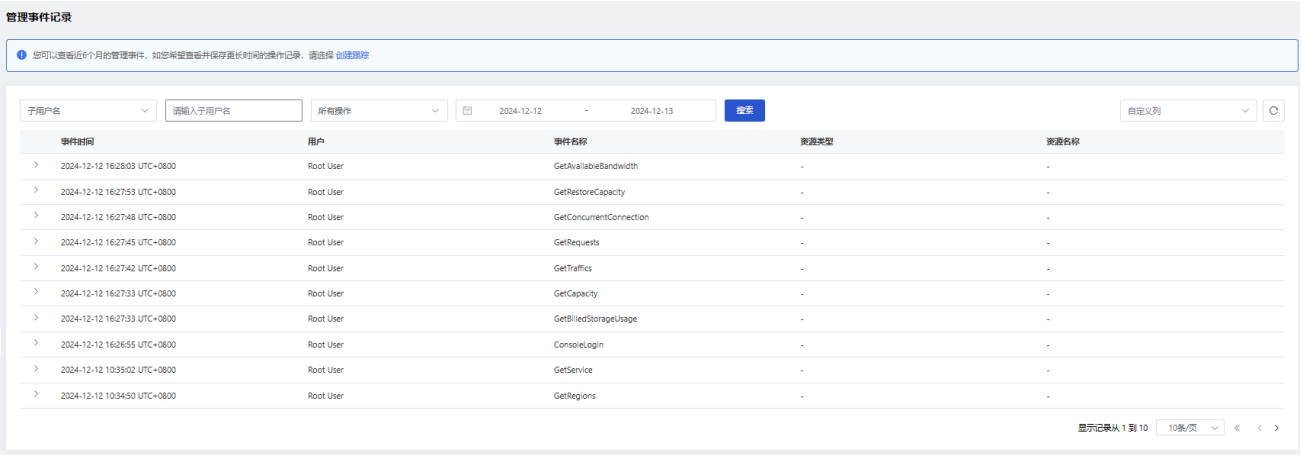
6 操作跟踪

对于 IAM 子用户，拥有相应的权限才可以在控制台对操作跟踪进行操作，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

6.1 管理事件记录

进入“操作跟踪”>“管理事件记录”，可以查看近 6 个月内的管理事件，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，管理事件日志文件将保存在指定的 Bucket 中。



可以根据需要，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。

6.1.1 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： ● 对象存储网络： ■ OOS：oos-cn.ctyunapi.com ■ 操作跟踪：oos-cn-cloudtrail.ctyunapi.cn ■ IAM：oos-cn-iam.ctyunapi.cn ■ 统计 API：oos-cn-mg.ctyunapi.cn ■ 自服务门户：oos-cn.ctyun.cn ● 对象存储网络 2： ■ OOS：oos-cn2.ctyunapi.com ■ 操作跟踪：oos-cn2-cloudtrail.ctyunapi.cn ■ IAM：oos-cn2-iam.ctyunapi.cn ■ 统计 API：oos-cn2-mg.ctyunapi.cn

	■ 自服务门户：oos-cn2.ctyun.cn ● 香港节点： ■ OOS：oos-cnhk-hqnet.ctyunapi.cn（香港精品网）或 oos-cnhk-nqnet.ctyunapi.cn（香港普通网） ■ 操作跟踪：oos-cnhk-cloudtrail.ctyunapi.cn ■ IAM：oos-cnhk-iam.ctyunapi.cn ■ 统计 API：oos-cnhk-mg.ctyunapi.cn ■ 自服务门户：oos-cnhk-hqnet.ctyun.cn（香港精品网）或 oos-cnhk-nqnet.ctyun.cn（香港普通网）
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。

点击事件中的“查看事件”，可以查看事件的详细信息，如下例所示：


```
{
    "eventId": "7486360614268895607",
    "resource": [
        {
            "name": "test1111111",
            "type": "CloudTrail Trail",
            "arn": "arn:ctyun:cloudtrail::32fefj64y54gc:trail/test1111111"
        }
    ],
    "eventVersion": "1.06",
    "eventSource": "oos-cn.ctyun.cn",
    "requestParameters": {
        "Name": "test1111111"
    },
    "userAgent": "oos-cn.ctyun.cn",
    "readOnly": true,
    "userIdentity": {
        "accountId": "32fefj64y54gc",
        "principalId": "32fefj64y54gc",
        "type": "Root",
        "arn": "arn:ctyun:iam::32fefj64y54gc:root"
    },
    "eventType": "ApiCall",
    "serviceName": "CloudTrail",
    "sourceIp": "124.127.58.136",
    "requestId": "38701ee164e04054",
    "requestURL": "http://oos-cn.ctyun.cn/",
    "eventTime": "2025-01-16 15:10:22 UTC+0800",
    "eventName": "GetTrailStatus",
```

```
    "requestRegion": "cn",
    "managementEvent": true
}
```

事件信息描述

字段	描述
eventId	事件 ID。
resource	资源信息。
eventVersion	操作跟踪版本。
eventSource	事件源。
requestParameters	请求参数。
userAgent	用户代理。 发送 API 请求的客户端代理标识，除控制台外，都按照客户端 API 发出的 User-Agent 请求头展示，如无法获取到则不展示。 请求由用户通过控制台发出，显示 oos-cn.ctyun.cn。
readOnly	是否为只读操作： ● true：读操作。 ● false：写操作。
userIdentity	用户信息。
eventType	事件请求类型。
serviceName	服务名称。
sourceIp	源 IP。
requestId	请求 ID。
requestURL	请求 URL。
eventTime	事件发生的时间。
eventName	事件名称。
requestRegion	请求区域。
managementEvent	是否为管理事件： ● true：是管理事件。 ● false：非管理事件。

6.1.2 事件列表

类别	事件
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
统计	GetCapacity
	GetBilledStorageUsage
	GetRestoreCapacity
	GetDeleteCapacity
	GetTraffics
	GetRequests
	GetReturnCode
	GetConcurrentConnection
	GetUsage
	GetBandwidth
控制台	ConsoleLogin
	LogoutUser
	CheckMfa
操作跟踪	CreateTrail
	DeleteTrail
	DescribeTrails
	GetTrailStatus
	PutEventSelectors
	GetEventSelectors
	UpdateTrail
	StartLogging
	StopLogging
	LookupEvents

访问控制	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

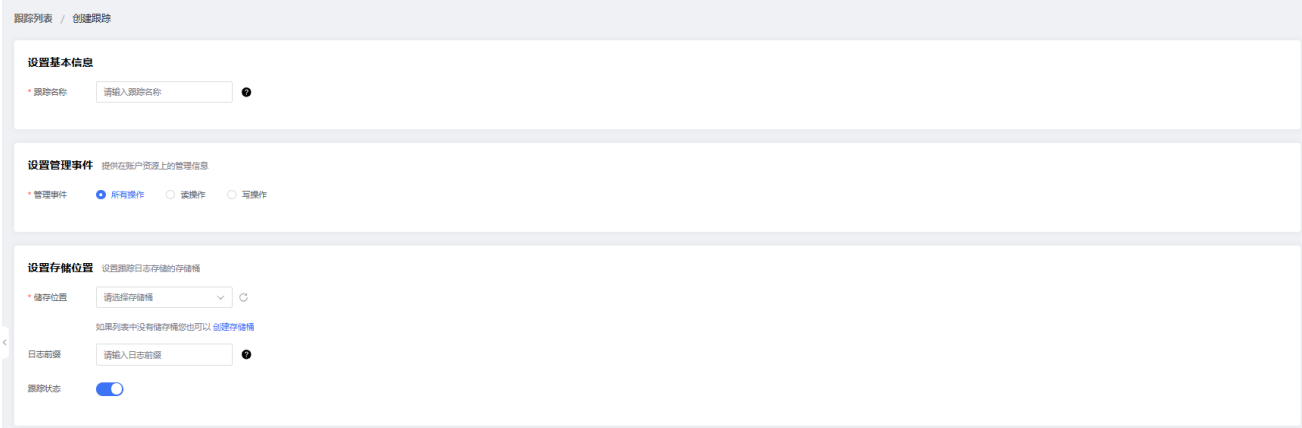
6.2 跟踪列表

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。

6.2.1 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“创建”，进入“创建跟踪”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**：
  - 所有操作：包括读操作和写操作。
  - 读操作。

- 写操作。

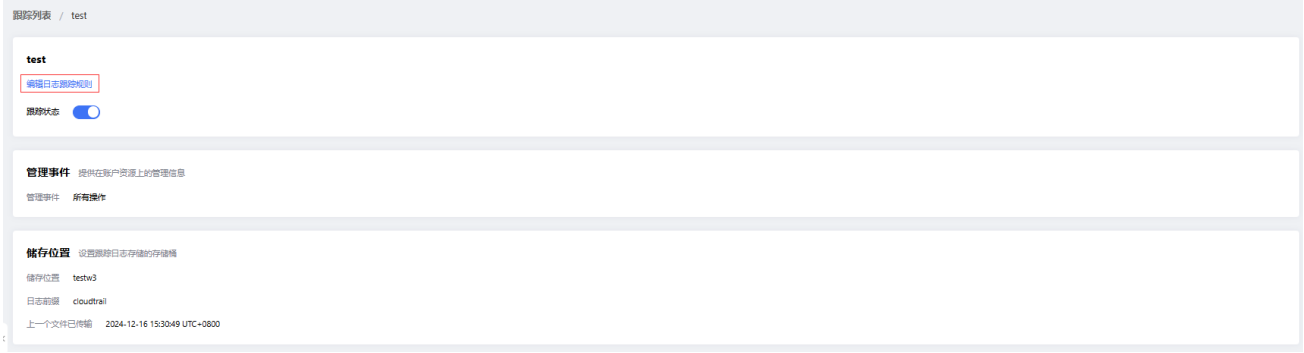
- **设置存储位置**：设置跟踪日志存储的存储位置、日志前缀和跟踪状态。

项目	描述
存储位置	操作跟踪事件存储的位置。 可以存储到现有存储桶（用户需要有对应的存储桶权限），也可以在账户中创建新的存储桶（用户需要有创建存储桶的权限），并将跟踪日志存储至新创建的存储桶。
日志前缀	操作跟踪存储日志的前缀，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	创建的跟踪状态： ● ON：表示跟踪日志开启。 ● OFF：表示跟踪日志未开启。

6.2.2 修改跟踪

在“跟踪列表”页面，点击跟踪“操作”列的“开启/关闭”、“管理”和“删除”按钮，可以对操作跟踪进行相应的修改。

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。


跟踪列表 / test
test
编辑日志跟踪规则
跟踪状态
管理事件 提供在账户资源上的管理信息
管理事件 所有操作
储存位置 设置跟踪日志存储的存储桶
储存位置 testw3
日志前缀 cloudtrail
上一个文件已传输 2024-12-16 15:30:49 UTC+0800

7 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: GetAccessKeyLastUsed、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

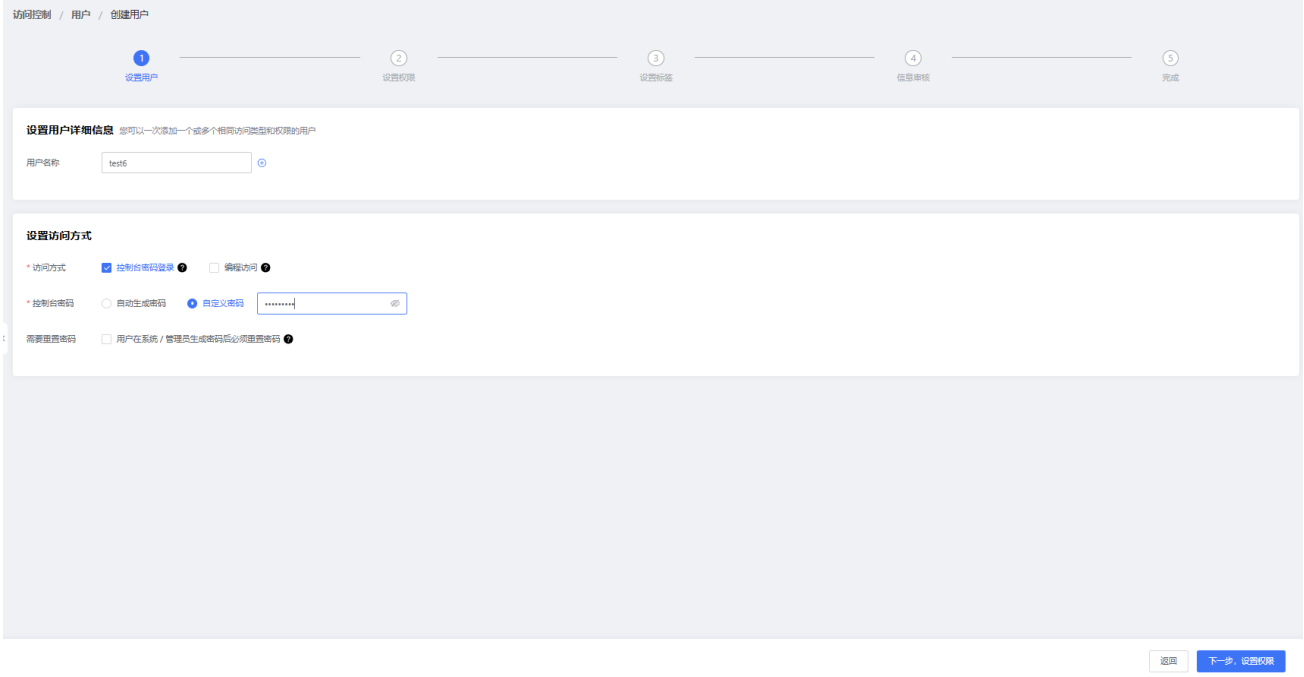
用户组	创建用户组	iam:CreateGroup 建议同时赋予的权限：iam:ListGroups、iam:ListPolicies、iam:AttachGroupPolicy
	查看用户组信息	iam:ListGroups、iam:ListAttachedGroupPolicies、iam:GetGroup
	修改用户组	iam:ListUsers、iam:ListGroups、iam:ListGroupsForUser、iam:ListPolicies、iam:ListAttachedGroupPolicies、iam:GetGroup、iam:AddUserToGroup、iam:RemoveUserFromGroup、iam:AttachGroupPolicy、iam:DetachGroupPolicy
	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
	创建自定义策略	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
安全设置	编辑密码规则	iam:GetAccountPasswordPolicy、iam:UpdateAccountPasswordPolicy
	清除密码规则	iam:GetAccountPasswordPolicy、iam:DeleteAccountPasswordPolicy
	编辑登录规则	iam:GetAccountLoginSecurityPolicy、iam:UpdateAccountLoginSecurityPolicy

	清除登录规则	iam:UpdateAccountLoginSecurityPolicy、iam:DeleteAccountLoginSecurityPolicy
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

