天翼云对象存储

控制台使用指南

天翼云科技有限公司

目 录

1 产品介绍

1.1 什么是对象存储服务

对象存储服务（Object Storage Service，OBS）是一个基于对象的海量存储服务，为客户提供海量、安全、高可靠、低成本的数据存储能力，包括：创建、修改、删除桶，上传、下载、删除对象等。

OBS 系统和单个桶都没有总数据容量和对象/文件数量的限制，为用户提供了超大存储容量的能力，适合存放任意类型的文件，适合普通用户、网站、企业和开发者使用。OBS 是一项面向 Internet 访问的服务，提供了基于 HTTP/HTTPS 协议的 Web 服务接口，用户可以随时随地连接到 Internet，通过 OBS 管理控制台或客户端访问和管理存储在 OBS 中的数据。此外，OBS 支持 OBS API 接口，可使用户方便管理自己存储在 OBS 上的数据，以及开发多种类型的上层业务应用。

云服务实现了在多区域部署基础设施，具备高度的可扩展性和可靠性，用户可根据自身需要指定区域使用 OBS，由此获得更快的访问速度和实惠的服务价格。

1.2 产品优势

OBS 与自建存储服务器对比

在信息时代，企业数据直线增长，自建存储服务器存在诸多劣势，已无法满足企业日益强烈的存储需求。表 1-1 向您详细展示了 OBS 与自建存储服务器的优劣势对比。

表1-1 OBS 与自建存储服务器对比

对比项	OBS	自建存储服务器
数据存储量	提供海量的存储服务，所有业务、存储节点采用分布式集群方式部署，各节点、集群都可以独立扩容，用户永远不必担心存储容量不够。	数据存储量受限于搭建存储服务器时使用的硬件设备，存储量不够时需要重新购买存储硬盘，进行人工扩容。
安全性	支持 HTTPS/SSL 安全协议，支	需自行承担网络信息安全、技术漏

对比项	OBS	自建存储服务器
	持数据加密上传。同时 OBS 通过访问密钥（AK/SK）对访问用户的身份进行鉴权，结合 IAM 策略、桶策略、ACL、防盗链等多种方式和技术确保数据传输与访问的安全。	洞、误操作等各方面的数据安全风险。
成本	即开即用，免去了自建存储服务器前期的资金、时间以及人力成本的投入，后期设备的维护交由 OBS 处理。	前期安装难、设备成本高、初始投资大、自建周期长、后期运维成本高，无法匹配快速变更的企业业务，安全保障的费用还需额外考虑。

OBS 的优势

- **数据稳定，业务可靠**：OBS 支撑数亿用户访问，稳定可靠。
- **多重防护，授权管理**：OBS 支持多版本控制、服务端加密、防盗链、VPC 网络隔离、访问日志审计以及细粒度的权限控制，保障数据安全可信。
- **千亿对象，千万并发**：OBS 通过智能调度和响应，优化数据访问路径，并结合传输加速、大数据垂直优化等，为各场景下用户的千亿对象提供千万级并发、超高带宽、稳定低时延的数据访问体验。
- **简单易用，便于管理**：OBS 支持标准 REST API 和数据迁移工具，让业务快速上云。无需事先规划存储容量，存储资源和性能可线性无限扩展，不用担心存储资源扩容、缩容问题。

1.3 应用场景

- OBS 可用于存取任何格式、海量的对象/文件数据；因为它是互联网存储，可以在互联网的任何位置随时执行对 OBS 的存取操作。对任何基于互联网的应用程序而言，包括 web 网站、视频应用、SaaS 应用、网盘、移动 APP 等，开发人员均可以将其作为数据存储的理想选择。此外，对于备份、大数据存储、归档等近线、离线存储场景，OBS 也是节省投资的存储方式。
- OBS 的主要特点是海量（容量巨大、线性扩展）、省钱（零初始投资，用多少算多少，用得越多越经济）、可靠、安全（访问、传输、保存端到端安全）。使用 OBS 后，开发人员可以无须关注底层存储技术，而是专注于业务创新，因为无论业务如何发展，开发人员都无须规划存储容量，数据可以快速访问、线性扩容，且具有高可靠性和高安全性。最重要的是业务使用 IT 的成本可以大大降低。

OBS 可应用于视频监控、视频点播、备份归档、HPC（High-performance computing，高性能计算）、移动互联网、企业云盘（网盘）等场景。

1.4 权限管理

如果您需要对 OBS 资源，为企业中的员工设置不同的用户访问权限，以达到不同员工之间的权限隔离，您可以使用统一身份认证服务（Identity and Access Management，简称 IAM）进行精细的权限管理。该服务提供用户身份认证、权限分配、访问控制等功能，可以帮助您安全的控制云服务资源的访问。

通过 IAM，您可以在帐号中给员工创建 IAM 用户，并授权控制他们对资源的访问范围。例如您的员工中有负责软件开发的人员，您希望他们拥有 OBS 的使用权限，但是不希望他们拥有删除 OBS 资源等高危操作的权限，那么您可以使用 IAM 为开发人员创建用户，通过授予仅能使用 OBS，但是不允许删除 OBS 资源的权限，控制他们对 OBS 资源的使用范围。

如果帐号已经能满足您的要求，不需要创建独立的 IAM 用户进行权限管理，您可以跳过本章节，不影响您使用 OBS 的其它功能。

IAM 是云平台提供权限管理的基础服务，无需付费即可使用，您只需要为您帐号中的资源进行付费。关于 IAM 的详细介绍，请参见《天翼云-统一身份认证服务用户指南》“产品介绍”章节。

OBS 权限

默认情况下，新建的 IAM 用户没有任何权限，您需要将其加入用户组，并给用户组授予策略，才能使得用户组中的用户获得策略定义的权限，这一过程称为授权。授权后，用户就可以基于策略对云服务进行操作。IAM 系统预置了各服务的常用权限，例如完全控制权限、只读权限，您可以直接使用这些系统策略。

OBS 部署时不区分物理区域，为全局级服务。授权时，在全局项目中设置策略，访问 OBS 时，不需要切换区域。

RBAC 策略：RBAC 策略是将服务作为一个整体进行授权，授权后，用户可以拥有这个服务的所有权限，如访问整个服务、管理整个服务，RBAC 策略无法针对服务中的具体操作做权限控制。

说明

由于缓存的存在，对用户、用户组以及企业项目授予 OBS 相关的 RBAC 策略后，大概需要等待 10~15 分钟策略才能生效。

表 1-2 为 OBS 的所有系统策略。

表1-2 OBS 系统策略

策略名称	描述	策略类别
Tenant Administrator	操作权限：对帐号拥有的所有云资源执行任意操作。 OBS 策略在“全局服务>对象存储服务”下配置。	RBAC 策略
Tenant Guest	操作权限：对帐号拥有的所有云资源的只读权限。	RBAC 策略

策略名称	描述	策略类别
	OBS 策略在“全局服务>对象存储服务”下配置。	

用户拥有 OBS 资源权限后，对应在 OBS 上可以执行的具体操作下表所示。

表1-3 OBS 操作与资源权限关系

操作名称	Tenant Administrator 权限	Tenant Guest 权限
列举桶	可以	可以
创建桶	可以	不可以
删除桶	可以	不可以
获取桶基本信息	可以	可以
管理桶访问权限	可以	不可以
管理桶策略	可以	不可以
列举对象	可以	可以
列举多版本对象	可以	可以
上传文件	可以	不可以
新建文件夹	可以	不可以
删除文件	可以	不可以
删除文件夹	可以	不可以
下载文件	可以	可以
删除多版本文件	可以	不可以
下载多版本文件	可以	可以
取消删除文件	可以	不可以
删除碎片	可以	不可以
管理对象访问权限	可以	不可以
设置对象元数据	可以	不可以
获取对象元数据	可以	不可以
管理多版本控制	可以	不可以
管理日志记录	可以	不可以
管理标签	可以	不可以

操作名称	Tenant Administrator 权限	Tenant Guest 权限
管理生命周期规则	可以	不可以
管理静态网站托管	可以	不可以
管理 CORS 规则	可以	不可以
管理防盗链	可以	不可以
管理跨区域复制	可以	不可以
管理图片处理	可以	不可以
设置对象 ACL	可以	不可以
设置指定版本对象 ACL	可以	不可以
获取对象 ACL	可以	可以
获取指定版本对象 ACL	可以	可以
多段上传	可以	不可以
列举已上传段	可以	可以
取消多段上传任务	可以	不可以

OBS 资源权限管理

OBS 桶和对象的权限可以通过 IAM 用户权限、桶策略和 ACL 共同控制。

更多关于 OBS 资源权限管理的内容请参见权限管理概述。

1.5 使用方式

您可以通过以下工具连接到 OBS 资源，对资源进行管理操作。

表1-4 OBS 资源管理工具

工具	描述
管理控制台	管理控制台是网页形式的。通过管理控制台，您可以使用直观的界面进行相应的操作。
OBS Browser+	OBS Browser+是一款运行在 Windows 系统上的对象存储服务客户端，可以非常方便地让您在个人电脑上进行对象存储的操作。
API	OBS 提供 REST 形式的访问接口，使用户能够非常容易地从 Web 应用中访问 OBS。用户可以通过本文档提供的简单的

工具	描述
	REST 接口，在任何时间、任何地点、任何互联网设备上进行上传和下载数据。

1.6 与其他服务的关系

表1-5 与其他服务的关系

功能	相关服务	位置
通过 IAM 服务实现以下功能： • 用户身份鉴权 • IAM 用户权限设置 • IAM 委托设置	统一身份认证服务（Identity and Access Management，IAM）	权限管理 设置用户权限 创建 IAM 委托
标签用于标识 OBS 中的桶，以实现对 OBS 中的桶进行分类。	标签管理服务（Tag Management Service，TMS）	标签简介
通过密钥管理 KMS 功能对上传到 OBS 中的文件进行加密。	数据加密服务（Data Encryption Workshop，DEW）	服务端加密简介

OBS 可以作为其他云服务的存储资源池，例如关系型数据库（RDS），镜像服务（IMS），云审计服务（CTS）等。

1.7 基本概念

1.7.1 对象

对象（Object）是 OBS 中数据存储的基本单位，一个对象实际是一个文件的数据与其相关属性信息（元数据）的集合体。用户上传至 OBS 的数据都以对象的形式保存在桶中。

对象包括了 Key，Metadata，Data 三部分：

- Key：键值，即对象的名称，为经过 UTF-8 编码的长度大于 0 且不超过 1024 的字符序列。一个桶里的每个对象必须拥有唯一的对象键值。
- Metadata：元数据，即对象的描述信息，包括系统元数据和用户元数据，这些元数据以键值对（Key-Value）的形式被上传到 OBS 中。

  - 系统元数据由 OBS 自动产生，在处理对象数据时使用，包括 Date，Content-length，Last-modify，ETag 等。
  - 用户元数据由用户在上传对象时指定，是用户自定义的对象描述信息。
- Data：数据，即文件的数据内容。

通常，我们将对象等同于文件来进行管理，但是由于 OBS 是一种对象存储服务，并没有文件系统中的文件和文件夹概念。为了使用户更方便进行管理数据，OBS 提供了一种方式模拟文件夹。通过在对象的名称中增加“/”，例如“test/123.jpg”。此时，“test”就被模拟成了一个文件夹，“123.jpg”则模拟成“test”文件夹下的文件名了，而实际上，对象名称（Key）仍然是“test/123.jpg”。

在 OBS 管理控制台和客户端上，用户均可直接使用文件夹的功能，符合文件系统下的操作习惯。

1.7.2 桶

桶（Bucket）是 OBS 中存储对象的容器。对象存储提供了基于桶和对象的扁平化存储方式，桶中的所有对象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。

每个桶都有自己的访问权限、所属区域等属性，用户可以在不同区域创建不同访问权限的桶，并配置更多高级属性来满足不同场景的存储诉求。

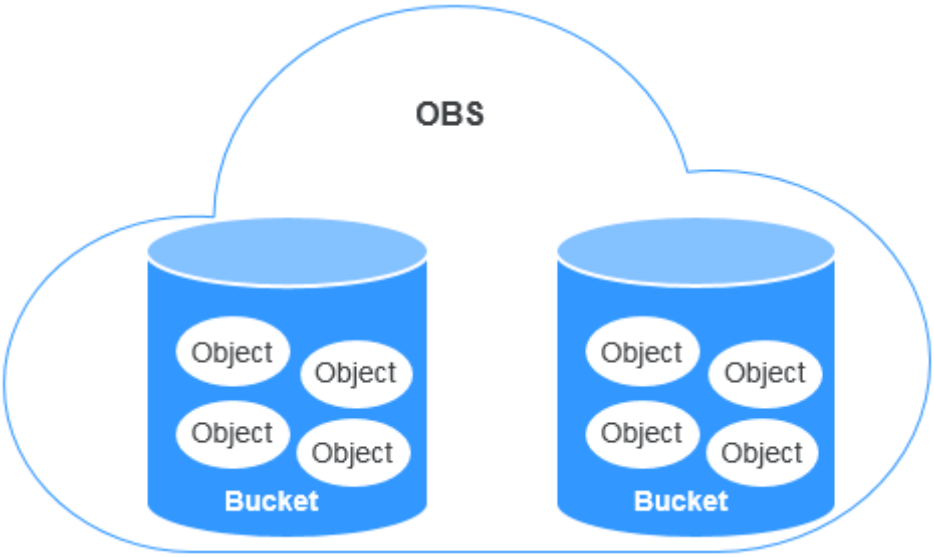
在 OBS 中，桶名必须是全局唯一的且不能修改，即用户创建的桶不能与自己已创建的其他桶名称相同，也不能与同帐号、其他帐号及帐号下的所有 IAM 用户创建的桶名称相同。桶所属的区域在创建后也不能修改。每个桶在创建时都会生成默认的桶 ACL（Access Control List，访问控制列表），桶 ACL 的每项包含了对被授权用户授予什么样的权限，如读取权限、写入权限等。用户只有对桶有相应的权限，才可以对桶进行操作，如创建、删除、显示、设置桶 ACL 等。

一个帐号及帐号下的所有 IAM 用户可创建的桶+并行文件系统的上限为 100 个。每个桶中存放的对象的数量和大小总和没有限制，用户不需要考虑数据的可扩展性。

由于 OBS 是基于 REST 风格 HTTP 和 HTTPS 协议的服务，您可以通过 URL（Uniform Resource Locator）来定位资源。

OBS 中桶和对象的关系如图 1-1 所示：

图1-1 桶和对象



1.7.3 并行文件系统

并行文件系统（Parallel File System）是对象存储服务（Object Storage Service，OBS）提供的一种经过优化的高性能文件系统，提供毫秒级别访问时延，以及 TB/s 级别带宽和百万级别的 IOPS，能够快速处理高性能计算（HPC）工作负载。

并行文件系统的详细介绍和使用说明，请参见《对象存储（OBS）-并行文件系统特性指南》。

1.7.4 访问密钥（AK/SK）

OBS 支持通过 AK/SK 认证方式进行认证鉴权，即使用 Access Key ID（AK）/Secret Access Key（SK）加密的方法来验证某个请求发送者身份。当您使用 OBS 提供的 API 进行二次开发并通过 AK/SK 认证方式完成认证鉴权时，需要按照 OBS 定义的签名算法来计算签名并添加到请求中。

OBS 支持使用永久 AK/SK 鉴权，也支持通过临时 AK/SK 和 securitytoken 进行认证鉴权。

永久 AK/SK

用户可以在“我的凭证”页面创建永久 AK/SK。

- Access Key Id（AK）：访问密钥 ID。与私有访问密钥关联的唯一标识符；访问密钥 ID 和私有访问密钥一起使用，对请求进行加密签名。
- Secret Access Key（SK）：与访问密钥 ID 结合使用的私有访问密钥，对请求进行加密签名，可标识发送方，并防止请求被修改。

临时 AK/SK

临时 AK/SK 和 securitytoken 是系统颁发给用户的临时访问令牌，有效期范围为 15 分钟至 24 小时，过期后需要重新获取。临时 AK/SK 和 securitytoken 遵循权限最小化原则，可应用于临时访问 OBS。如果未使用 securitytoken，会返回 403 错误。

- 临时 Access Key Id：临时访问密钥 ID。与私有访问密钥关联的唯一标识符；访问密钥 ID 和私有访问密钥一起使用，对请求进行加密签名。
- 临时 Secret Access Key：与临时访问密钥 ID 结合使用的临时私有访问密钥，对请求进行加密签名，可标识发送方，并防止请求被修改。
- securitytoken：与临时访问密钥 ID 和临时私有访问密钥结合使用，可以访问指定帐号下所有资源。

当使用如下工具访问 OBS 资源时，需配置 AK/SK 用于生成鉴权信息进行安全认证。

表1-6 OBS 资源管理工具

工具	AK/SK 配置方式
OBS Browser+	在配置帐号时配置 AK 和 SK。
API	在计算签名时添加 AK 和 SK 到请求中。

1.7.5 终端节点（Endpoint）和访问域名

终端节点（Endpoint）：OBS 为每个区域提供一个终端节点，终端节点可以理解为 OBS 在不同区域的区域域名，用于处理各自区域的访问请求。请从帮助中心获取区域和终端节点信息。

访问域名：OBS 会为每一个桶分配默认的访问域名。访问域名是桶在互联网中的域名地址，可应用于直接通过域名访问桶的场景，比如：云应用开发、数据分享等。

OBS 桶访问域名的结构为：**BucketName.Endpoint**。其中 **BucketName** 为桶名称，**Endpoint** 为桶所在区域的终端节点（区域域名）。

除了桶访问域名外，表 1-7 列出了与 OBS 相关的其他域名的结构、协议类型等信息，以便您全面地了解 OBS 域名。

表1-7 OBS 域名组成规则

域名类型	域名结构	说明	协议类型
区域域名	**Endpoint**	不同的区域分配各自对应的域名，即各区域的终端节点。 请从帮助中心获取区域和终端节点信息。	HTTPS HTTP
桶访问	**BucketName.Endpoint**	桶创建成功后，可以使用桶	HTT