7.1 快速入门

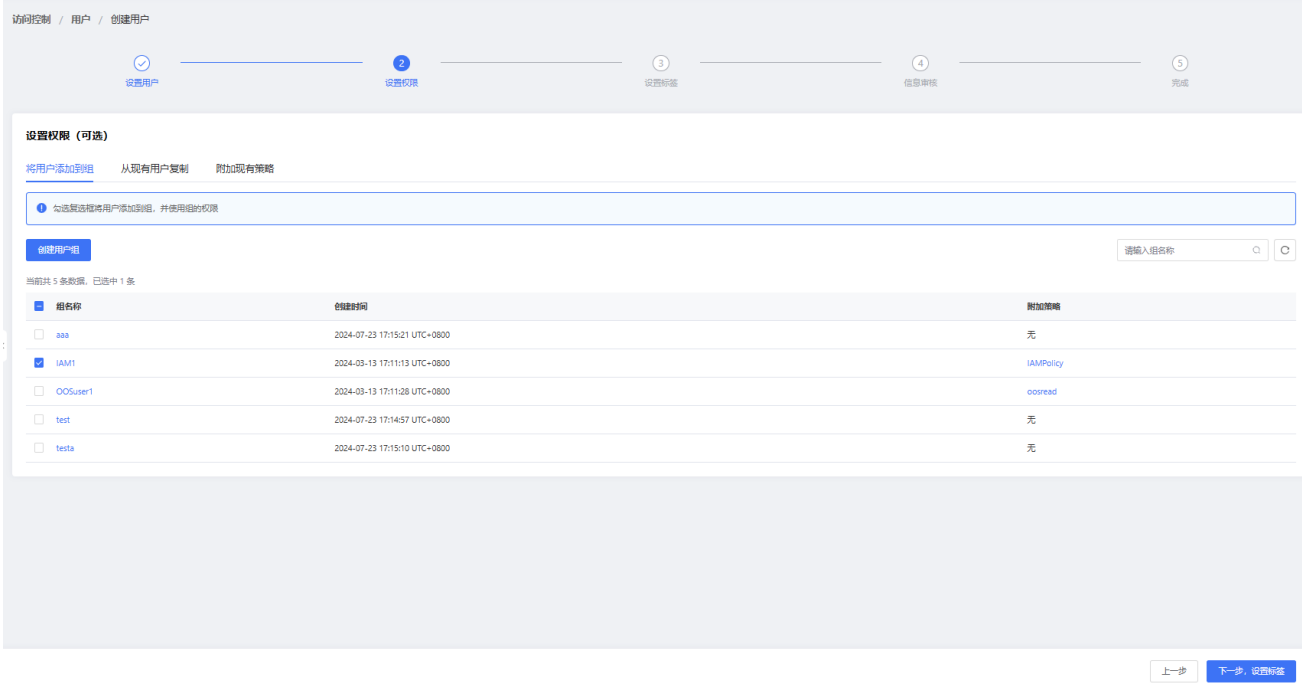
进入“访问控制”>“概览”，点击“创建用户”，进入“创建用户”页面，启动创建用户。可以按照下列步骤创建子用户：

1. **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。

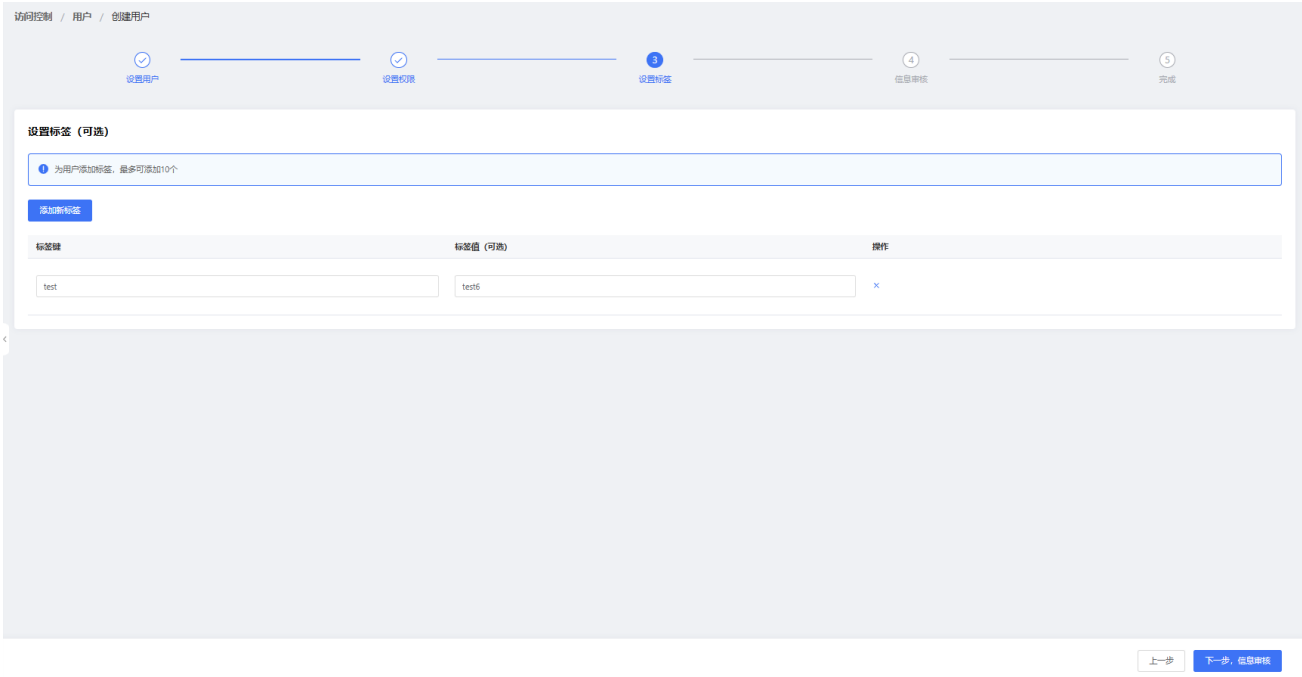


2. **设置权限（可选）**：为用户添加权限，有三种添加权限的方式（只能选择一种）：
   - **将用户添加到组**（前提：已经有用户组）：用户将继承该用户组的所有权限。

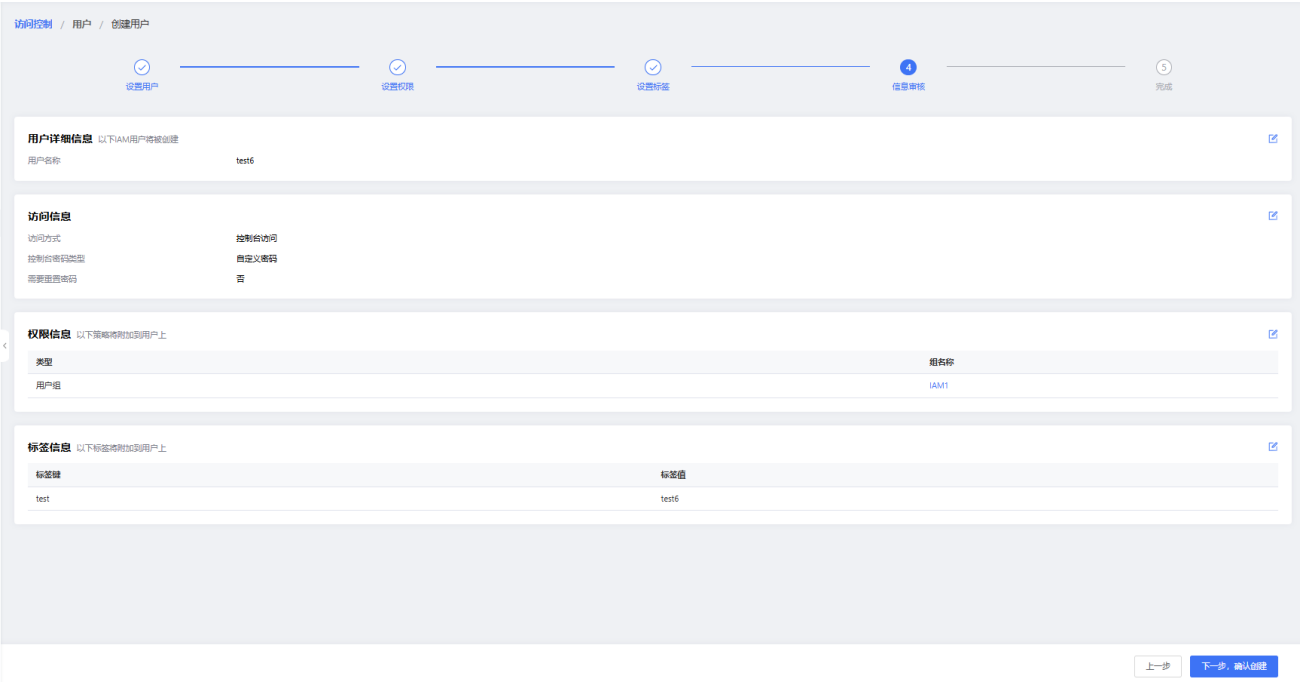
- **从现有用户复制**（前提：现有用户有通过直接附加的方式被授权的策略），每次只能复制一个用户的权限。只能复制现有用户直接附加的策略，不能复制用户所在组的策略。
- **附加现有策略**。



3. **设置标签（可选）**：可以为创建的用户添加标签键和标签值。每个用户最多可添加 10 个标签。

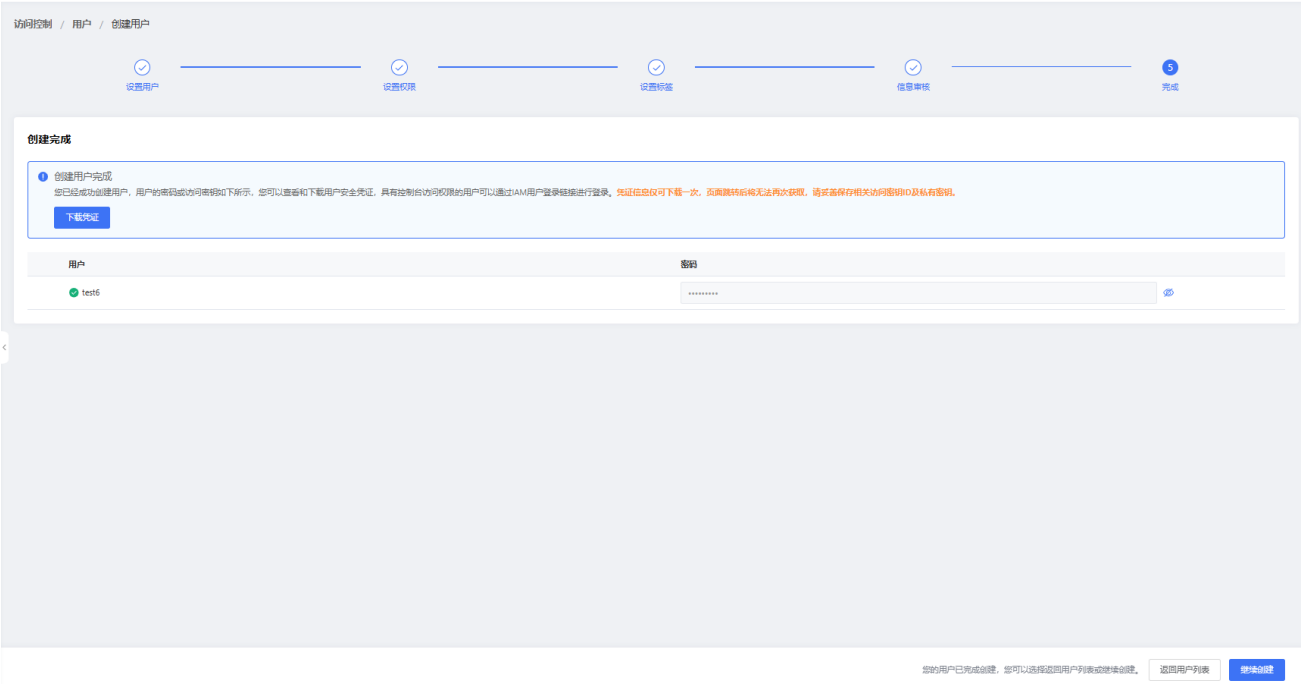


4. **信息审核**：对创建的用户信息进行审核，如果需要更改，可以在此页面点击对应的编辑标识，然后到对应的页面进行修改。



5. **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。

   注意：凭证信息仅可下载一次，页面跳转后无法再次获取，请妥善保存相关访问密钥 ID 及私有密钥。



7.2 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。

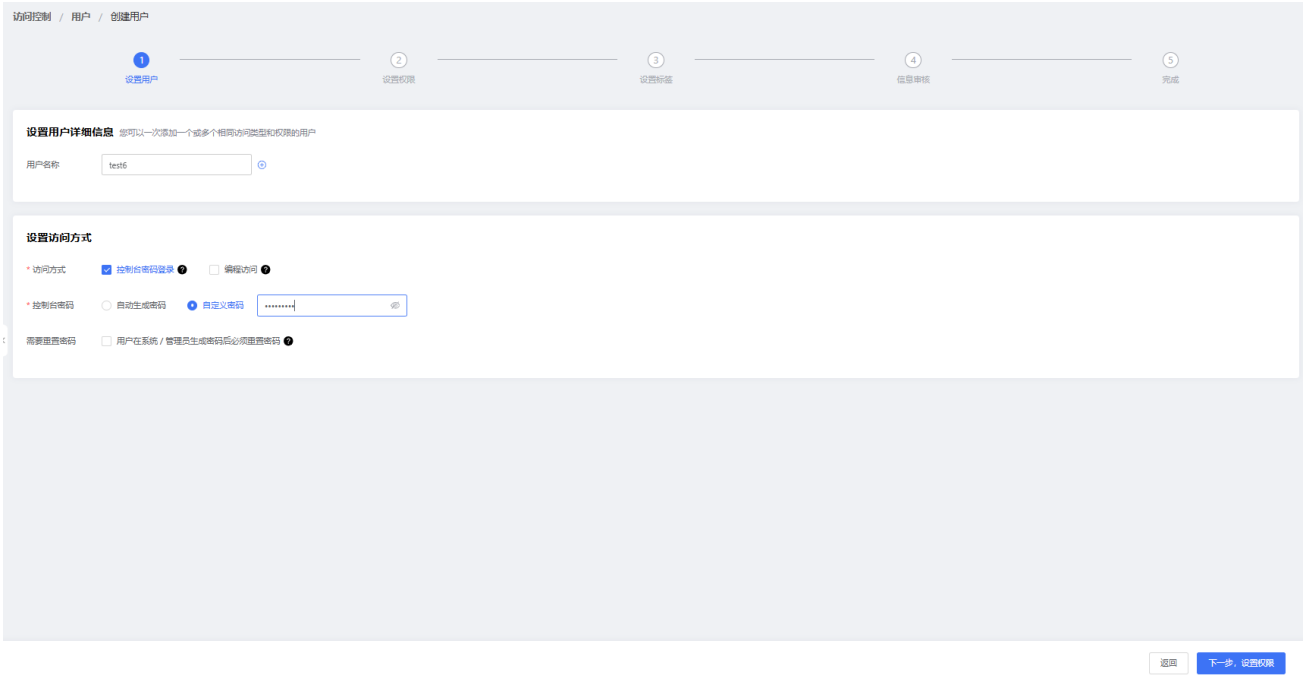
默认情况下 IAM 用户没有任何权限，根用户或具有 IAM 授权的相关子用户可以给 IAM 子用户授权。授权后，IAM 用户可以根据自己的权限对资源进行操作。

7.2.1 创建 IAM 用户

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“创建”。操作步骤：

1. **设置用户**

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。

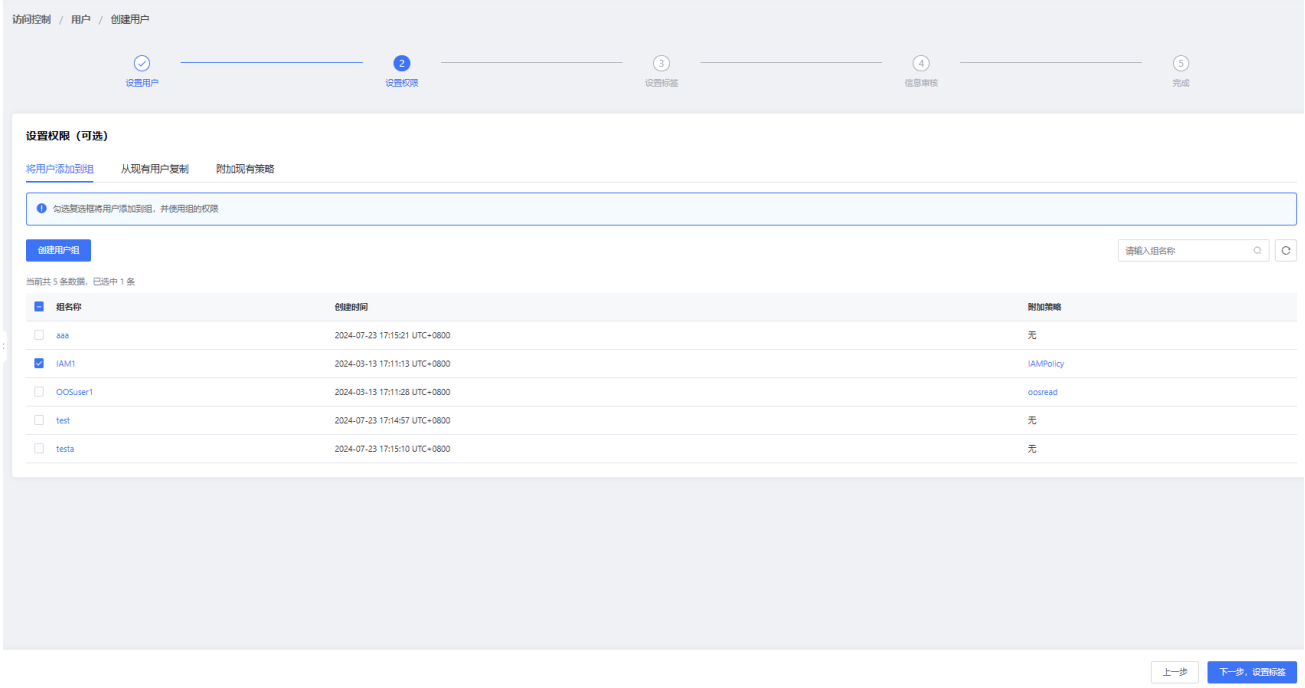


项目	描述
用户名	登录 OOS 的用户名，管理员一次可以添加 1-10 个具有相同访问类型和访问权限的 IAM 用户。用户名需遵循下列原则： ● 本账户下，IAM 用户名必须唯一。 ● 1~64 位字符串组成，字符只能包含字母、数字或特殊字符，字母不区分大小写，特殊字符只能是：下划线（_）、中划线（-）、逗号（,）、句点（.）、加号（+）、等号（=）和 at 符号（@）。