域名类型	域名结构	说明	协议类型
域名		访问域名来访问桶。您可以根据访问域名结构自行拼接，也可以通过在 OBS 管理控制台、OBS Browser+上查看桶基本信息获取。	PS HTTP
对象访问域名	**BucketName.Endpoint/ObjectName**	对象上传到桶中后，可以使用对象访问域名来访问桶中的指定对象。您可以根据访问域名结构自行拼接，也可以通过在 OBS 管理控制台、OBS Browser+上查看对象属性获取。	HTTPS HTTP
静态网站访问域名	**BucketName.obs-website.Endpoint**	桶配置为静态网站托管时，桶的静态网站访问域名。	HTTPS HTTP

1.7.6 区域和可用区

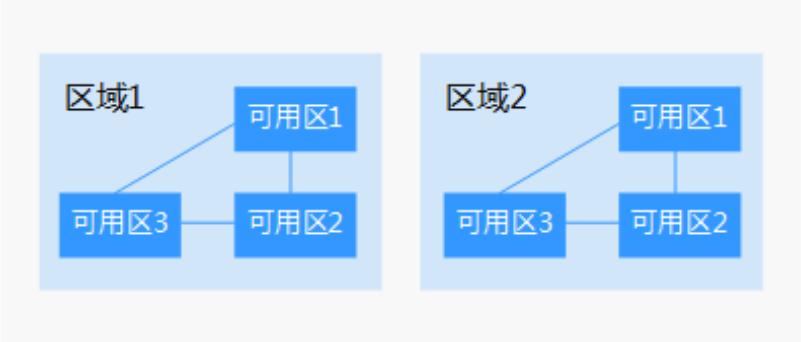
什么是区域、可用区？

我们用区域和可用区来描述数据中心的位置，您可以在特定的区域、可用区创建资源。

- 区域（Region）指物理的数据中心。每个区域完全独立，这样可以实现最大程度的容错能力和稳定性。资源创建成功后不能更换区域。
- 可用区（AZ，Availability Zone）是同一区域内，电力和网络互相隔离的物理区域，一个可用区不受其他可用区故障的影响。一个区域内可以有多个可用区，不同可用区之间物理隔离，但内网互通，既保障了可用区的独立性，又提供了低价、低时延的网络连接。

图 1-2 阐明了区域和可用区之间的关系。

图1-2 区域和可用区



如何选择区域？

建议就近选择靠近您或者您的目标用户的区域，这样可以减少网络时延，提高访问速度。

如何选择可用区？

是否将资源放在同一可用区内，主要取决于您对容灾能力和网络时延的要求。

- 如果您的应用需要较高的容灾能力，建议您将资源部署在同一区域的不同可用区内。
- 如果您的应用要求实例之间的网络延时较低，则建议您将资源创建在同一可用区内。

区域和终端节点

当您通过 API 使用资源时，您必须指定其区域终端节点。请向企业管理员获取区域和终端节点信息。

2 控制台指南

2.1 控制台功能概述

目前，OBS 管理控制台提供的功能如表 2-1 所示：

表2-1 功能概述

功能	说明
桶基本操作	指定 region（不同服务区域）创建桶、删除桶等。
对象基本操作	管理对象，包括上传（含多段上传功能）、下载、删除等。
服务端加密	用户可根据需要对对象进行服务端加密，使对象更安全的存储在 OBS 中。
对象元数据	根据用户需要为对象设置属性。
碎片管理	碎片管理功能可以清除由于对象上传失败而产生的碎片。
多版本控制	管理桶的多版本状态，允许桶内同一个对象存在多个版本。
日志记录	支持对桶的访问请求创建并保存访问日志记录，可用于进行请求分析或日志审计。
权限控制	支持通过 IAM 策略、桶策略&对象策略和桶/对象 ACL 对 OBS 进行访问控制。
生命周期管理	支持设置桶的生命周期管理策略，实现定时删除桶中的对象。
跨区域复制	跨区域复制是指通过创建跨区域复制规则，在同一个帐号下，将一个桶（源桶）中的数据自动、异步地复制到不同区域的另外一个桶（目标桶）中。 跨区域复制能够为用户提供跨区域数据容灾的能力，满足用户数据复制到异地进行备份的需求。

功能	说明
标签	用于对 OBS 中的桶进行标识和分类。
静态网站托管	支持设置桶的网站属性，实现静态网站托管；也可设置网页重定向，访问桶资源可以重定向至指定的主机。
防盗链	提供防盗链功能，防止 OBS 中的对象链接被其他网站盗用。
跨域资源共享	跨域资源共享（CORS）是由 W3C 标准化组织提出的一种网络浏览器的规范机制，定义了一个域中加载的客户端 Web 应用程序与另一个域中的资源交互的方式。而在通常的网页请求中，由于同源安全策略（Same Origin Policy，SOP）的存在，不同域之间的网站脚本和内容是无法进行交互的。

天翼云各区域支持的能力不一致，具体清单参见如下链接：

https://www.ctyun.cn/document/10000101/10028441

2.2 使用限制

OBS 管理控制台支持的浏览器版本如表 2-2 所示：

表2-2 OBS 管理控制台支持的浏览器版本

浏览器	版本
Internet Explorer	• Internet Explorer 9 (IE9) • Internet Explorer 10 (IE10) • Internet Explorer 11 (IE11)
Firefox	Firefox 55 及以后
Chrome	Chrome 60 及以后

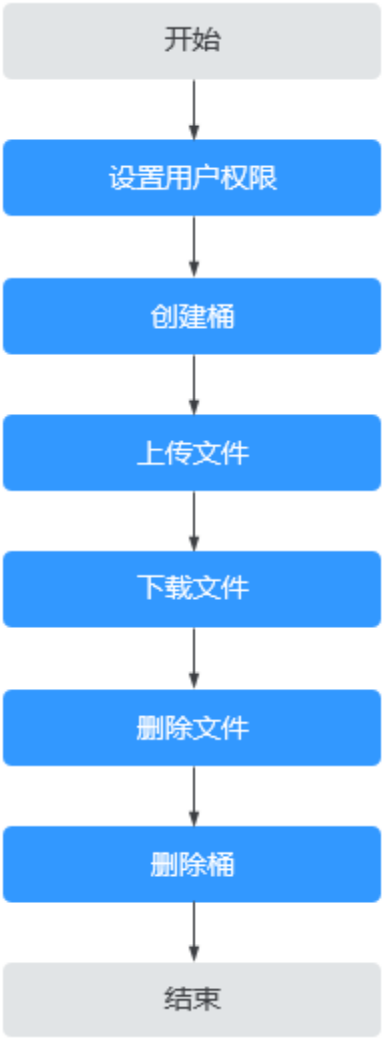
2.3 入门

2.3.1 流程简介

OBS 最基础的入门操作包括创建桶、上传对象和下载对象，通过这三个操作就能完成数据上传和下载。

以下章节介绍如何使用 OBS 管理控制台来完成图 2-1 中所示的任务。

图2-1 快速入门



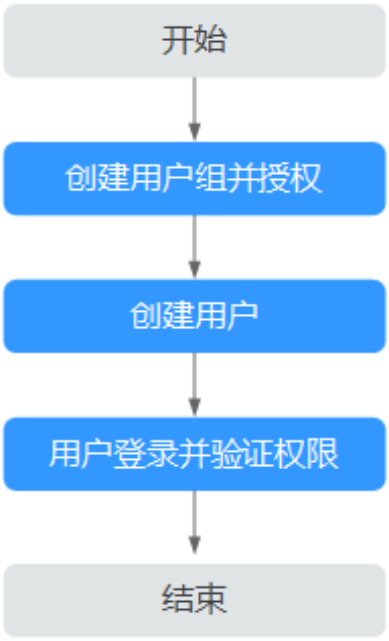
2.3.2 设置用户权限

若云服务帐号已经能满足您的要求，不需要创建独立的 IAM 用户，您可以跳过本章节，不影响您使用 OBS 的其它功能。

若您使用 IAM 用户，则需要先配置 IAM 用户的 OBS 资源权限。OBS 与其他云资源是分开部署的。

示例流程

图2-2 为 IAM 用户授权 OBS 资源权限



操作步骤

步骤 1 使用云服务帐号登录管理控制台。

步骤 2 在顶部导航栏选择“服务列表>管理与部署>统一身份认证服务”，进入“统一身份认证服务”管理控制台。

步骤 3 创建用户组并授予 OBS 资源权限。

用户组是用户的集合，IAM 通过用户组功能实现用户的授权。您在 IAM 中创建的用户，需要加入特定用户组后，用户才具备用户组所拥有的权限。

1. 在左侧导航栏单击“用户组”，进入“用户组”界面。
2. 单击“创建用户组”。
3. 在“创建用户组”界面，输入“用户组名称”和“描述”，单击“创建”。
   用户组创建完成，界面自动返回用户组列表，列表中显示新建的用户组。
4. 单击所创建的用户组右侧操作列的“权限配置”。
5. 在用户组详情页，选择“权限管理”页签，单击“配置权限”。
6. 作用范围选择“全局服务”，根据需求选中权限，单击“确定”。