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/管理员生成密码后必须重置密码”，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”。

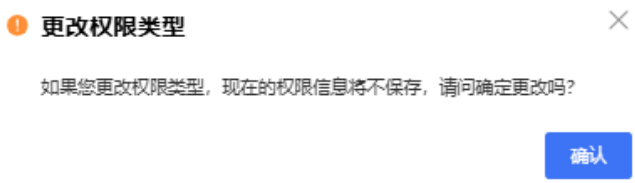
2. **设置权限**

为 IAM 用户设置权限。



- **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，一个用户最多可以加入 10 个组。
- **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**：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：

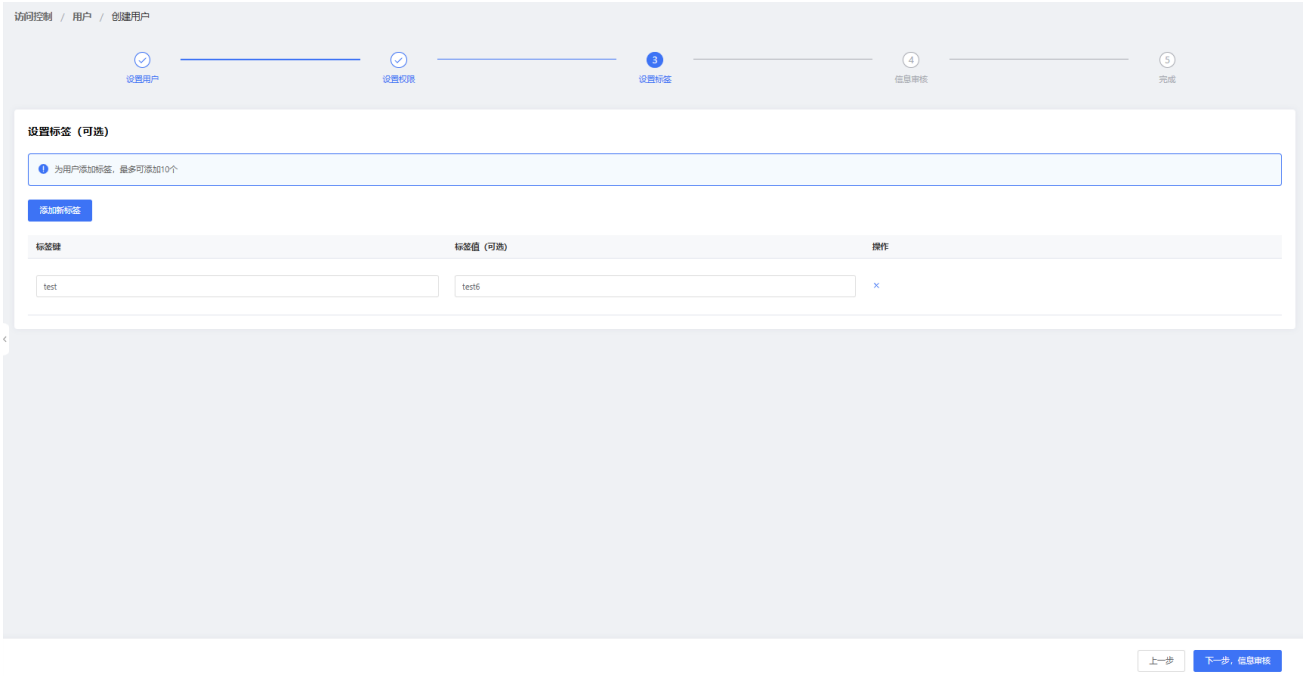


说明：可以创建用户时为用户添加策略，也可以用户创建完成后，再为其添加策略。

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。

3. 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。

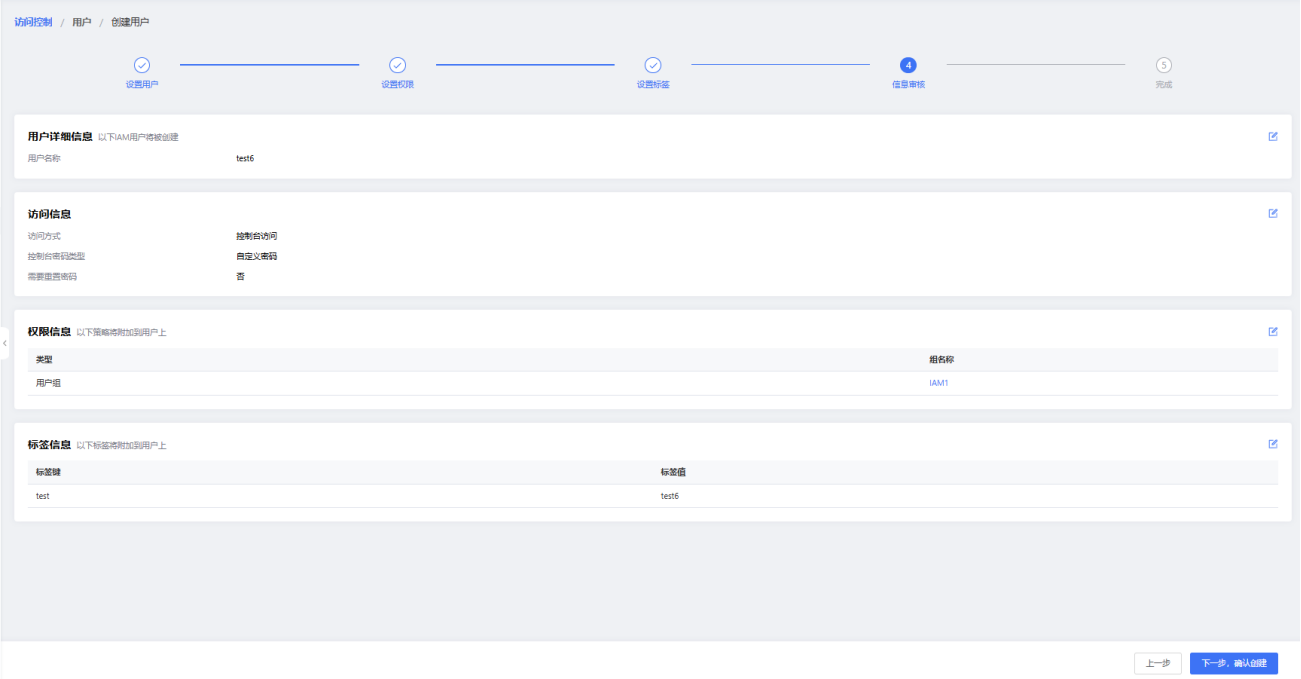


说明：不能为单个标签指定多个值，但多个标签键可以有相同的标签值。

项目	描述
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。
操作	可以对标签进行删除。

4. 信息审核

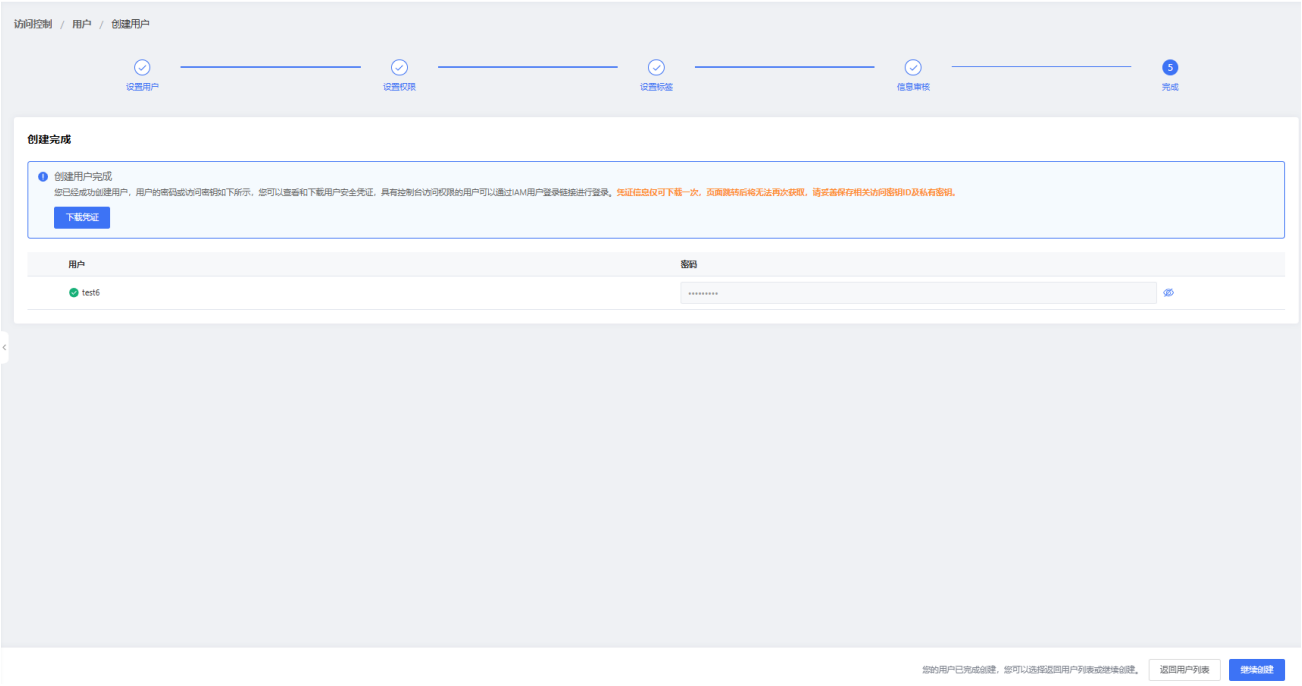
对于创建的用户信息进行审核。如果需要修改，可以在此页面点击对应的编辑标识，然后到对应的页面进行修改。



5. 完成

点击下载凭证，保存新创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“创建密钥”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。



7.2.2 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:

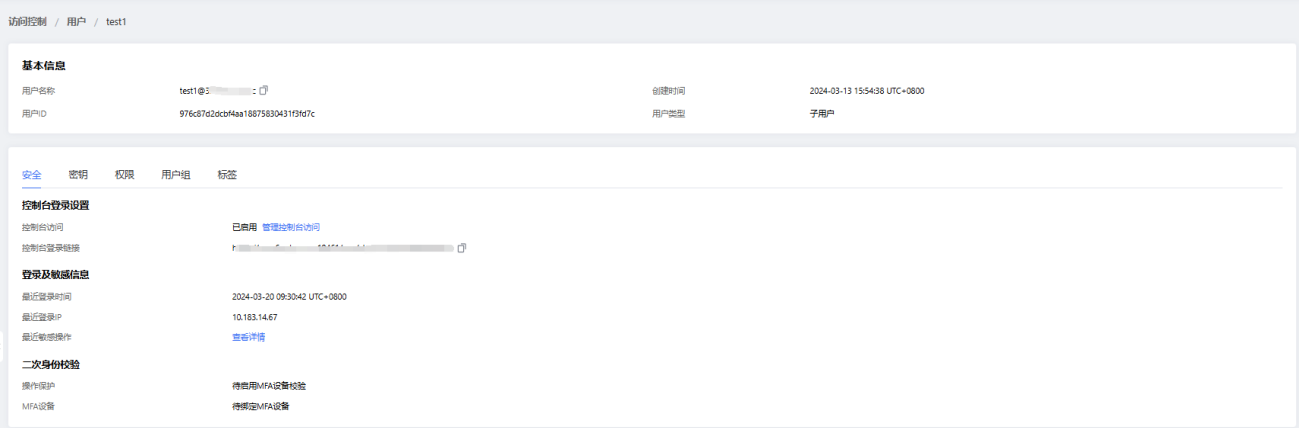
- 用户名称
- 密码使用时长
- 密码剩余使用期限
- 最近控制台访问时间
- 用户 ID
- ARN
- 是否启用 MFA
- 编程访问
- 控制台访问

其中“用户名”、“操作”为必显示项。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
用户名称	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： ● 已启用。 ● 未启用。
编程访问	是否启用编程访问： ● 已启用。 ● 未启用。
控制台访问	是否启用控制台访问： ● 已启用。 ● 未启用。
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。



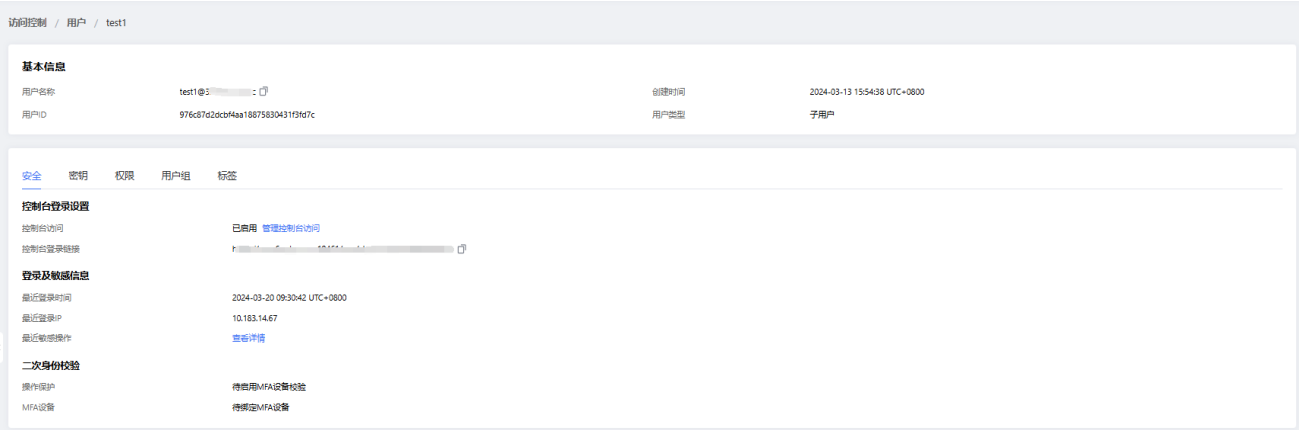
用户基本信息描述

项目	描述
用户名称	*<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。

7.2.2.1 查看和修改用户安全

点击“安全”，进入“安全”页面，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。

项目	描述

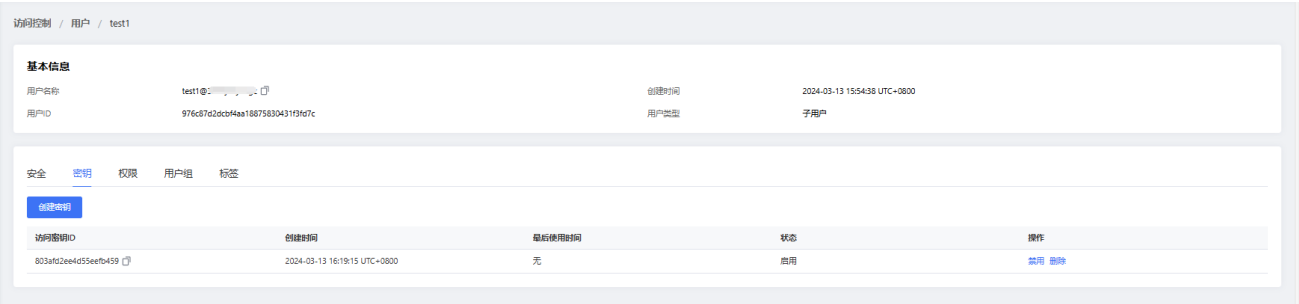
控制台密码登录	控制台密码登录是否开启： ● 开启：启用控制台密码登录，当前无控制台登录密码时，会生成新登录密码。 ● 关闭：禁用控制台密码登录，删除当前密码。
设置登录新密码	设置新密码方式： ● 保留当前密码：使用用户当前的登录密码，只有当前密码存在时才会有此项。 ● 重新自动生成密码：系统重新随机生成登录密码。 ● 重新设置自定义密码：管理员重新设置登录密码。
重置密码	设置新 IAM 用户在下次登录时是否需要重置密码。若勾选“用户在下次登录时必须重置密码”，即 IAM 用户在下次登录时，必须重置密码。

7.2.2.2 查看和修改密钥

点击**密钥**，可以对该用户密钥进行**创建**、**启用/禁用**、**删除**，

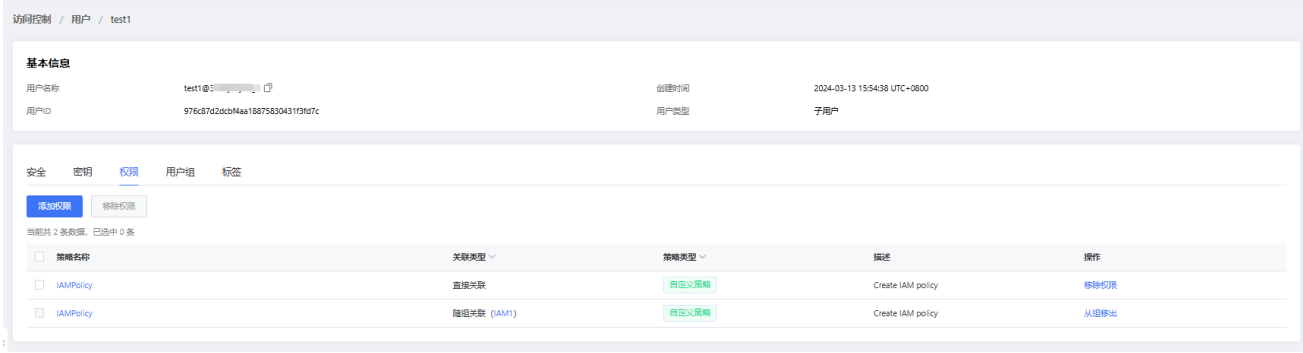
注意：

- 只有密钥少于 2 个时才能创建密钥（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“创建密钥”的方式获取新的密钥，并下载密钥凭证。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。

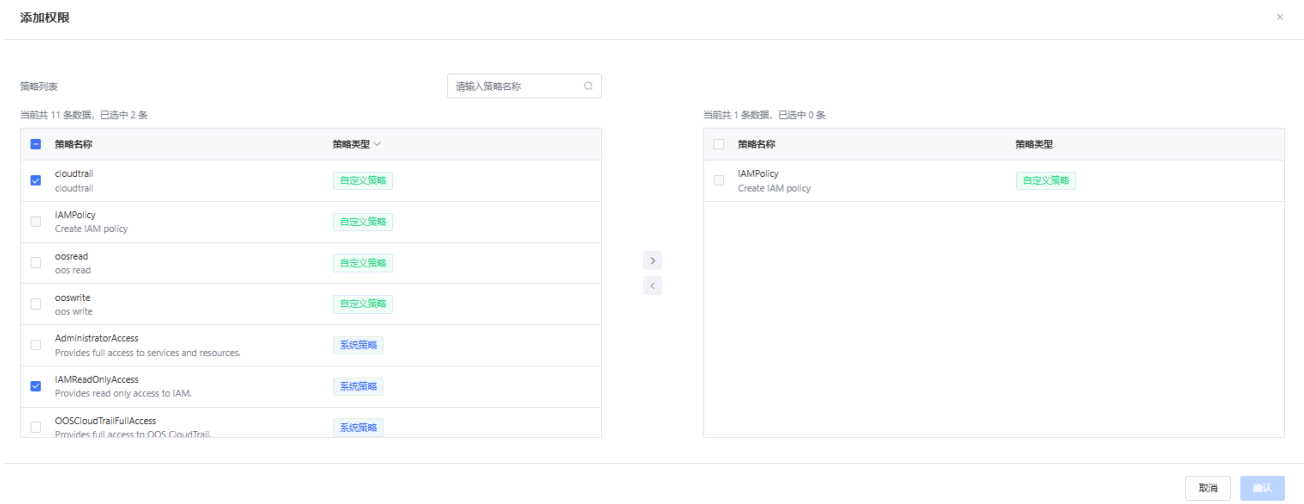


7.2.2.3 查看和修改权限

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。



- 添加权限：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。



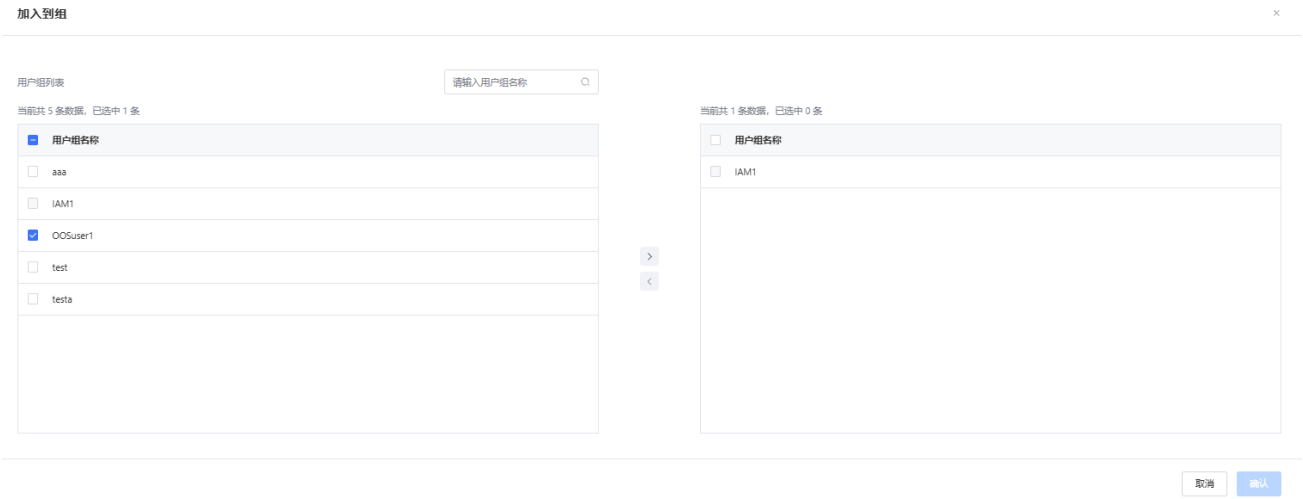
- 移除权限：选择需要移除的策略，点击“移除权限”，可以为用户删除多条策略。点击对应策略的“移除权限”，可以解除已关联的策略。
- 从组移出：点击“从组移出”，该用户将移出对应的组，并解除随组关联的策略。

7.2.2.4 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“确认”。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“操作”列的“移出组”，可以将用户从该组移出。

7.2.2.5 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。或者点击标签“操作”列的“删除”，可以将该标签删除。
- **编辑标签：**点击标签“操作”列的“编辑”，可以修改标签值。

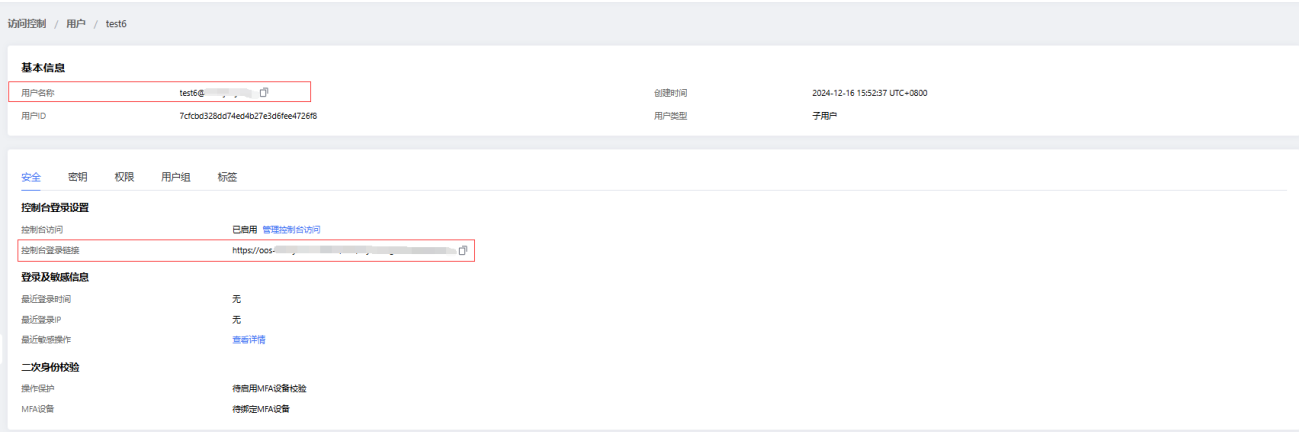
7.2.3 删除用户

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“操作”列的“删除”，删除用户。

说明：删除用户时，会弹出对话框，确认是否删除选中用户。

7.2.4 IAM 用户登录

根用户或有管理用户权限的 IAM 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 IAM 用户的登录链接。



根据提示，输入 IAM 用户名和登录密码，进行登录。

说明：IAM 用户名为“@”前面的部分。

IAM 子用户与根用户的页面基本一致，子用户的功能根据授权而定。如果需要更多权限，可以向根用户或有管理用户权限的 IAM 子用户进行申请。

7.3 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。

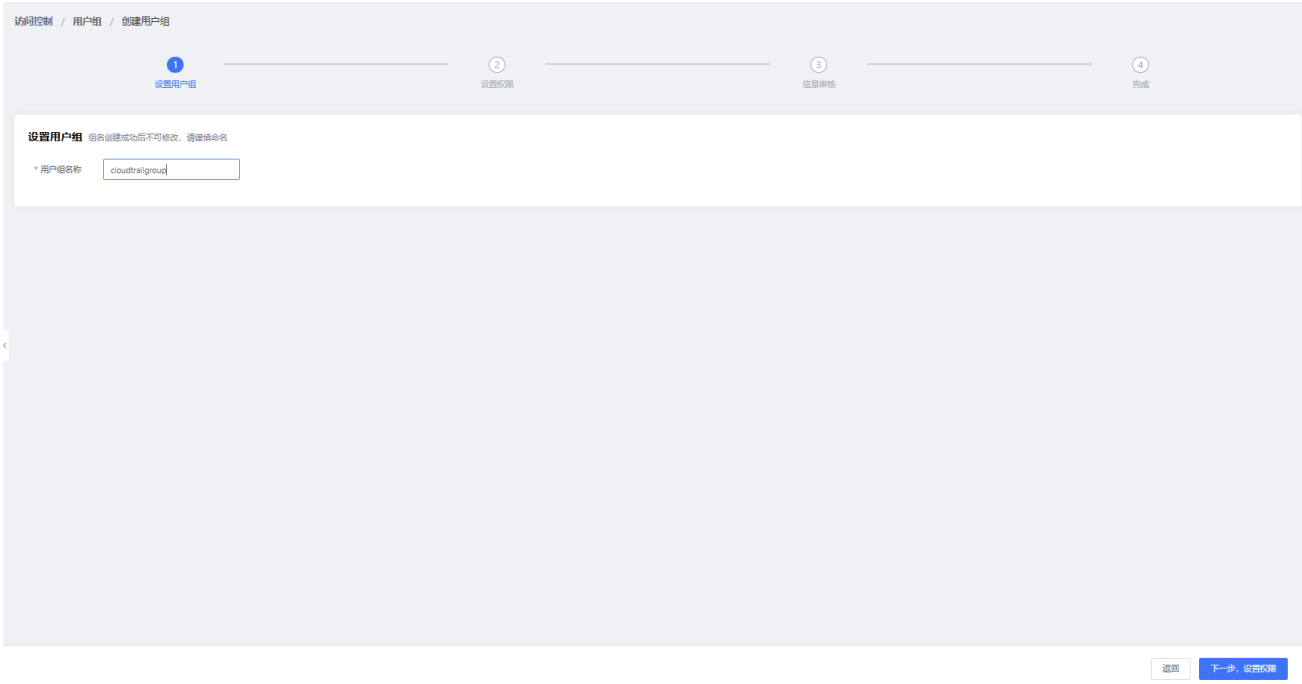
点击菜单栏中的“用户组”，可以：

- 创建用户组。
- 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。

7.3.1 创建用户组

点击“访问控制”>“用户管理”>“用户组”>“创建”，进入“创建用户组”页面，按照下列步骤创建用户组：

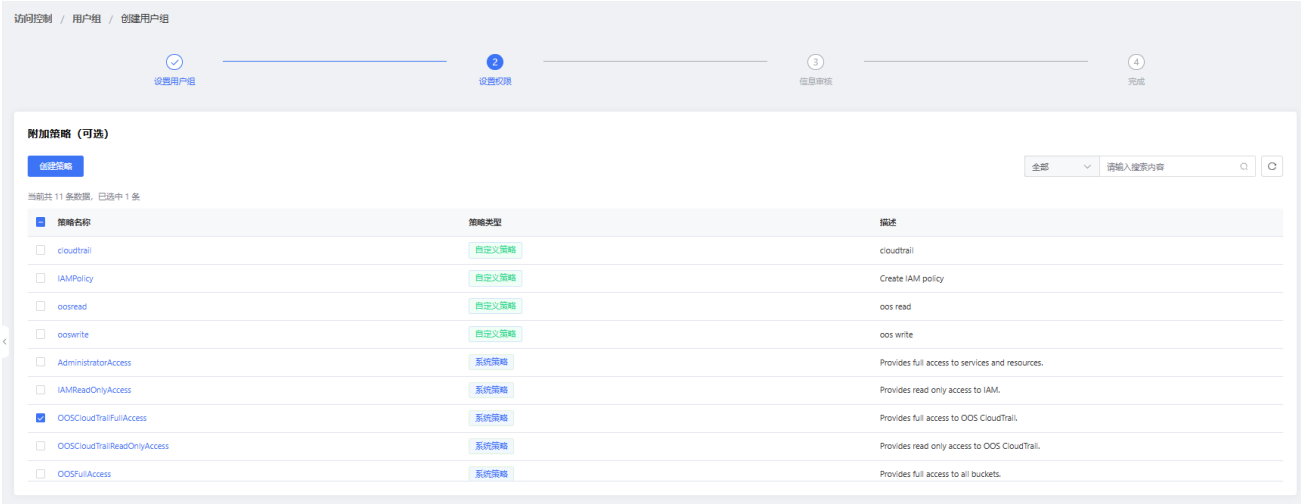
1. **设置用户组**



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



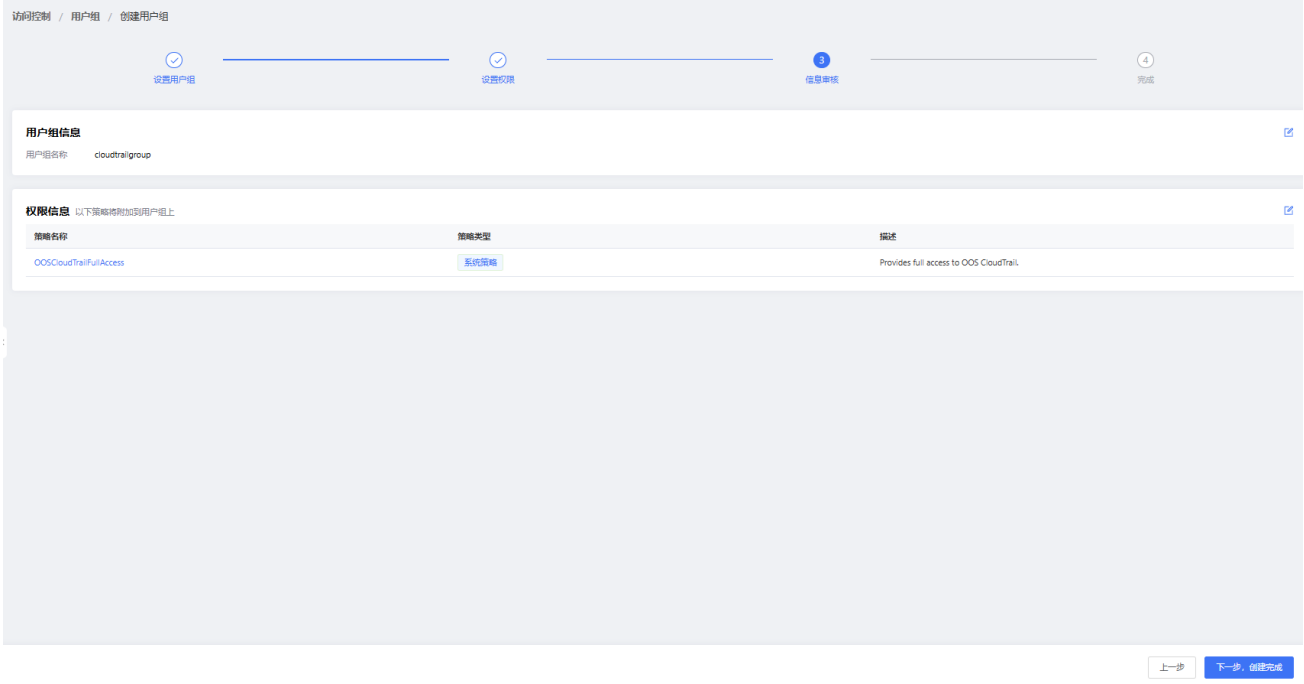
可以在搜索框中搜索匹配策略，搜索出的匹配策略以列表的形式展现出来，可以通过勾选对应策略，为用户组附加策略。