步骤 4 创建用户操作详见创建 IAM 用户。

步骤 5 使用 IAM 用户登录 OBS 管理控制台，验证用户权限。

----结束

2.3.3 创建桶

您可以通过 OBS 管理控制台创建桶。桶是 OBS 中存储对象的容器。您需要先创建一个桶，然后才能在 OBS 中存储数据。

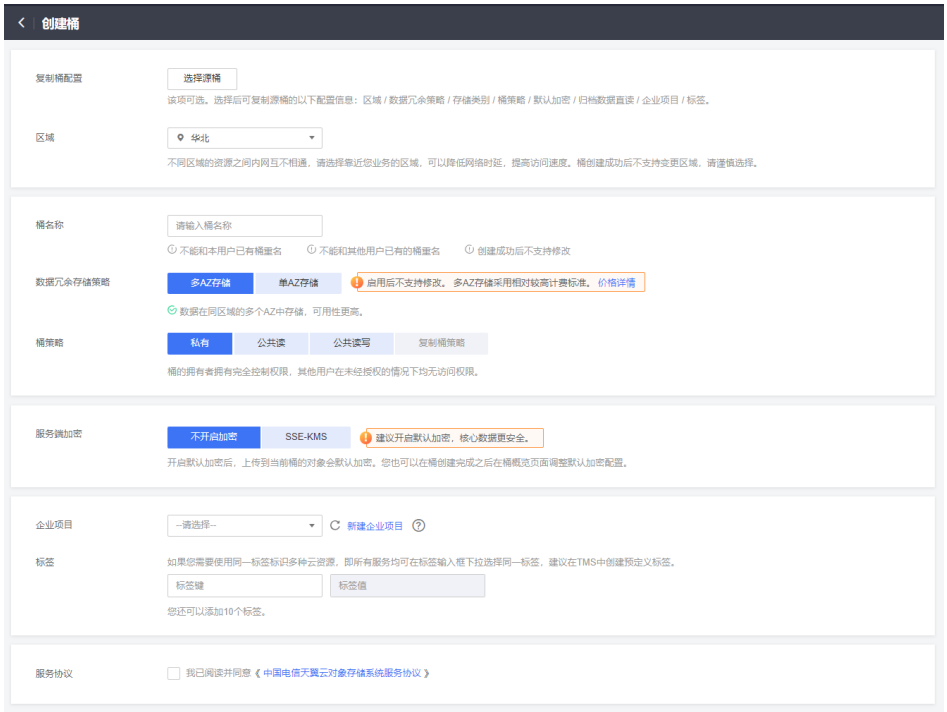
说明

一个帐号可创建的桶和并行文件系统的上限为 100 个。

操作步骤

步骤 1 在 OBS 管理控制台页面右上角单击“创建桶”，系统弹出如图 2-3 所示页面。

图2-3 创建桶



步骤 2 配置桶参数。

表2-3 桶参数说明

参数	描述
复制桶配置	可选。单击“选择源桶”后，可以在桶列表中选择一个源桶。返回后页面会自动复制源桶的以下配置信息：区域 / 数据冗余策略 / 桶策略 / 服务端加密 / 企业项目 / 标签。 选择后您仍可以根据业务情况对复制的配置信息进行部分或全部更改。
区域	桶所属区域。请选择靠近您业务的区域，以降低网络时延，提高访问速度。桶创建成功后，不支持变更区域，请谨慎选择。
桶名称	桶的名称。需全局唯一，不能与已有的任何桶名称重复，包括其他

参数	描述
	用户创建的桶。桶创建成功后，不支持修改名称，创建时，请设置合适的桶名。 OBS 中桶按照 DNS 规范进行命名，DNS 规范为全球通用规则，其具体命名规则如下： • 需全局唯一，不能与已有的任何桶名称重复，包括其他用户创建的桶。用户删除桶后，立即创建同名桶或并行文件系统会创建失败，需要等待 30 分钟才能创建。 • 长度范围为 3 到 63 个字符，支持小写字母、数字、中划线（-）、英文句号（.）。 • 禁止两个英文句号（.）相邻，禁止英文句号（.）和中划线（-）相邻，禁止以英文句号（.）和中划线（-）开头或结尾。 • 禁止使用 IP 地址。 **说明** 当用户使用虚拟主机方式通过 HTTPS 协议访问 OBS 时，如果桶名称中包含英文句号（.），会导致证书校验失败。所以该场景下，建议桶名称不要使用英文句号（.）。
数据冗余存储策略	• 多 AZ 存储：数据冗余存储至多个可用区（AZ），可靠性更高。 • 单 AZ 存储：数据仅存储在单个可用区（AZ），成本更低。 请根据业务情况提前规划数据冗余存储策略，桶一旦创建成功，数据冗余存储策略就确定了，后续无法更改。
桶策略	桶的读写权限控制。 • 私有：除桶 ACL 授权外的其他用户无桶的访问权限。 • 公共读：任何用户都可以对桶内对象进行读操作。 • 公共读写：任何用户都可以对桶内对象进行读/写/删除操作。
服务端加密	选择“SSE-KMS”加密。加密密钥类型您可以选择“默认密钥”，您上传的对象将使用当前区域的默认密钥进行加密，如果您没有默认密钥，系统将会在首次上传对象时自动为您创建，您也可以选择“自定义密钥”，通过单击“创建 KMS 密钥”进入数据加密服务页面创建自定义密钥，然后通过 KMS 密钥的下拉框选中您创建的 KMS 密钥。 若桶已开启了默认加密，上传对象可以继承桶的 KMS 加密特性。
企业项目	将桶加入到企业项目中统一管理。 请先在企业项目界面完成企业项目的创建，默认为 default 企业项目。 在企业项目界面创建企业项目，创建用户组并将用户加入到该用户组，然后将用户组添加到该企业项目。这时用户组内用户将获得用户组授权的该企业项目下的桶和对象的操作权限。 **说明** 仅企业帐号能够配置企业项目。

参数	描述
标签	可选。标签用于标识 OBS 中的桶，以此达到对 OBS 中的桶进行分类的目的。OBS 以键值对的形式来描述标签，每个标签有且只有一对键值。 有关添加标签的信息，请参见标签简介。

步骤 3 单击“立即创建”。

----结束

2.3.4 上传对象

您可以将本地文件直接通过 Internet 上传至 OBS 指定的位置。待上传的文件可以是任何类型：文本文件、图片、视频等。

说明

OBS 管理控制台单次最多支持 100 个文件同时上传，总大小不超过 5GB。

在未开启多版本控制功能的情况下，如果新上传的文件和桶内文件重名，则新上传的文件会自动覆盖老文件，且不会保留老文件的 ACL 等信息；如果新上传的文件夹和桶内文件夹重名，则上传后会将新老文件夹合并，合并过程如遇重名文件，会使用新上传的文件夹中的文件进行覆盖。

在开启了多版本控制功能的情况下，如果新上传的文件和桶内文件重名，则会在老文件上新增一个版本。关于多版本的详细介绍请参见多版本控制简介。

前提条件

- 至少已创建了一个桶。
- 若您需要将文件归类处理，可以先新建文件夹，然后将相关的文件上传到文件夹中。新建文件夹的步骤请参见新建文件夹。

操作步骤

步骤 1 在桶列表单击待操作的桶，进入“对象”页面。

步骤 2 进入待上传的文件夹，单击“上传对象”，系统弹出“上传对象”对话框。

说明

如果待上传至 OBS 的文件存放在 Microsoft OneDrive 中，建议这些待上传文件的名称不要超过 32 位，以保证兼容性。

步骤 3 拖拽本地文件或文件夹至“上传对象”区域框内添加待上传的文件。

也可以通过单击“上传对象”区域框内的“添加文件”，选择本地文件进行添加。

步骤 4 **服务端加密**：可以选择“不开启加密”或“SSE-KMS”。详情请参见使用服务端加密方式上传对象。

说明

如果桶配置了默认加密，上传对象时您可以选择“继承桶的加密配置”。

步骤 5 单击“上传”。

----结束

2.3.5 下载对象

您可以通过 OBS 管理控制台将存储在 OBS 中的文件下载至本地。

操作步骤

步骤 1 在桶列表单击待操作的桶，进入“对象”页面。

步骤 2 选中待下载的文件，并单击右侧的“下载”或“更多>下载为”，根据浏览器提示完成文件下载。

说明

在“下载为”对话框，右键单击“对象”，选择“复制链接地址”，可以获取到对象的下载链接地址。

----结束

2.3.6 删除对象

为节省空间和成本，您可以在 OBS 管理控制台上手动删除无用的文件。您可以删除单个文件，也可以批量删除多个文件。

操作步骤

步骤 1 在桶列表单击待操作的桶，进入“对象”页面。

步骤 2 选中待删除的文件，并单击右侧的“更多>删除”。

也可以选择多个文件，单击文件列表上方的“删除”删除多个文件。

步骤 3 单击“是”，确认删除文件。

删除对象任务在“任务中心”中显示。

----结束

使用建议

对于并行文件系统目录，大数据场景下（目录层级深、目录下文件多）的删除，可能会因超时而删除失败，建议使用：

- 给目录配置生命周期规则，通过生命周期后台删除。

2.3.7 删除桶

如果您不再需要一个桶，可以在 OBS 管理控制台上将其删除，以免占用桶数量配额。

前提条件

- 已彻底删除桶中对象。只有彻底删除对象后，才能删除桶。

须知

对象、碎片和已删除对象列表中对象都要删除。

- 只有桶的拥有者才能删除桶。

操作步骤

步骤 1 在 OBS 管理控制台桶列表中，选择待删除的桶，并单击右侧的“删除”。

说明

用户删除桶后，需要等待 30 分钟才能创建同名桶和并行文件系统。

步骤 2 单击“是”，确认删除桶。

----结束

2.4 桶管理

2.4.1 创建桶

您可以通过 OBS 管理控制台创建桶。桶是 OBS 中存储对象的容器。您需要先创建一个桶，然后才能在 OBS 中存储数据。

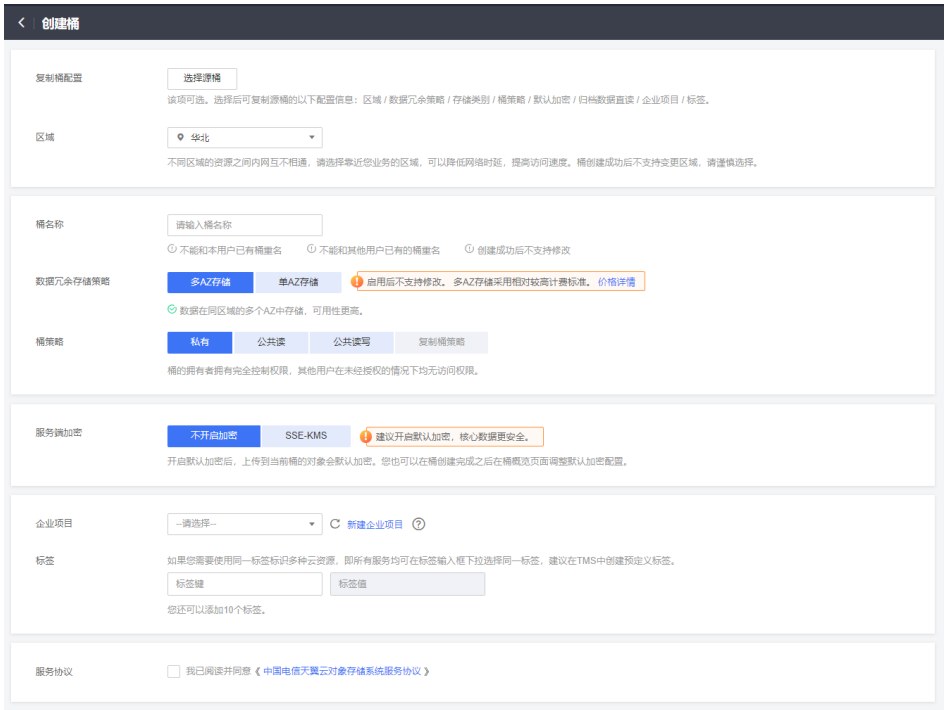
说明

一个帐号可创建的桶和并行文件系统的上限为 100 个。

操作步骤

步骤 1 在 OBS 管理控制台页面右上角单击“创建桶”，系统弹出如图 2-4 所示页面。

图2-4 创建桶



步骤 2 配置桶参数。

表2-4 桶参数说明

参数	描述
复制桶配置	可选。单击“选择源桶”后，可以在桶列表中选择一个源桶。返回后页面会自动复制源桶的以下配置信息：区域 / 数据冗余策略 / 桶策略 / 服务端加密 / 企业项目 / 标签。 选择后您仍可以根据业务情况对复制的配置信息进行部分或全部更改。
区域	桶所属区域。请选择靠近您业务的区域，以降低网络时延，提高访问速度。桶创建成功后，不支持变更区域，请谨慎选择。
桶名称	桶的名称。需全局唯一，不能与已有的任何桶名称重复，包括其他用户创建的桶。桶创建成功后，不支持修改名称，创建时，请设置合适的桶名。 OBS 中桶按照 DNS 规范进行命名，DNS 规范为全球通用规则，其具体命名规则如下： • 需全局唯一，不能与已有的任何桶名称重复，包括其他用户创建的桶。用户删除桶后，立即创建同名桶或并行文件系统会创建失败，需要等待 30 分钟才能创建。 • 长度范围为 3 到 63 个字符，支持小写字母、数字、中划线（-）、英文句号（.）。 • 禁止两个英文句号（.）相邻，禁止英文句号（.）和中划线（-）相邻，禁止以英文句号（.）和中划线（-）开头或结尾。

参数	描述
	• 禁止使用 IP 地址。 **说明** 当用户使用虚拟主机方式通过 HTTPS 协议访问 OBS 时，如果桶名称中包含英文句号（.），会导致证书校验失败。所以该场景下，建议桶名称不要使用英文句号（.）。
数据冗余存储策略	• 多 AZ 存储：数据冗余存储至多个可用区（AZ），可靠性更高。 • 单 AZ 存储：数据仅存储在单个可用区（AZ），成本更低。 请根据业务情况提前规划数据冗余存储策略，桶一旦创建成功，数据冗余存储策略就确定了，后续无法更改。
桶策略	桶的读写权限控制。 • 私有：除桶 ACL 授权外的其他用户无桶的访问权限。 • 公共读：任何用户都可以对桶内对象进行读操作。 • 公共读写：任何用户都可以对桶内对象进行读/写/删除操作。
服务端加密	选择“SSE-KMS”加密。加密密钥类型您可以选择“默认密钥”，您上传的对象将使用当前区域的默认密钥进行加密，如果您没有默认密钥，系统将会在首次上传对象时自动为您创建，您也可以选择“自定义密钥”，通过单击“创建 KMS 密钥”进入数据加密服务页面创建自定义密钥，然后通过 KMS 密钥的下拉框选中您创建的 KMS 密钥。 若桶已开启了默认加密，上传对象可以继承桶的 KMS 加密特性。
企业项目	将桶加入到企业项目中统一管理。 请先在企业项目界面完成企业项目的创建，默认为 default 企业项目。 在企业项目界面创建企业项目，创建用户组并将用户加入到该用户组，然后将用户组添加到该企业项目。这时用户组内用户将获得用户组授权的该企业项目下的桶和对象的操作权限。 **说明** 仅企业帐号能够配置企业项目。
标签	可选。标签用于标识 OBS 中的桶，以此达到对 OBS 中的桶进行分类的目的。OBS 以键值对的形式来描述标签，每个标签有且只有一对键值。 有关添加标签的信息，请参见标签简介。

步骤 3 单击“立即创建”。

----结束

2.4.2 查看桶的信息

您可以通过 OBS 管理控制台直接查看某个桶的详情。

操作步骤

步骤 1 在桶列表单击待操作的桶，进入“对象”页面。

步骤 2 在左侧导航栏，单击“概览”进入“概览”页面。

步骤 3 在“基本信息”下查看桶的基本信息，如图 2-5 所示。

图2-5 桶的基本信息

表2-5 桶信息参数说明

参数	说明
桶名称	桶的名称。
桶版本号	桶的版本号。
区域	桶所在的区域。
存储用量	桶中存储的对象占用的存储空间，为桶中最新版本对象和所有历史版本对象的容量总和。
对象数量	桶中存储的对象数量，为桶内文件夹、最新版本对象和所有历史版本的对象总和。
帐号 ID	桶的拥有者全局唯一标识，与“我的凭证”页面的“Domain ID”相同。
创建时间	桶的创建时间。
多版本控制	多版本控制的状态。
Endpoint	桶所在区域的终端节点。OBS 为每个区域提供一个终端节点，终端节点可以理解为 OBS 在不同区域的区域域名，用于处理各自区域的访问请求。
访问域名	OBS 会为每一个桶分配默认的访问域名。访问域名是桶在互联网中的域名地址，可应用于直接通过域名访问桶的场景，比如：云应用开发、数据分享等。 格式：*BucketName.Endpoint*
数据冗余存储策略	桶的数据冗余存储策略，包括多 AZ 存储和单 AZ 存储。数据冗余存储策略无法修改。
企业项目	桶所属的企业项目。

说明

“存储用量”和“对象数量”非实时数据，系统更新存在至少 15 分钟的延迟。

----结束

2.4.3 搜索桶

OBS 管理控制台支持按桶名称、区域、数据冗余存储策略和企业项目搜索桶。

操作步骤

步骤 1 在 OBS 管理控制台桶列表上方上方 搜索框中输入需要查找查找的桶。

步骤 2 单击 。

搜索到的桶会显示在桶列表中。

例如：您需要查找桶名中包含“test”字符的所有桶，您只需在主页面右上角的搜索框中输入“test”并单击  ，所有包含“test”字符的桶都会展示到桶列表中。

----结束

相关操作

桶列表支持按照“桶名称”、“区域”、“数据冗余存储策略”、“存储用量”、“对象数量”、“企业项目”和“创建时间”进行排序，您可以单击参数后的  按钮进行排序。

2.4.4 删除桶

如果您不再需要一个桶，可以在 OBS 管理控制台上将其删除，以免占用桶数量配额。

前提条件

- 已彻底删除桶中对象。只有彻底删除对象后，才能删除桶。

须知

对象、碎片和已删除对象列表中对象都要删除。

- 只有桶的拥有者才能删除桶。

操作步骤

步骤 1 在 OBS 管理控制台桶列表中，选择待删除的桶，并单击右侧的“删除”。

说明

用户删除桶后，需要等待 30 分钟才能创建同名桶和并行文件系统。

步骤 2 单击“是”，确认删除桶。

----结束

2.5 对象管理

2.5.1 新建文件夹

您可以通过 OBS 管理控制台在已创建的桶中新建一个文件夹，从而更方便的对存储在 OBS 中的数据进行管理。

背景知识

- 由于 OBS 是一种对象存储服务，并没有文件系统中的文件和文件夹概念。为了使用户更方便进行管理数据，OBS 提供了一种方式模拟文件夹。实际上在 OBS 内部

是通过在对象的名称中增加“/”，将该对象在 OBS 管理控制台上模拟成一个文件夹的形式展现。通过 API 列举对象，获取到的对象名就是以“/”分隔的，最后一个“/”后的内容就是对象名。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对象的性能。