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

注意：每个用户组最多添加 10 条策略。

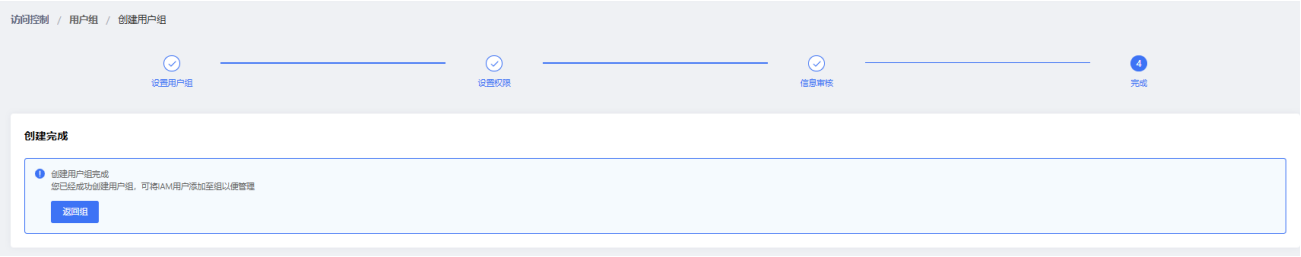
3. 信息审核

对于新创建的用户组信息进行审核。如果有需要修改的地方，可以点击编辑图标 进行修改。



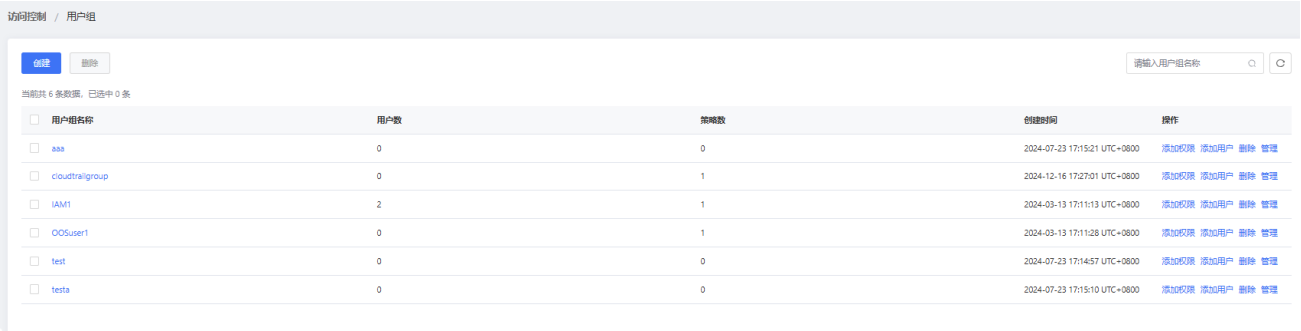
4. 完成

完成用户组创建后，可以将 IAM 用户添加到组，以便管理。



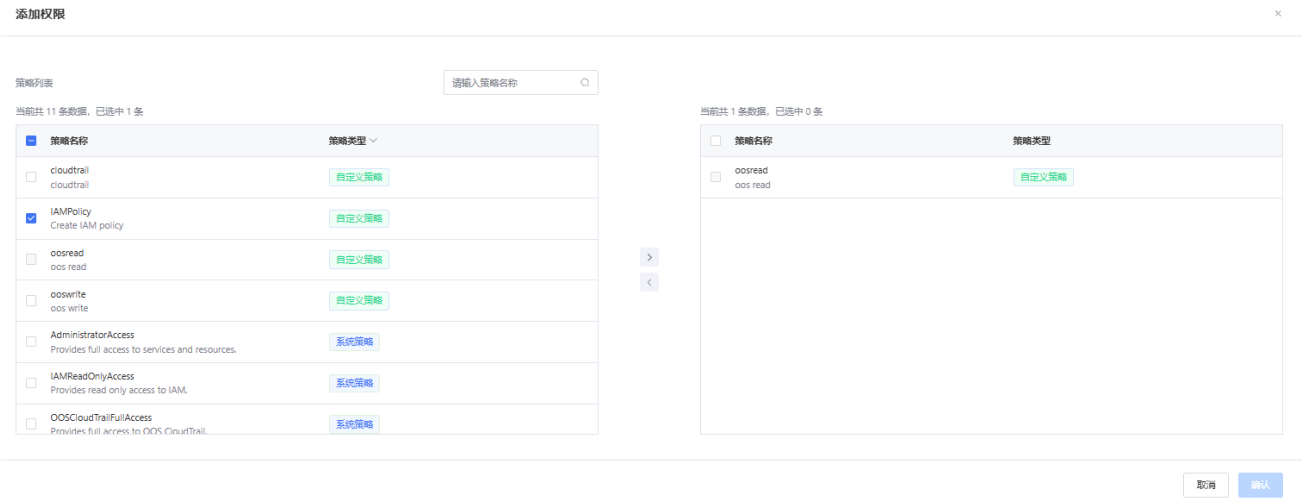
7.3.2 查看和修改用户组信息

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。



7.3.2.1 为用户组设置权限

- 添加权限
  - 在“用户组”页面，点击对应用户组操作中的“添加权限”，弹出“添加权限”页面，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。

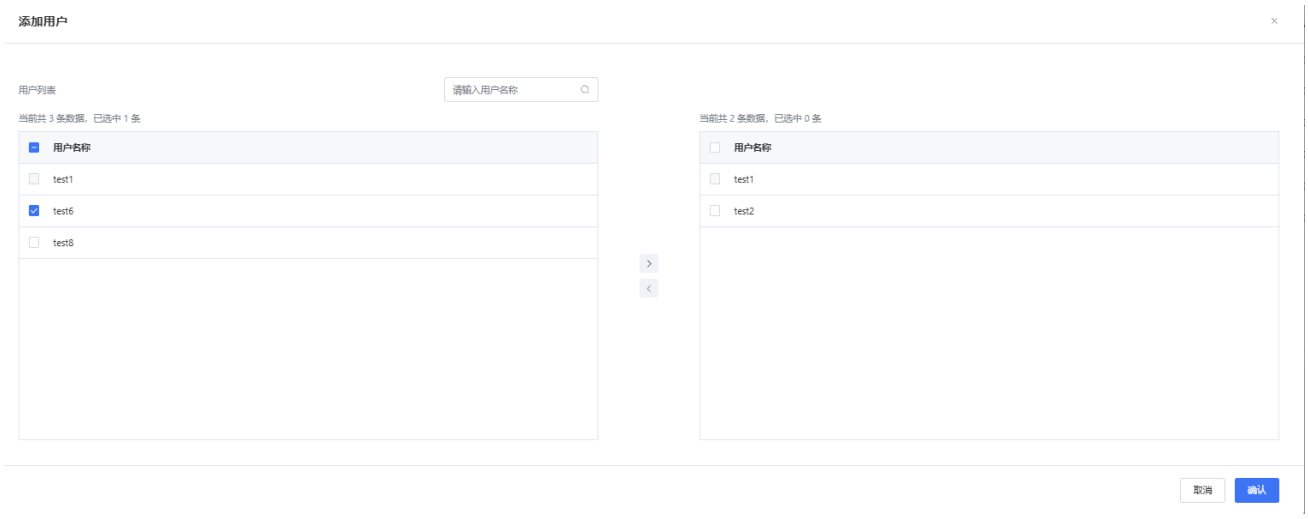


- 移除权限

  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“操作”列的“移除权限”，可以为用户组删除对应的策略。

7.3.2.2 为用户组添加或移除用户

- 添加用户
  - 在“用户组”页面，点击对应用户组操作中的“添加用户”，弹出“添加用户”页面，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。

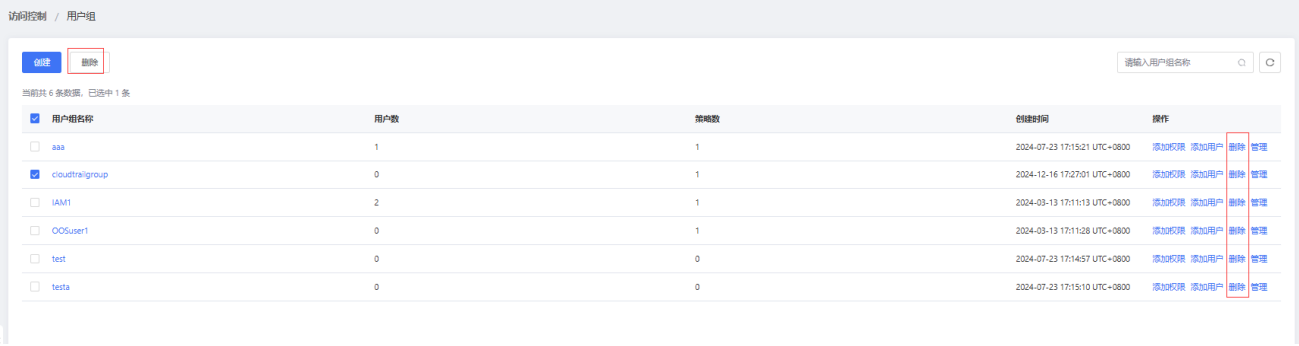


- **移除用户**

  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“移除用户”，可以为用户组删除多个用户。或者点击对应用户“操作”列的“移除用户”，为用户组移出对应用户。

7.3.3 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“操作”列的“删除”，删除用户组。



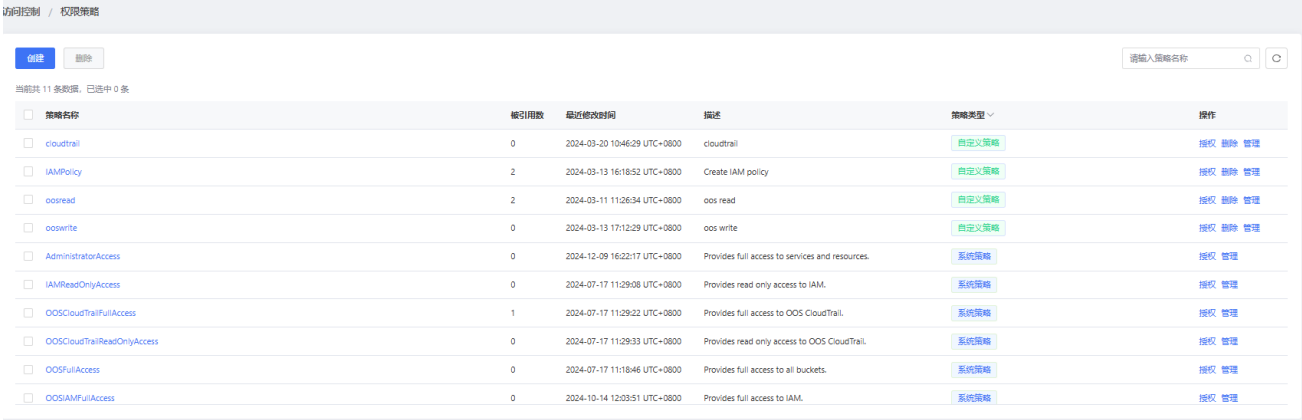
7.4 IAM 策略

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**：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。



7.4.1 系统策略

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：PutBucket、GetRegions、DeleteBucket、ListAllMyBucket、ListBucket、GetObject。 ● ClouldTrail：所有操作。
OOSCloudTrailReadOnlyAccess	操作跟踪读相关的权限，包括： ● OOS：GetObject、ListAllMyBucket、ListBucket。

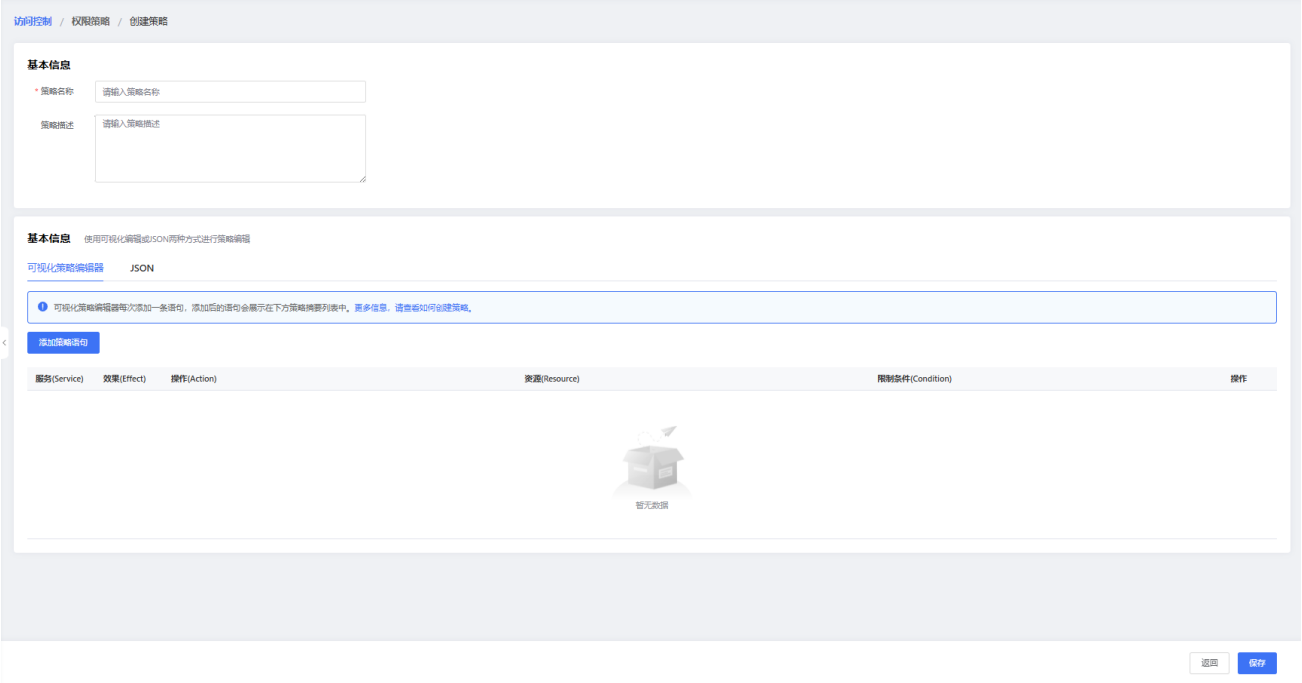
	● CloudTrail：GetTrailStatus、DescribeTrails、LookupEvents、GetEventSelectors。
OOSFullAccess	OOS 的所有权限，包括存储桶和文件的所有操作。
OOSIAMFullAccess	IAM 所有权限。
OOSReadOnlyAccess	OOS 只读权限，包括存储桶和文件的 GET、List 相关操作。

7.4.2 自定义策略

7.4.2.1 创建自定义策略

点击“访问控制”>“权限策略”>“创建”，进入创建策略页面，创建自定义策略。

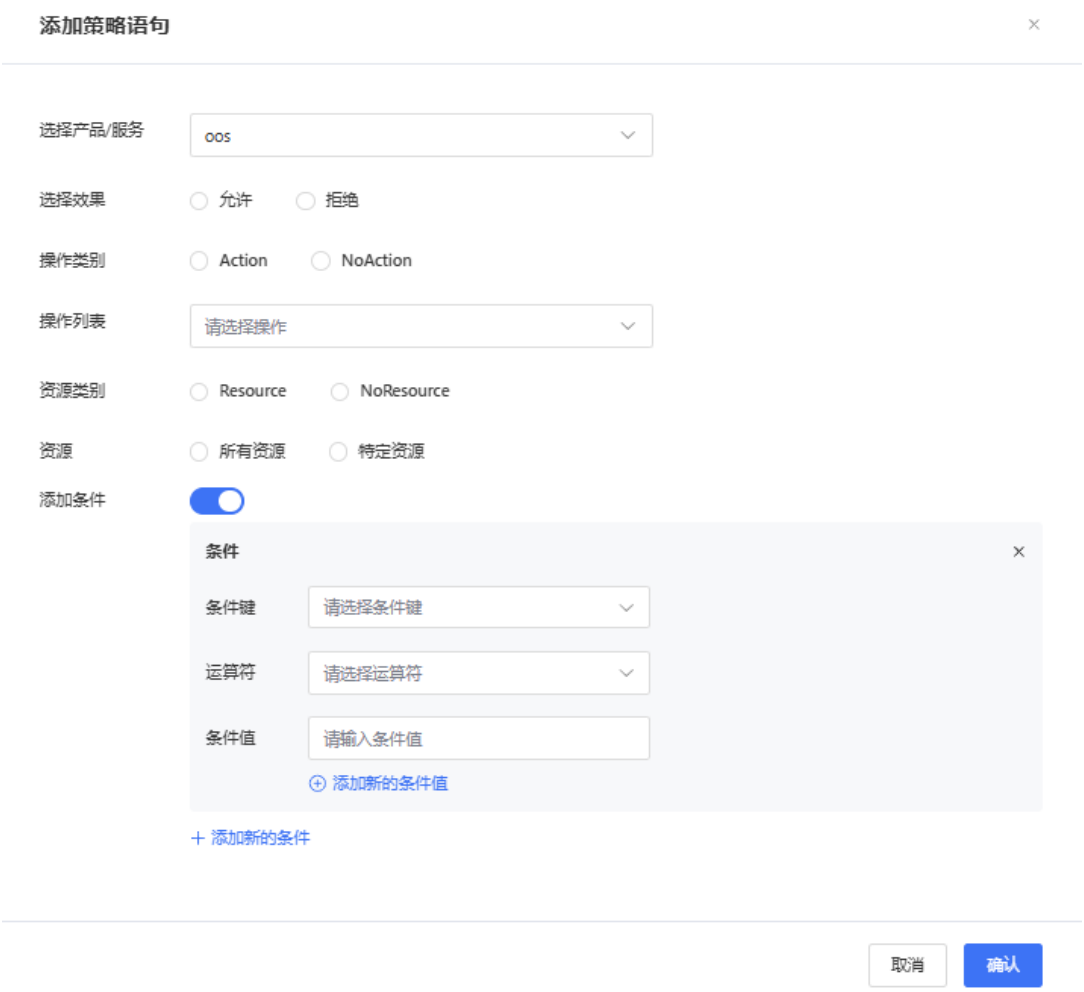
说明：对于各操作权限对应的具体资源、API 详见**操作权限与 API 对应关系**。



名称	描述
策略名称	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（@）。 **注意：**策略名必须唯一。
策略描述	可选，对策略进行概要描述。
策略内容	使用可视化策略编辑或 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，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。 **说明**：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 ● GetBucketLocation ● GetBucketPolicy ● GetLifecycleConfiguration ● GetBucketWebsite ● GetBucketCORS ● GetBucketLogging

	● GetObject ● ListMultipartUploadParts ● GetBucketInventoryConfiguration
	写： ● DeleteBucket ● PutLifecycleConfiguration ● PutBucketWebsite ● DeleteBucketWebsite ● PutBucketCORS ● PutBucketLogging ● PutObject ● DeleteObject ● DeleteMultipleObjects ● AbortMultipartUpload ● PutBucket ● PutBucketInventoryConfiguration
	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 ● GetAccountLoginSecurityPolicy
	写： ● CreateAccessKey ● DeleteAccessKey ● UpdateAccessKey ● CreateUser ● DeleteUser ● TagUser ● UntagUser ● CreateGroup ● DeleteGroup ● AddUserToGroup ● RemoveUserFromGroup ● ChangePassword ● UpdateAccountPasswordPolicy ● DeleteAccountPasswordPolicy ● UpdateAccountLoginSecurityPolicy ● DeleteAccountLoginSecurityPolicy ● 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	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。 ● **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	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（=）和 at 符号（@）。 **说明：**运算符为 **StringLike** 和 **StringNotLike**，可以包含通配符。

	(?)。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 (?)。	
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	字符串，可以包含特殊字符。

	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。	
ctyun:SecureTransport	**Bool**：布尔匹配。	● **true** ● **false**
ctyun:MultiFactorAuthPresent	**Bool**：布尔匹配。 **说明**：不建议对 GetObject 接口设置该条件键，否则在 OOS 控制台上无法下载、预览、分享文件和编辑元数据。	● **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。	整数形式，以秒为单位。

	● **NumericGreaterThanEquals**：大于等于指定的值。 **说明**：不建议对 GetObject 接口设置该条件键，否则在 OOS 控制台上无法下载、预览、分享文件和编辑元数据。	
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 (?)。 **说明**：本条件键仅对 ListBucket 生效。	字符串形式。
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。	字符串形式。 取值为： ● private：私有 ● public-read：公共读

	● **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 (?)。 **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。	● public-read-write：公共读写

● 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:ListAllMyBucket",
        "oos:GetBucketLocation"
      ],
      "Resource": " arn:ctyun:oos::02elbe4neijs7:* ",
       "Condition" :  {
            "DateGreaterThan" : {
              "ctyun:CurrentTime" : "2019-01-16T00:00:00Z"
```

```
                 },
                "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	定义操作的类别	格式为*服务名:操作* 服务名： ● **oos**：对象存储。 ● **cloudtrail**：操作跟踪。 ● **statistics**：管理 API。 ● **iam**：访问控制。 操作详见**操作列表**。

	一		
	● **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。	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"，…] } } **注意**：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。