- 文件夹不支持通过管理控制台进行下载，您可以使用 OBS Browser+来下载文件夹。

操作步骤

步骤 1 在桶列表单击待操作的桶，进入“对象”页面。

步骤 2 单击“新建文件夹”，或者单击进入目标文件夹后，再单击“新建文件夹”。

步骤 3 在“文件夹名称”中输入新文件夹名称。

- 支持创建单个文件夹和多层级的文件夹。
- 文件夹名称不能包含以下字符 ：**\:*?"<>|**+。
- 文件夹名称不能以英文句号（.）或斜杠（/）开头或结尾。
- 文件夹的绝对路径总长度不能超过 1023 字符。
- 任何单个斜杠（/）表示分隔并创建多层级的文件夹。
- 不能包含两个以上相邻的斜杠（/）。

步骤 4 单击“确定”。

----结束

后续操作

您可以单击文件夹后面的“复制路径”，复制文件夹的路径。您可以将获取到路径共享给其他用户，其他用户可以找到存储对象的桶后，在搜索对象框中输入该路径值即可获取到对象。

2.5.2 上传对象

您可以将本地文件直接通过 Internet 上传至 OBS 指定的位置。待上传的文件可以是任何类型：文本文件、图片、视频等。

约束与限制

- OBS 管理控制台单次最多支持 100 个文件同时上传，总大小不超过 5GB。
- OBS 管理控制台支持批量上传多个文件，单次最多支持 100 个文件同时上传，总大小不超过 5GB。超过 5GB 的文件，请使用 OBS API 的多段上传接口上传。
- 在未开启多版本控制功能的情况下，如果新上传的文件和桶内文件重名，则新上传的文件会自动覆盖老文件，且不会保留老文件的 ACL 等信息；如果新上传的文件夹和桶内文件夹重名，则上传后会将新老文件夹合并，合并过程如遇重名文件，会使用新上传的文件夹中的文件进行覆盖。
- 在开启了多版本控制功能的情况下，如果新上传的文件和桶内文件重名，则会在老文件上新增一个版本。关于多版本的详细介绍请参见多版本控制简介。

前提条件

- 至少已创建了一个桶。
- 若您需要将文件归类处理，可以先新建文件夹，然后将相关的文件上传到文件夹中。新建文件夹的步骤请参见新建文件夹。

操作步骤

步骤 1 在桶列表单击待操作的桶，进入“对象”页面。

步骤 2 进入待上传的文件夹，单击“上传对象”，系统弹出“上传对象”对话框。

说明

如果待上传至 OBS 的文件存放在 Microsoft OneDrive 中，建议这些待上传文件的名称不要超过 32 位，以保证兼容性。

步骤 3 拖拽本地文件或文件夹至“上传对象”区域框内添加待上传的文件。

也可以通过单击“上传对象”区域框内的“添加文件”，选择本地文件进行添加。

步骤 4 **服务端加密**：可以选择“不开启加密”或“SSE-KMS”。详情请参见使用服务端加密方式上传对象。

说明

如果桶配置了默认加密，上传对象时您可以选择“继承桶的加密配置”。

步骤 5 单击“上传”。

----结束

后续操作

您可以单击对象后面的“复制路径”，复制对象的路径。

您可以将获取到路径共享给其他用户，其他用户可以找到存储对象的桶后，在搜索对象框中输入该路径值即可获取到对象。

2.5.3 下载对象

您可以通过 OBS 管理控制台将存储在 OBS 中的文件下载至本地。下载文件可选择下载至浏览器自带的下载路径，或下载至本地指定的位置。

操作步骤

步骤 1 在桶列表单击待操作的桶，进入“对象”页面。

步骤 2 选中待下载的文件，并单击右侧的“下载”或“更多>下载为”，根据浏览器提示完成文件下载。

说明

在“下载为”对话框，右键单击“对象”，选择“复制链接地址”，可以获取到对象的下载链接地址。

----结束

2.5.4 分享对象

操作场景

您可以使用对象分享功能，通过对象的临时 URL 将存放在 OBS 中的对象分享给所有用户。

背景知识

文件分享强调临时性，所有分享的 URL 都是临时 URL，存在有效期。

临时 URL 是由文件的访问域名和临时鉴权信息组成。

临时鉴权信息主要包含 **AccessKeyId**、**Expires**、**x-obs-security-token** 和 **Signature** 四个参数。其中 **AccessKeyId**、**x-obs-security-token** 和 **Signature** 用于鉴权，**Expires** 定义鉴权的有效期。

当在 OBS 控制台上单击了对象后的“分享”之后，OBS 就会以默认 5 分钟的有效期获取临时鉴权信息，并生成分享链接，此时链接就已经生效并且开始计算时间了。每调整一次 URL 有效期，OBS 就会重新获取一次鉴权信息以生成新的分享链接，新链接的有效期从调整的时候开始计算。

约束与限制

- 通过 OBS 控制台分享的文件，有效期的范围为 1 分钟到 18 小时。如果想要设置更长的有效期，建议使用客户端工具 OBS Browser+，OBS Browser+支持 1 分钟到 30 天的有效期。如果想要设置永久的权限，请通过桶策略或对象策略实现。
- 仅桶版本号为 3.0 的桶支持文件分享功能。桶版本号可以在桶概览页的“基本信息”中查看。
- 加密对象不能分享。

操作步骤

步骤 1 在桶列表单击待操作的桶，进入“对象”页面。

步骤 2 选中待分享的文件，并单击右侧的“分享”。

此时，链接信息中的链接就已经生效并开始计时，有效期为默认的 5 分钟。修改 URL 有效期，链接会相应变化，新链接的有效期从修改时开始计算。

图2-6 分享文件

步骤 3 URL 相关操作。

- 单击“打开 URL”，将在新页面打开文件进行预览或者直接下载文件到本地。
- 单击“复制链接”，您可以将该链接分享给所有用户，用户可以在浏览器中通过此链接直接访问文件。
- 单击“复制路径”，您可将该路径分享给所有拥有对象所在桶权限的用户，用户可以在对应桶中的文件搜索框中输入该路径搜索并访问文件。

说明

在“URL 有效期”内，任何用户都可以访问该文件。

----结束

2.5.5 搜索对象或文件夹

OBS 管理控制台支持按前缀搜索文件或文件夹。

按前缀搜索

步骤 1 在桶列表单击待操作的桶，进入“对象”页面。

步骤 2 在对象列表右上方的搜索框中输入需要查找的文件或文件夹的前缀。

搜索结果为根目录级别下的前缀为搜索内容的文件和文件夹。

说明

如果要在某个文件夹中进行搜索，您可以使用以下两种方式，搜索结果显示该文件夹下前缀为搜索内容的文件和文件夹。

- 根目录下，在搜索框中输入“文件夹路径/前缀”进行搜索。例如，搜索“abc/123/example”，搜索结果显示为“abc/123”文件夹下前缀为“example”的所有文件和文件夹。
- 进入该文件夹后，在搜索框中输入要搜索的前缀内容进行搜索。例如，进入“abc/123”文件夹后，搜索“example”，搜索结果显示为“abc/123”文件夹下前缀为“example”的所有文件和文件夹。

步骤 3 单击 ，搜索结果在对象列表中显示。

----结束

相关操作

对象列表支持按照“大小”和“最后修改时间”进行排序，您可以单击参数后的 按钮进行排序。

2.5.6 通过对象 URL 访问对象

将对象权限设置为匿名用户读取权限，通过分享对象 URL，匿名用户通过分享的链接地址可访问对象数据。

前提条件

已经设置匿名用户对该对象的读取权限。权限开启方法请参见为匿名用户设置对象的访问权限。

说明

不能对已加密的对象进行共享。

操作步骤

步骤 1 在桶列表单击待操作的桶，进入“对象”页面。

步骤 2 单击待共享对象，在网页上方显示对象的信息。“链接”显示该对象的共享链接地址。

匿名用户单击该链接地址即可通过浏览器访问该对象。对象链接地址格式为：https://*桶名.域名/文件夹目录层级/对象名*。如果该对象存在于桶的根目录下，其链接地址将不会有文件夹目录层级。