- **…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 } }
```

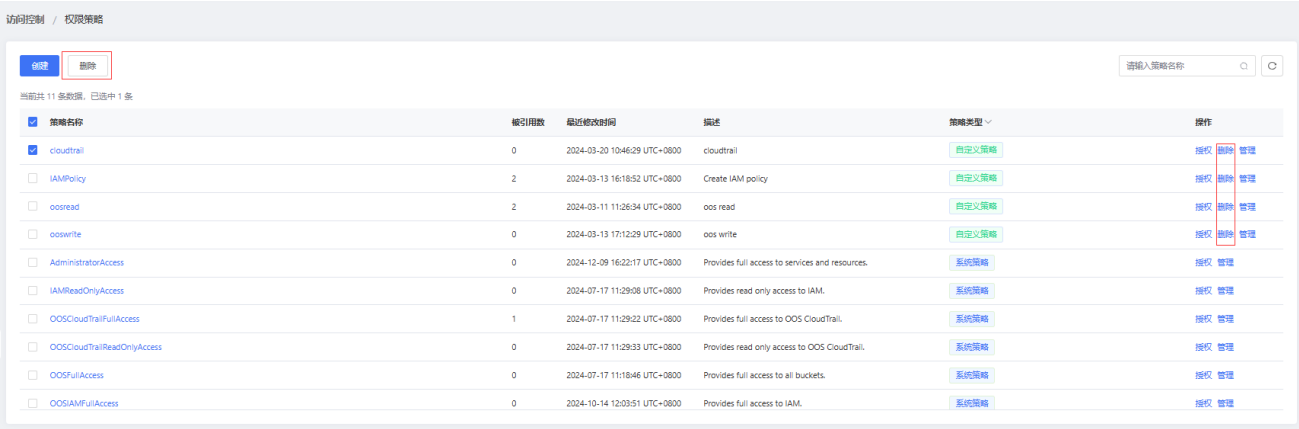
7.4.2.2 修改自定义策略

点击“权限策略”>“策略名称”>“策略内容”>“编辑策略”，弹出编辑策略页面，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**创建自定义策略**。

7.4.2.3 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。以通过两种方式删除自定义的策略：

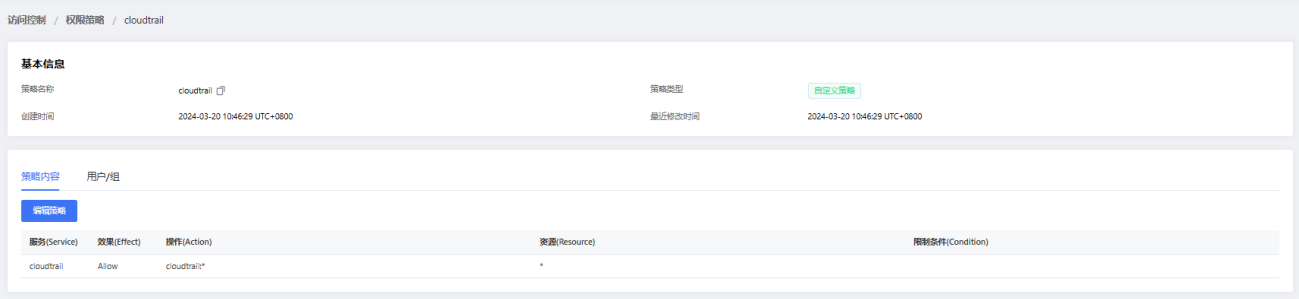
- 选择需要删除的策略进行勾选，点击“删除策略”，可以删除对应的策略。
- 点击“操作”中的“删除”，可以删除该策略。



7.4.3 查看策略基本信息

在“权限策略”页面，点击具体策略名或者“操作”列的“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。

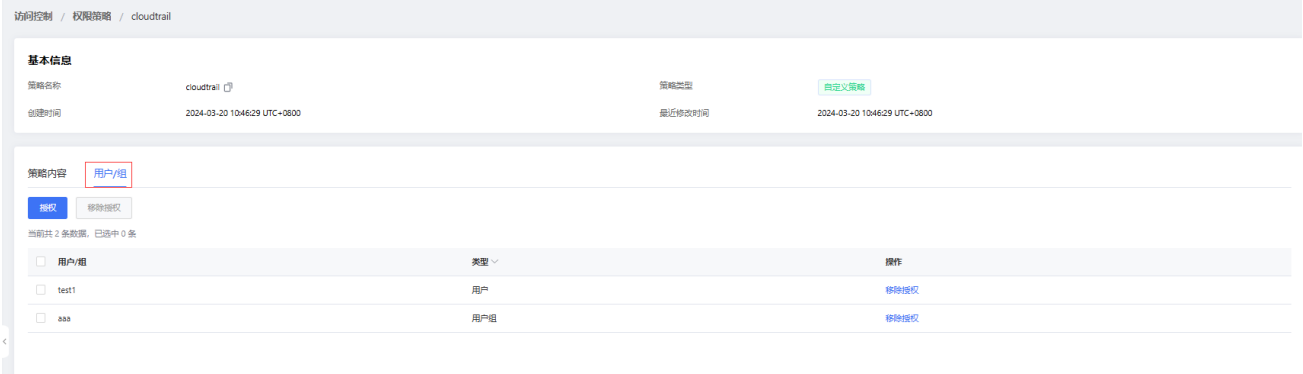
策略基本信息包含：策略名称、策略类型、创建时间、最近修改时间、描述。



7.4.4 授权用户/用户组

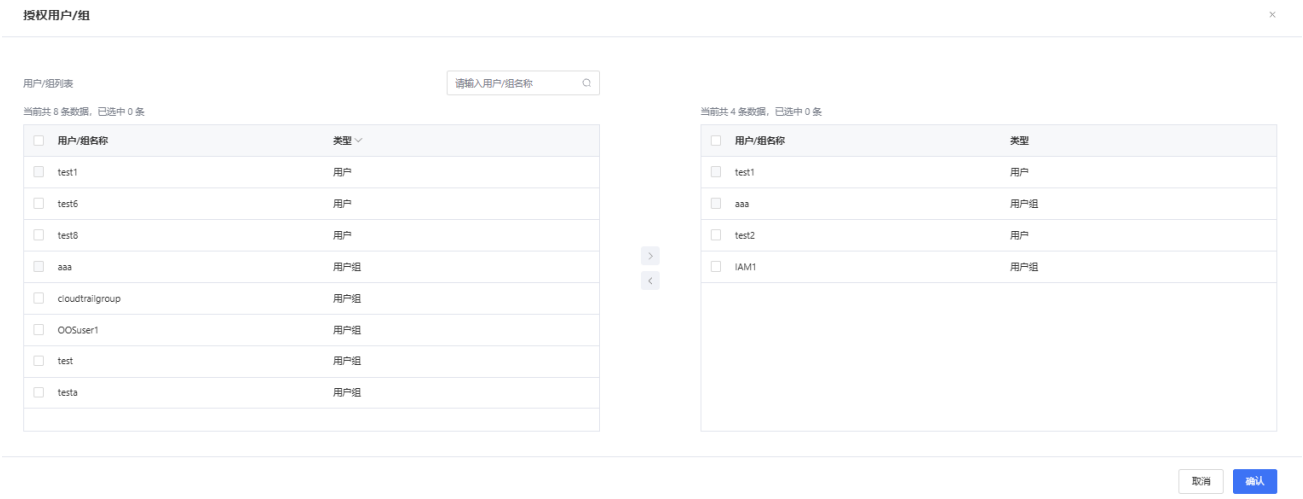
- **查看授权用户/用户组**

在权限策略页，点击对应策略名或者“操作”列的“管理”，进入对应策略详情页，可以在“用户/组”页面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。



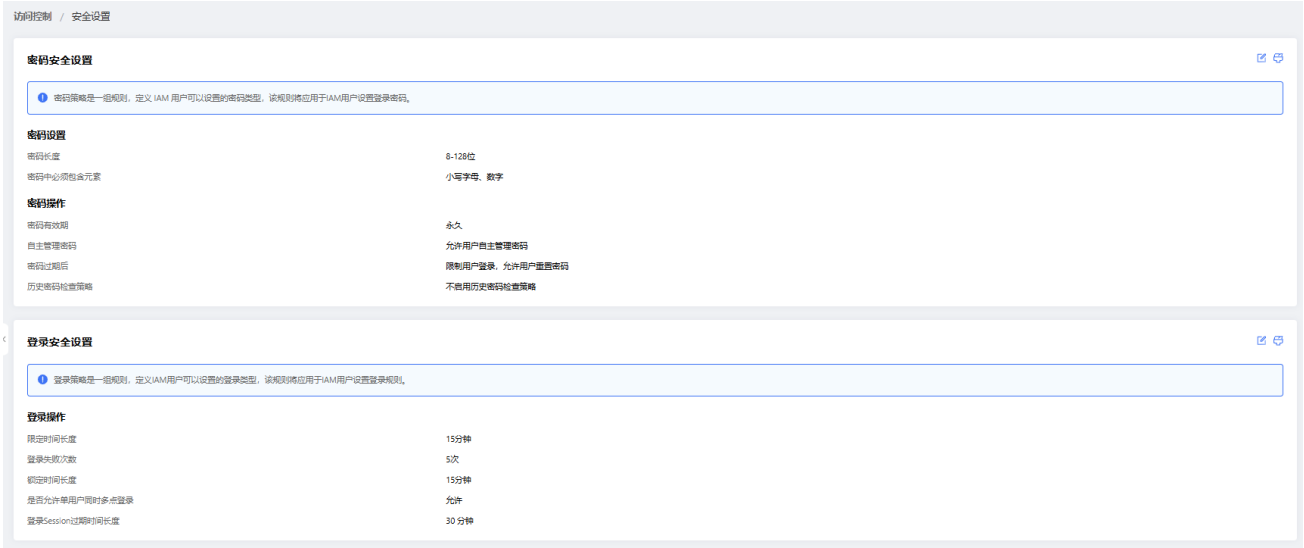
- **授权用户/用户组**

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。



7.5 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和登录安全设置。



7.5.1 密码安全设置

点击“访问控制”>“安全设置”，进入“安全设置”页面，在“密码安全设置”处可以进行编辑密码规则和清除密码规则。

7.5.1.1 编辑密码规则

在“密码安全设置”处点击“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。

7.5.1.2 清除密码规则

在“密码安全设置”处点击“清除密码规则”，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。

7.5.2 登录安全设置

点击“访问控制”>“安全设置”，进入“安全设置”页面，在“登录安全设置”处可以进行编辑登录规则和清除登录规则。

登录策略是一组规则，定义 IAM 用户可以设置的登录类型，该规则将应用于 IAM 用户设置登录规则。

7.5.2.1 编辑登录规则

在“登录安全设置”处点击“编辑登录规则”，可以对 IAM 用户登录规则进行重新设置。

项目	描述
限定登录时长	登录失败次数的限定时间。 如果在限定登录时长内 IAM 用户达到登录失败次数后，会被锁定一段时间，锁定时间结束后，才能重新登录。

	取值：整数形式，[15, 60]，单位是分钟。
登录失败次数	IAM 用户在限定时间内允许连续登录失败的次数。 取值：整数形式，[5, 10]。
锁定时间长度	IAM 用户被锁定的时间。 取值：整数形式，[15, 60]，单位是分钟。
是否允许单用户同时多点登录	是否允许 IAM 用户同一时刻在多个客户端登录。当配置为不允许时，则 IAM 用户不能同时在多个客户端登录，即最后一次的登录会保持，之前的登录将被强制下线。系统默认配置为允许。
登录 Session 过期时间长度	IAM 用户登录控制台后，在无任何操作时，保存会话的时间长度。 取值：整数形式，[10, 30]，单位是分钟。

7.5.2.2 清除登录规则

在“登录安全设置”处点击“清除登录规则”，改为默认登录规则。默认登录规则为：

- 限定时间长度：15 分钟。
- 登录失败次数：5。
- 锁定时间长度：15 分钟。
- 是否允许单用户同时单点登录：允许。
- 登录 Session 过期时间长度：30 分钟。

7.6 安全凭证

7.6.1 密钥

点击“访问控制”>“安全凭证”，可以查看账户详细信息和密钥。账户详细信息包括：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

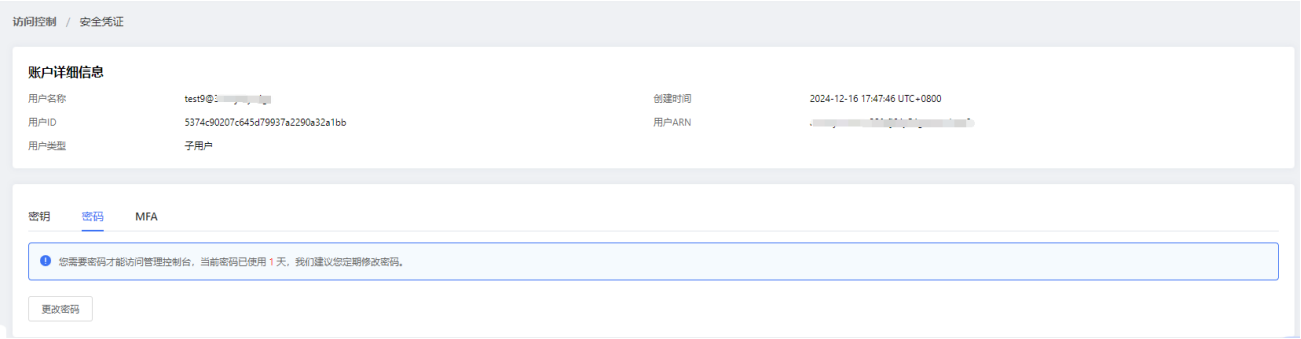
项目	描述
AccessKeyID	密钥 ID。点击编辑按钮，可以对密钥 ID 进行复制。
SecretAccessKey	密钥值，点击查看按钮，可以查看密钥值的明文形式。 **说明：**在 IAM 上线之前创建的密钥才有此项。
创建时间	密钥创建时间。 **无：**表示该密钥是在 IAM 功能上线前创建的。
最后使用时间	密钥最后一次使用的时间。
密钥类型	● **主密钥。** ● **普通密钥。** **说明：**在 IAM 上线之前创建的密钥有此项。
状态	密钥启用状态： ● 启用。 ● 禁用。
操作	可以对密钥进行操作：

	● 启用。 ● 禁用。 ● 删除。

7.6.2 密码

对于 IAM 用户，点击“访问控制”>“安全凭证”>“密码”，可以修改登录密码。

注意：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。



7.6.3 MFA

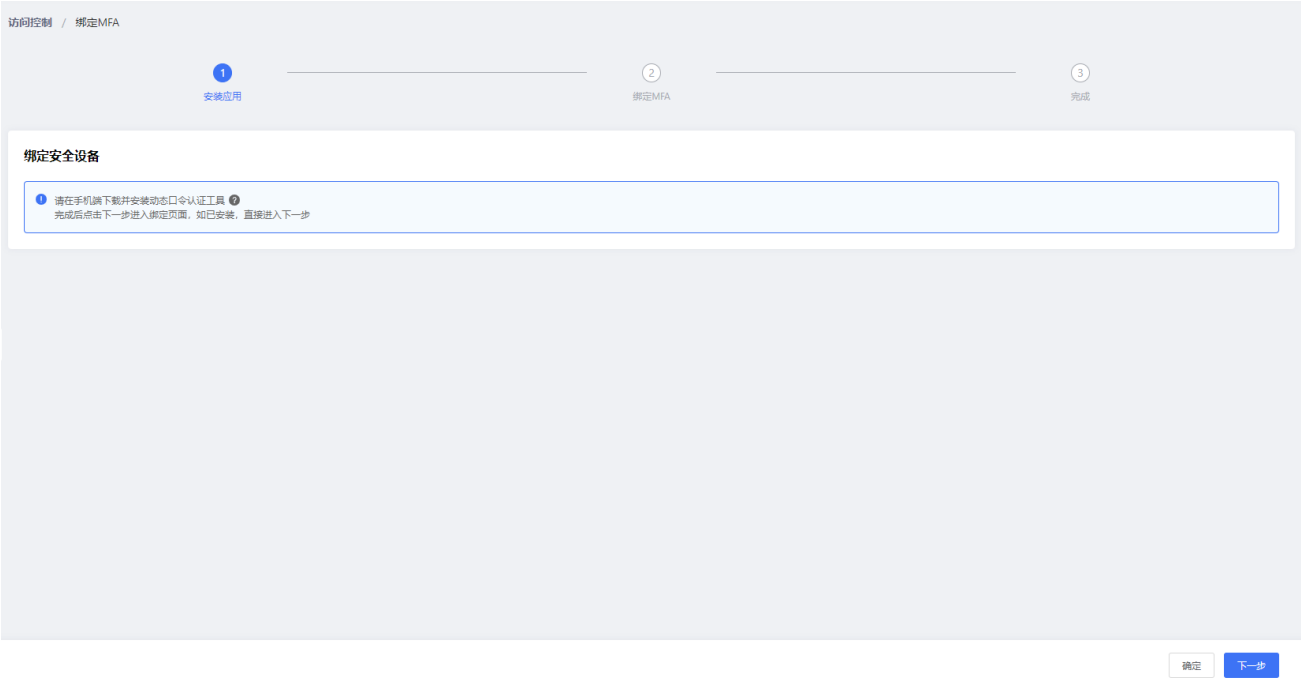
对于 IAM 用户，点击“访问控制”>“安全凭证”>“MFA”，可以绑定 MFA。

注意：MFA 认证仅 IAM 用户支持，但是如果没有授权使用 MFA 认证，则 IAM 用户无法进行 MFA 认证。

点击绑定，进行 MFA 绑定，步骤如下：

1. 安装应用

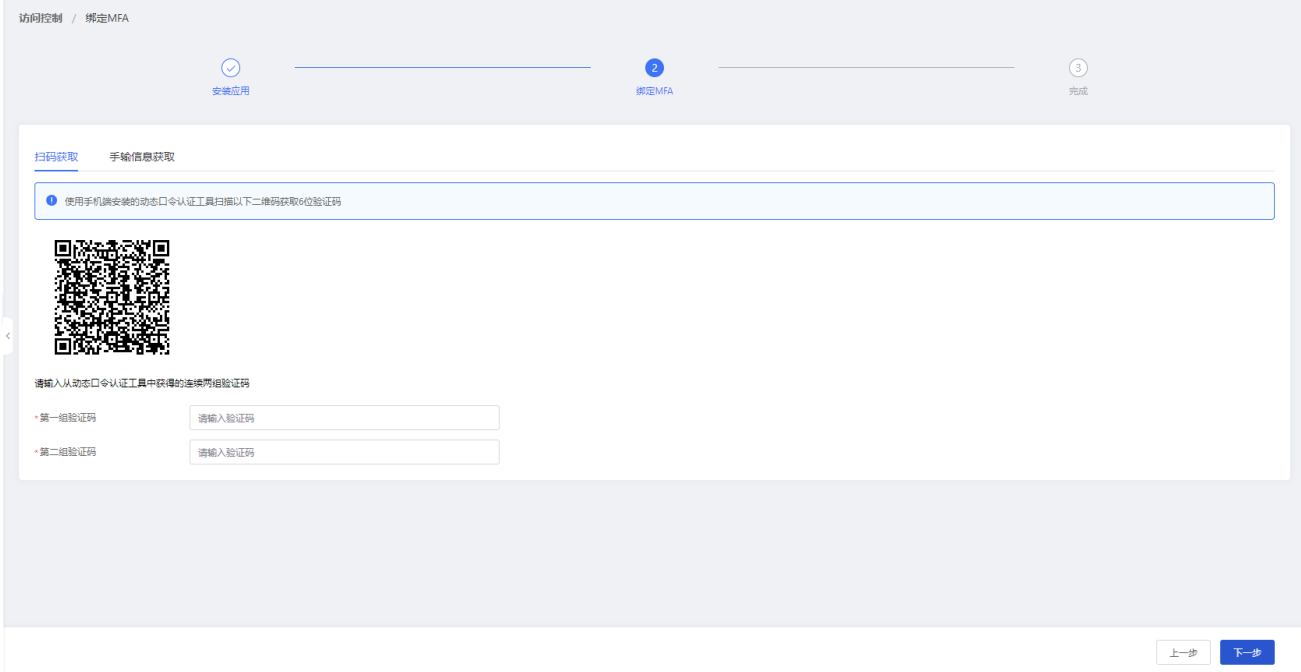
   在手机端下载安装基于时间的一次性密码（TOTP）口令认证工具。



2. 绑定 MFA

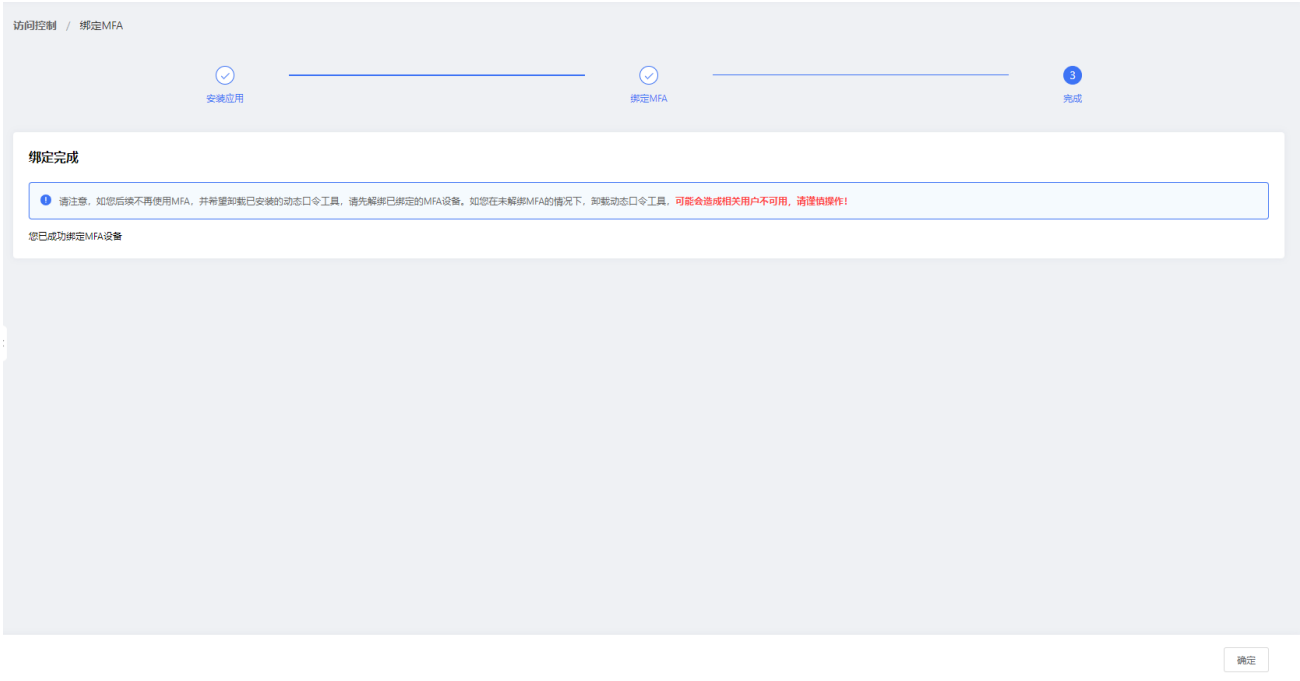
可以使用扫码获取和手动获取两种方式获取验证码。

注意：输入的“第一组验证码”和“第二组验证码”必须是连续的。



3. 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
安装应用
绑定MFA
3
完成
绑定完成
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！
您已成功绑定MFA设备
确定

7.7 IAM 最佳实践

7.7.1 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**

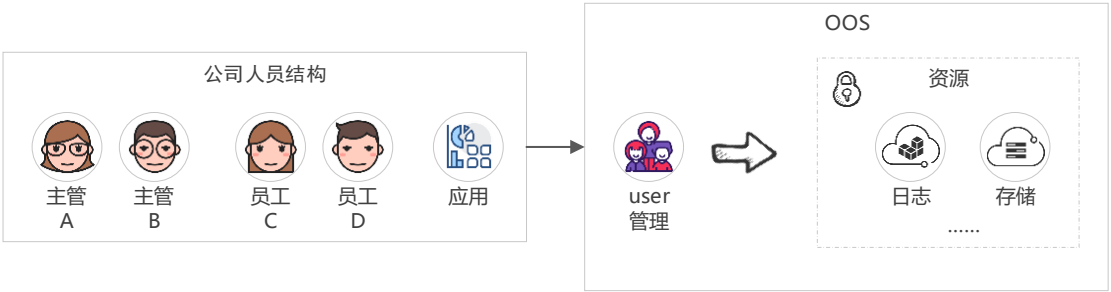
  开启 OOS 的操作跟踪功能，记录用户在账户中做了哪些操作、使用了哪些资源。操作跟踪日志会记录操作的类型、时间、操作的源 IP、操作人员等，并且可以长久的保存在 OOS 存储桶中。

  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。

7.7.2 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 可以查看存储桶文件。
- 编程用户可以对存储桶上传文件。

创建用户组并关联策略

IAM 用户组	包含用户	策略说明	访问方式
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。	控制台访问
IAM 管理组	主管 A	可以进行 IAM 的相关管理操作。	控制台访问
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。	控制台访问
查看文件组	员工 C 和员工 D	查看上传文件的权限。	控制台访问
上传文件组	编程用户	通过 API 可以向指定的 Bucket 内写入数据。	编程访问

保密数据组权限策略示例：

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