----结束

2.5.7 删除对象或文件夹

操作场景

为节省空间和成本，您可以通过 OBS 管理控制台删除无用的文件或文件夹。

本小节主要介绍如何在 OBS 管理控制台上手动删除文件或文件夹。

除此之外，OBS 还提供了生命周期管理功能，来满足您定期自动删除桶中文件或者一次性清空桶中所有文件和文件夹的诉求。详情请参见配置生命周期规则。

对于并行文件系统目录，大数据场景下（目录层级深、目录下文件多）的删除，可能会因超时而删除失败，建议使用：

1. hadoop 客户端（嵌套 OBS 客户端插件 OBSA）删除目录：hadoop fs - rmr obs://{并行文件系统名}/{目录名}。
2. 给目录配置生命周期规则，通过生命周期后台删除。

背景知识

多版本控制功能启用时的对象删除机制

桶的多版本控制功能启用时，删除的目标不同，OBS 会采取不同的处理方式：

- 删除文件或文件夹：文件或文件夹不会立即被彻底删除，而是保留在“已删除对象”列表中，同时会为文件打上删除标记。在“已删除对象”列表中单击对象名，在对象的“版本”页签下可以看到最新的对象版本有删除标记。
  - 如果想要彻底删除，需要再到“已删除对象”列表进行删除。删除方法请参见本小节的操作步骤。
  - 如果想要找回删除的文件，可以通过“取消删除”功能来找回。找回方法请参见取消删除对象。
- 删除文件的某个版本：该版本会被彻底删除且无法恢复。如果删除的是文件的最新版本，那么时间最近的那个历史版本将会变成最新版本。

操作步骤

步骤 1 在桶列表单击待操作的桶，进入“对象”页面。

步骤 2 选中待删除的文件或文件夹，并单击右侧的“更多 > 删除”。

也可以选中多个文件或文件夹，单击文件列表上方的“删除”进行批量删除。

步骤 3 单击“是”，确认删除文件或文件夹。

步骤 4 对于启用了多版本控制的 OBS 桶，想要彻底删除文件或文件夹，需要再到“已删除对象”列表进行删除。

1. 单击“已删除对象”。
2. 在待删除的文件或文件夹所在行的操作列，单击“彻底删除”。

   也可以选中多个文件或文件夹，单击文件列表上方的“彻底删除”进行批量删除。

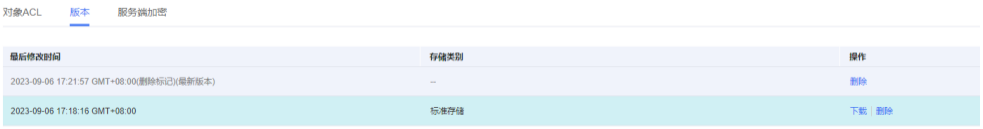
图2-7 彻底删除文件或文件夹

----结束

相关操作

在多版本控制功能启用的场景下，在“已删除对象”中的文件仍然会保留多版本，在对不同的版本进行删除时需要注意：

图2-8 “已删除对象”中文件的版本列表



- 如果删除的是带“删除标记”的版本，实际上是找回该文件，等同于“取消删除”文件，而非彻底删除。相关方法请参见取消删除对象的相关操作。
- 如果删除的是不带“删除标记”的版本，则会彻底删除该历史版本，即使后续该文件找回后，也无法恢复这个被彻底删除的历史版本。

2.5.8 取消删除对象

操作场景

在启用了多版本控制功能的 OBS 桶中，如果想将删除的文件找回，可以通过“取消删除”功能来实现。

背景知识

多版本控制功能启用时的对象删除机制

桶的多版本控制功能启用时，删除的目标不同，OBS 会采取不同的处理方式：

- 删除文件或文件夹：文件或文件夹不会立即被彻底删除，而是保留在“已删除对象”列表中，同时会为文件打上删除标记。
  - 如果想要彻底删除，需要再到“已删除对象”列表进行删除。删除方法请参见删除对象或文件夹。
  - 如果想要找回删除的文件，可以通过“取消删除”功能来找回。找回方法请参见本小节的操作步骤。

- 删除文件的某个版本：该版本会被彻底删除且无法恢复。如果删除的是文件的最新版本，那么时间最近的那个历史版本将会变成最新版本。

多版本控制功能启用时的对象找回机制

启用了多版本控制功能的 OBS 桶中的文件从“对象”列表删除后，OBS 不会立即将其彻底删除，而是保留在“已删除对象”中，同时会为其打上删除标记。您可以通过“取消删除”功能来找回被删除的文件。

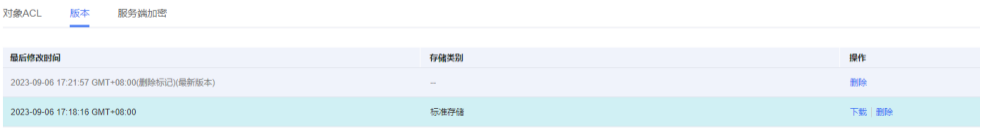
使用“取消删除”功能需要注意以下几点：

1. 只支持对文件“取消删除”，不支持对文件夹“取消删除”。

   “取消删除”文件后，该文件会恢复到“对象”列表中，此时可以正常使用对象的基本功能。如果文件存放于某个文件夹下，“取消删除”文件后依然会保留原有的目录结构。

2. “已删除对象”中的文件仍然会保留多版本，在对不同的版本进行删除时需要注意：
   - 如果删除的是带“删除标记”的版本，实际上是找回该文件，等同于“取消删除”文件，而非彻底删除。具体步骤请参见相关操作。
   - 如果删除的是不带“删除标记”的版本，则会彻底删除该历史版本。即使后续该文件找回后，也无法恢复这个被彻底删除的历史版本。

   图2-9 “已删除对象”中文件的版本列表

3. “已删除对象”中的文件至少需要保留一个不带“删除标记”的历史版本，否则无法执行“取消删除”操作。

前提条件

- OBS 桶的多版本控制功能已启用。启用方法请参见配置多版本控制。
- 待找回的文件在“已删除对象”列表中，未被彻底删除，且至少保留一个不带“删除标记”的历史版本。

操作步骤

步骤 1 在桶列表单击待操作的桶，进入“对象”页面。

步骤 2 单击“已删除对象”。

步骤 3 在要找回的已删除文件所在行，单击右侧的“取消删除”。

也可以选中多个文件，单击文件列表上方的“取消删除”进行批量找回。

----结束

相关操作

通过删除带“删除标记”的版本来找回文件的方法：

步骤 1 在桶列表单击待操作的桶，进入“对象”页面。

步骤 2 单击“已删除对象”。

步骤 3 单击要找回的文件名称，系统显示该文件信息。

步骤 4 在“版本”页签，显示该文件的所有版本。

- 删除带“删除标记”的版本，将找回该文件，恢复到“对象”列表中。
- 删除不带“删除标记”的历史版本，将彻底删除该历史版本。

----结束

2.5.9 清理碎片

背景知识

OBS 采用分段上传的模式上传数据，在下列情况下（但不仅限于此）通常会导致数据上传失败而产生碎片。

- 网络条件较差，与 OBS 的服务器之间的连接经常断开。
- 上传过程中，人为中断上传任务。
- 设备故障。
- 突然断电等特殊情况。

上传失败而产生的碎片会存储在 OBS 中，需手动清理碎片。文件上传失败后，需重新上传。

须知

OBS 中的碎片会占用存储空间，会按照存储空间计费项进行计费。

操作步骤

步骤 1 在桶列表单击待操作的桶，进入“对象”页面。

步骤 2 单击“碎片”，选中需要清理的碎片，单击右侧的“删除”。

也可选中多个碎片，单击对象列表上方的“删除”进行批量删除。

步骤 3 单击“是”，确认删除碎片。

----结束

2.6 服务端加密

2.6.1 服务端加密简介

当启用服务端加密功能后，用户上传对象时，数据会在服务端加密成密文后存储。用户下载加密对象时，存储的密文会先在服务端解密为明文，再提供给用户。

KMS 通过使用硬件安全模块 (HSM) 保护密钥安全的托管，帮助用户轻松创建和控制加密密钥。用户密钥不会明文出现在 HSM 之外，避免密钥泄露。对密钥的所有操作都会进行访问控制及日志跟踪，提供所有密钥的使用记录，满足监督和合规性要求。

需要上传的对象可以通过数据加密服务器提供密钥的方式进行服务端加密。用户首先需要在 KMS 中创建密钥（或者使用 KMS 提供的默认密钥），当用户在 OBS 中上传对象时使用该密钥进行服务端加密。

OBS 支持通过接口提供 KMS 托管密钥的服务端加密(SSE-KMS)，采用行业标准的 AES256 加密算法。

2.6.2 桶默认加密

OBS 支持将桶配置为默认加密，配置后，上传到桶中的对象都会自动使用指定的 KMS 密钥进行加密，提高数据存储安全。

您可以在创建桶时选择开启桶默认加密，详情请见创建桶；也可以在已创建的桶中根据需要开启或关闭桶默认加密。

OBS 仅会对开启桶默认加密之后上传的对象进行加密，不会改变开启前已有对象的加密状态。关闭默认加密，也不会影响桶中已有对象的加密状态，关闭默认加密后可在上传对象时进行单独加密。