```
}
```

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": [
        {
                "Effect": "Allow",
                "Action": [
                    "oos:ListAllMyBucket"
                ],
                "Resource": "*"
        },
        {
        "Sid": "AllowGroupToManageTrail",
        "Effect": "Allow",
        "Action": "cloudtrail:*",
```

```
        "Resource": "*"
        },
        {
        "Sid": "AllowGroupToSeeBucket",
        "Effect": "Allow",
        "Action": [
            "oos:GetObject",
            "oos:ListBucket"
            ],
        "Resource": [
            "arn:ctyun:oos::10rc2arpn6306:trailbucket",
            "arn:ctyun:oos::10rc2arpn6306:trailbucket/*"
            ]
        }
    ]
}
```

查看文件组策略示例

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

上传文件组策略示例

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

8 资源包管理

根据用量需求，您可以订购对象存储资源包，订购须知请参见 https://www.ctyun.cn/h5/orderconsole/oos/buy。

在“**资源包管理**”页面，可以查看已经订购的资源包，订购新的资源包，或者对已有资源包进行续订、退订操作。

9 附录

9.1 域名（Endpoint）列表

对象存储网络、对象存储网络 2、香港节点的 Endpoint 不同。

9.1.1 对象存储网络

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。对象存储网络 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。

说明：对于对象存储网络中的 OOS API，如果您的数据存储在某个资源池，建议您直接使用该资源池的 Endpoint。Endpoint 列表如下（Endpoint 列表仅为资源池 Endpoint 访问信息描述，与资源状态无关联）：

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

9.1.2 对象存储网络 2

对象存储网络 2 中的各个地区，使用统一的 OOS API、统计、操作跟踪和 IAM API 的 Endpoint。对象存储网络 2 Endpoint 列表如下：

- OOS API Endpoint: oos-cn2.ctyunapi.cn，支持 HTTP 和 HTTPS。
- 统计 API Endpoint: oos-cn2-mg.ctyunapi.cn，支持 HTTPS。
- 操作跟踪 API Endpoint：oos-cn2-cloudtrail.ctyunapi.cn，支持 HTTPS。
- IAM Endpoint: oos-cn2-iam.ctyunapi.cn，支持 HTTPS。

说明：对于对象存储网络 2 中的 OOS API，如果您的数据存储在某个资源池，建议您直接使用该资源池的 Endpoint。Endpoint 列表如下（Endpoint 列表仅为资源池 Endpoint 访问信息描述，与资源状态无关联）：

地区	OOS API Endpoint
内蒙古 1	oos-nm1.ctyunapi.cn
杭州 1	oos-hz1.ctyunapi.cn

9.1.3 香港节点

香港节点分为**香港精品网络**和**香港普通网络**两种方式，精品网和普通网 OOS API 的 Endpoint 不同，统计、操作跟踪和 IAM API 的 Endpoint 相同：

- 香港精品网 OOS API Endpoint: oos-cnhk-hqnet.ctyunapi.cn，香港普通网 OOS API Endpoint：oos-cnhk-nqnet.ctyunapi.cn。支持 HTTP 和 HTTPS。
- 统计 API Endpoint: oos-cnhk-mg.ctyunapi.cn，支持 HTTP 和 HTTPS。
- 操作跟踪 API Endpoint：oos-cnhk-cloudtrail.ctyunapi.cn，支持 HTTPS。
- IAM Endpoint：oos-cnhk-iam.ctyunapi.cn，支持 HTTPS。

9.2 操作权限与 API 对应关系

说明：下列表格中“**涉及资源**”列表示操作权限对应的资源（resource），括号内为生效示例。当资源范围为*时，表示将所有资源都赋予策略中的 Action。建议您在分配资源时尽量不使用*，以避免分配过多的资源。

表1 OOS 的操作权限与 API 对应关系

操作权限		涉及资源	API
Bucket 列表	ListBucket	Bucket（*bucketname* 或*）	GET Bucket（List Objects）、HEAD Bucket
	ListAllMyBucket	所有（*）	GET Service
	GetRegions	所有（*）	GET Regions
Bucket 读取	ListBucketMultipartUploads	Bucket（*bucketname* 或*）	List Multipart Uploads
	GetBucketAcl	Bucket（*bucketname* 或*）	GET Bucket acl
	GetBucketLocation	Bucket（*bucketname* 或*）	GET Bucket location
	GetBucketPolicy	Bucket（*bucketname* 或*）	GET Bucket policy
	GetLifecycleConfiguration	Bucket（*bucketname* 或*）	GET Bucket lifecycle
	GetBucketWebsite	Bucket（*bucketname* 或*）	GET Bucket website
	GetBucketCORS	Bucket（*bucketname* 或*）	GET Bucket cors
	GetBucketLogging	Bucket（*bucketname* 或*）	GET Bucket logging
	GetBucketObjectLockConfiguration	Bucket（*bucketname* 或*）	GET Bucket Object Lock
	GetBucketInventoryConfiguration	Bucket（*bucketname* 或*）	GET Bucket Inventory Configuration、List Bucket Inventory Configuration
Bucket 写入	PutBucket	Bucket（*bucketname* 或*）	PUT Bucket
	DeleteBucket	Bucket（*bucketname* 或*）	DELETE Bucket
	DeleteMultipleObjects	Bucket（*bucketname* 或*）	DELETE Multiple Objects
	PutLifecycleConfiguration	Bucket（*bucketname* 或*）	PUT Bucket lifecycle、DELETE Bucket lifecycle
	PutBucketWebsite	Bucket（*bucketname* 或*）	PUT Bucket website

	DeleteBucketWebsite	Bucket（*bucketname* 或*）	DELETE Bucket website
	PutBucketCORS	Bucket（*bucketname* 或*）	PUT Bucket cors、DELETE Bucket cors
	PutBucketLogging	Bucket（*bucketname* 或*）	PUT Bucket logging
	PutBucketObjectLockConfiguration	Bucket（*bucketname* 或*）	PUT Bucket Object Lock
	DeleteBucketObjectLockConfiguration	Bucket（*bucketname* 或*）	DELETE Bucket Object Lock
	PutBucketInventoryConfiguration	Bucket（*bucketname* 或*）	PUT Bucket Inventory Configuration、DELETE Bucket Inventory Configuration
Bucket 权限	PutBucketPolicy	Bucket（*bucketname* 或*）	PUT Bucket policy
	DeleteBucketPolicy	Bucket（*bucketname* 或*）	DELETE Bucket policy
Object 读取	ListMultipartUploadParts	Object（*bucketname*/*objectname*、*bucketname*/*或*）	List Parts
	GetObject	Object（*bucketname*/*objectname*、*bucketname*/*或*）	GET Object、HEAD Object
Object 写入	PutObject	Object（*bucketname*/*objectname*、*bucketname*/*或*）	PUT Object、PUT Object-Copy、POST Object、Initiate Mulitipart Upload、Upload Part、Compelete Multipart Upload、Upload Part – Copy
	DeleteObject	Object	DELETE Object

		（*bucketname*/*objectname*、*bucketname*/*或*）	
	AbortMultipartUpload	Object（*bucketname*/*objectname*、*bucketname*/*或*）	Abort Multipart Upload

表2 统计的操作权限与 API 对应关系

操作权限	涉及资源	API
GetAccountStatistcsSummary	所有（*）	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		涉及资源	API
列表	DescribeTrails	trail（trail/*或*）	DescribeTrails
	LookupEvents	trail（trail/*或*）	LookupEvents
读取	GetEventSelectors	trail（trail/*trailname*、trail/*或*）	GetEventSelectors
	GetTrailStatus	trail（trail/*trailname*、trail/*或*）	GetTrailStatus
写入	PutEventSelectors	trail（trail/*trailname*、trail/*或*）	PutEventSelectors
	StopLogging	trail（trail/*trailname*、trail/*或*）	StopLogging
	CreateTrail	trail（trail/*trailname*、trail/*或*）	CreateTrail
	UpdateTrail	trail（trail/*trailname*、trail/*或*）	UpdateTrail
	DeleteTrail	trail（trail/*trailname*、trail/*或*）	DeleteTrail
	StartLogging	trail（trail/*trailname*、trail/*或*）	StartLogging

表4 IAM 的操作权限与 API 对应关系

操作权限		涉及资源	API
列表	GetAccountSummary	所有（*）	GetAccountSummary
	GetLoginProfile	user（user/*username*、user/*或*）	GetLoginProfile
	ListAccessKeys	user（user/*username*、user/*或*）	ListAccessKeys
	ListUsers	user（user/*或*）	ListUsers
	ListUserTags	user（user/*username*、user/*或*）	ListUserTags
	ListGroups	group（group/*或*）	ListGroups
	ListGroupsForUser	user（user/*username*、user/*或*）	ListGroupsForUser
	ListPolicies	policy（policy/*或*）	ListPolicies
	ListAttachedGroupPolicies	group（group/*groupname*、group/*或*）	ListAttachedGroupPolicies
	ListAttachedUserPolicies	user（user/*username*、user/*或*）	ListAttachedUserPolicies
	ListEntitiesForPolicy	policy（policy/*policyname*、policy/*或*）	ListEntitiesForPolicy
	ListMFADevices	user（user/*username*、user/*或*）	ListMFADevices
	ListVirtualMFADevices	mfa（mfa/*或*）	ListVirtualMFADevices
读取	GetUser	user（user/*username*、user/*或*）	GetUser
	GetAccessKeyLastUsed	user（user/*username*、user/*或*）	GetAccessKeyLastUsed

	GetGroup	group（group/*groupname*、group/*或*）	GetGroup
	GetPolicy	policy（policy/*policyname*、policy/*或*）	GetPolicy
	GetAccountPasswordPolicy	所有（*）	GetAccountPasswordPolicy
	GetAccountLoginSecurityPolicy	所有（*）	GetAccountLoginSecurityPolicy
写入	CreateAccessKey	user（user/*username*、user/*或*）	CreateAccessKey
	DeleteAccessKey	user（user/*username*、user/*或*）	DeleteAccessKey
	UpdateAccessKey	user（user/*username*、user/*或*）	UpdateAccessKey
	CreateUser	user（user/*username*、user/*或*）	CreateUser
	DeleteUser	user（user/*username*、user/*或*）	DeleteUser
	TagUser	user（user/*username*、user/*或*）	TagUser
	UntagUser	user（user/*username*、user/*或*）	UntagUser
	CreateGroup	group（group/*groupname*、group/*或*）	CreateGroup
	DeleteGroup	group（group/*groupname*、group/*或*）	DeleteGroup

	AddUserToGroup	group（group/*groupname*、group/*或*）	AddUserToGroup
	RemoveUserFromGroup	group（group/*groupname*、group/*或*）	RemoveUserFromGroup
	ChangePassword	user（user/*username*、user/*或*）	ChangePassword
	UpdateAccountPasswordPolicy	所有（*）	UpdateAccountPasswordPolicy
	DeleteAccountPasswordPolicy	所有（*）	DeleteAccountPasswordPolicy
	UpdateAccountLoginSecurityPolicy	所有（*）	UpdateAccountLoginSecurityPolicy
	DeleteAccountLoginSecurityPolicy	所有（*）	DeleteAccountLoginSecurityPolicy
	CreateVirtualMFADevice	mfa（mfa/*mfaname*、mfa/*或*）	CreateVirtualMFADevice
	DeactivateMFADevice	user（user/*username*、user/*或*）	DeactivateMFADevice
	DeleteVirtualMFADevice	mfa（mfa/*mfaname*、mfa/*或*）	DeleteVirtualMFADevice
	EnableMFADevice	user（user/*username*、user/*或*）	EnableMFADevice
	CreateLoginProfile	user（user/*username*、user/*或*）	CreateLoginProfile
	DeleteLoginProfile	user（user/*username*、user/*或*）	DeleteLoginProfile
	UpdateLoginProfile	user（user/*username*、user/*或*）	UpdateLoginProfile
权限	CreatePolicy	policy（policy/*policyname*、	CreatePolicy

		policy/*或*）	
	DeletePolicy	policy（policy/*policyname*、policy/*或*）	DeletePolicy
	AttachUserPolicy	user（user/*username*、user/*或*）	AttachUserPolicy
	DetachUserPolicy	user（user/*username*、user/*或*）	DetachUserPolicy
	AttachGroupPolicy	group（group/*groupname*、group/*或*）	AttachGroupPolicy
	DetachGroupPolicy	group（group/*groupname*、group/*或*）	DetachGroupPolicy

9.3 IAM 策略编写规则

9.3.1 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。

9.3.2 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，多个 JSON 语句块之间是逻辑或的关系。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）。

注意：如果多个 JSON 语句块之间有重叠或者冲突，默认情况下包含 Deny 的语句优先级最高，但是如果 JSON 语句块中包含 ctyun:MuliFactorAuthPresent 和 ctyun:MuliFactorAuthAge 的条件且请求来自 OOS 控制台，则优先判断该语句，通过后再判断其他 Deny 或者 Allow 的语句。

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/*"
            ]
        }
    ]
}
```

9.3.2.1 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。

9.3.2.2 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。

9.3.2.3 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：获取文件操作。

```
"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*"
```

9.3.2.4 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": "*",
    }]
}
```

9.3.2.5 Resource

Resource 元素指定执行策略的资源，可以指定一个或多个文件。

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

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。

9.3.2.6 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。

9.3.2.7 Condition

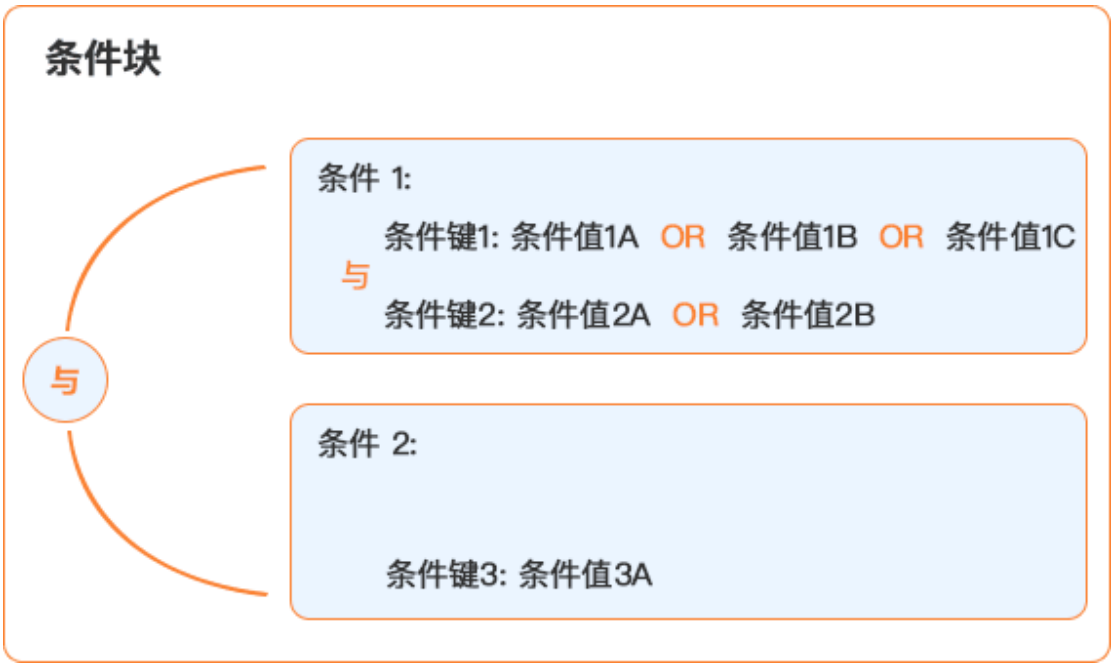
Condition 元素描述允许用户指定策略生效的条件。在 Condition 元素中，用户可构建表达式，并使用条件运算符将策略中的条件与请求值相匹配。

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	1~64 位字符串组成，

	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（=）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。	字符串，可以包含特殊字符。

	● **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: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**：不建议对 GetObject 接口设置该条件键，否则在 OOS 控制台上无法下载、预览、分享文件和编辑元数据。	● **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**：不建议对 GetObject 接口设置该条件键，否则在 OOS 控制台上无法下载、预览、分享文件和编辑元数据。	整数形式，以秒为单位。
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。	字符串形式。 说明：本条件键仅对 ListBucket 生效。

	● **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。	字符串形式。 取值为： ● private：私有 ● public-read：公共读 ● public-read-write：公共读写 **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 (?)。	

说明：

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

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 } }
```

9.3.2.8 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“**${ctyun:username}**”、“**${ctyun:AccessKey}**”。当策略执行时，策略变量将被替换为请求本身的用户名或 AccessKey。

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