开启桶默认加密

步骤 1 在桶列表单击待操作的桶，进入“对象”页面。

步骤 2 在左侧导航栏，单击“概览”进入“概览”页面。

步骤 3 在“基础配置”区域下，单击“默认加密”卡片，系统弹出“默认加密”对话框。

步骤 4 选择“SSE-KMS”。

开启“SSE-KMS”加密后，您可以选择“默认密钥”，您上传的对象将使用当前区域的默认密钥进行加密，如果您没有默认密钥，系统将会在首次上传对象时自动为您创建。您也可以选择“自定义密钥”，通过单击“创建 KMS 密钥”进入数据加密服务页面创建自定义密钥，然后通过 KMS 密钥的下拉框选中您创建的 KMS 密钥。

步骤 5 单击“确定”。

----结束

关闭桶默认加密

步骤 1 在桶列表单击待操作的桶，进入“对象”页面。

步骤 2 在左侧导航栏，单击“概览”进入“概览”页面。

步骤 3 在“基础配置”区域下，单击“默认加密”卡片，系统弹出“默认加密”对话框。

步骤 4 选择“不开启加密”。

步骤 5 单击“确定”。

----结束

2.6.3 使用服务端加密方式上传对象

用户可根据需要对对象进行服务端加密，使对象更安全的存储在 OBS 中。

如果文件要上传的桶未开启默认加密，上传时默认不加密，您可自行配置服务端加密上传文件。如果文件要上传的桶已开启默认加密，上传时可继承桶的加密配置，也可自行配置服务端加密上传。

约束与限制

- 对象的加密状态不可以修改。
- 使用中的密钥不可以删除，如果删除将导致加密对象不能下载。

前提条件

已通过 IAM 服务添加 OBS 所在区域的 **KMS Administrator** 权限。权限添加方法请参见《统一身份认证服务用户指南》。

操作步骤

步骤 1 在桶列表单击待操作的桶，进入“对象”页面。

步骤 2 单击“上传对象”，系统弹出“上传对象”对话框。

步骤 3 添加待上传的文件。

步骤 4 选择“SSE-KMS”，您可以选择“默认密钥”，您上传的对象将使用当前区域的默认密钥进行加密，如果您没有默认密钥，系统将会在首次上传对象时自动为您创建。您也可以选择“自定义密钥”，通过单击“创建 KMS 密钥”进入数据加密服务页面创建自定义密钥，然后通过 KMS 密钥的下拉框选中您创建的 KMS 密钥。

说明

如果桶开启了默认加密，上传对象时您可以选择“继承桶的加密配置”。

图2-10 加密上传对象

步骤 5 单击“上传”。

对象上传成功后，可在对象列表中查看对象的加密状态。

----结束

2.7 对象元数据

2.7.1 对象元数据简介

元数据（Metadata）为描述对象属性的信息，是一组名称和值的配对，用作对象管理的一部分。

当前仅支持系统定义的元数据。

系统定义的元数据又分为两种类别：系统控制和用户控制。如 Last-Modified 日期等数据由系统控制，不可修改；如为对象配置的 ContentLanguage，用户可以通过接口进行修改。用户可控制修改的元数据描述如下：

表2-6 OBS 的元数据

名称	说明
ContentDisposition	为请求的对象提供一个默认的文件名赋值给该对象，当下载对象或者访问对象时，以默认文件名命名的文

名称	说明
	件将直接在浏览器上显示或在访问时弹出文件下载对话框。 例如：元数据名称选择为“ContentDisposition”，元数据值填写为“attachment;filename="testfile.xls"”，当通过链接访问设置了该元数据的对象时，会直接弹出一个对象下载的对话框，且对象名称会被修改为“testfile.xls”。详情请参见 HTTP 协议中关于 ContentDisposition 的定义。
ContentLanguage	说明访问者希望采用的语言或语言组合，以根据自己偏好的语言来定制。详情请参见 HTTP 协议中关于 ContentLanguage 的定义。
WebsiteRedirectLocation	为对象提供重定向功能，重定向到其他对象或者外部的 URL。重定向功能通过静态网站托管实现。 例如，可根据如下步骤实现对象重定向功能。 1. 为桶“testbucket”根目录下的对象“testobject.html”设置元数据，元数据名称选择为“WebsiteRedirectLocation”，元数据值填写为“http://www.example.com” 说明 OBS 仅支持为桶根目录下的对象设置重定向，不支持为桶中文件夹下的对象设置重定向。 2. 在桶“testbucket”中配置静态网站托管，将该桶中的对象“testobject.html”设置为静态网站托管的“默认首页”。 3. 当通过静态网站托管页面上的“访问地址”访问对象“testobject.html”时，会直接重定向访问 http://www.example.com。
ContentEncoding	指定对象被下载时的内容编码格式，可以设置如下类型： • 标准定义：compress、deflate、exi、identity、gzip、pack200-gzip • 其他：br、bzip2、lzma 、peerdist、sdch、xpress、xz
ContentType	设置对象的文件类型。详见对象元数据 Content-Type 介绍。

说明

- 当桶开启多版本控制时，最新版本的对象支持设置元数据，历史版本的对象不支持设置元数据。

2.7.2 配置对象元数据

操作步骤

步骤 1 在桶列表单击待操作的桶，进入“对象”页面。

步骤 2 单击待操作的对象，然后再单击“元数据”。

步骤 3 单击“增加”，如图 2-11 所示。根据需要填写元数据信息。

图2-11 增加元数据

步骤 4 单击“确定”。

----结束

2.8 桶清单

2.8.1 桶清单简介

桶清单功能可以定期生成桶内对象的元数据信息，通过查看这些信息，可以帮助您更好地了解桶内对象的状态。

生成的桶清单为 CSV 格式的文件，您可以规定桶清单在生成后自动上传到指定桶中。

您可以通过对象前缀过滤需要生成清单的对象，指定清单的生成周期（每天或每周），选择是否列出对象的所有版本。同时您还可以根据实际业务需要，指定清单中要包含的对象元数据内容，包括文件大小、上次修改时间、ETag、分段上传、复制状态、加密状态等。

约束与限制

- 一个桶最多支持 10 条桶清单。
- 桶清单配置的源桶和目标桶必须归属同一个帐号。
- 桶清单配置的源桶和目标桶必须归属同一个区域。
- 只支持生成 CSV 格式的清单文件。
- 桶清单筛选条件目前仅支持设置为所有对象或指定前缀的对象。
- 同一个桶中多条清单规则的筛选条件不能彼此包含：
  - 如果已经存在针对桶中所有对象的规则，则无法再创建按对象名前缀筛选的规则。如需创建，要先删除针对所有对象的规则。
  - 如果已经存在按对象名前缀筛选的规则，则无法再创建针对桶中所有对象的规则。如需创建，要先删除所有按对象名前缀筛选的规则。
  - 如果已经存在某个按对象名前缀筛选的规则（如前缀 ab），则无法再创建与其存在包含或被包含关系的规则（如前缀 a 或前缀 abc）。如需创建，要先删除存在包含或被包含关系的规则。
- 桶清单加密方式目前只支持 SSE-KMS。

桶清单中配置的目标桶不能开启桶默认加密

2.8.2 配置桶清单

操作步骤

步骤 1 在桶列表单击待操作的桶，进入“对象”页面。

步骤 2 在左侧导航栏，单击“桶清单”进入“桶清单”页面。

步骤 3 单击“创建”，系统弹出“创建桶清单”对话框。

图2-12 清单配置

步骤 4 设置“清单配置”相关参数。

表2-7 清单配置参数说明

参数	描述
清单名称	桶清单的名称。
筛选条件	桶清单筛选条件，OBS 会为筛选出来的对象生成清单。 目前仅支持通过对象名前缀进行筛选；或者不输入，表示对桶中所有对象生成清单。 同一个桶中多条清单规则的筛选条件不能彼此包含。
清单存储桶	存储桶清单文件的桶，只能选择与源桶相同区域的桶。
清单文件前缀	清单文件的存储路径前缀。 清单文件生成后，将存储至清单存储桶的以下路径：清单文件前缀/源桶名/清单名称/日期时间/files/ 如不配置此参数，上述路径的一级目录“清单文件前缀”将由系统自动生成并命名为“BucketInventory”。
生成频率	设定桶清单的生成频率：每天或每周。
清单状态	开启，表示按照相关设置生成桶清单；关闭，表示不生成桶清单。

步骤 5 单击“下一步”，进入“报表配置”页面。

步骤 6 设置“报表格式”相关参数。

表2-8 报表格式参数说明

参数	描述
清单格式	支持生成 CSV 格式的桶清单文件。
对象版本	报表中对象的版本，可以设置为“仅限当前版本”和“包含所有版本”。
清单额外字段	桶清单文件中包含的对象信息：文件大小、上次修改时间、ETag、分段上传、复制状态、加密状态。

步骤 7 单击“下一步”，确认桶策略。

OBS 将在桶清单存储桶上创建桶策略，以允许其将清单文件存入该桶。

步骤 8 单击“确定”。

----结束

相关操作

桶清单列表页支持导出桶清单操作。

步骤 1 在桶列表单击待操作的桶，进入“对象”页面。

步骤 2 在左侧导航栏，单击“桶清单”，进入桶清单列表页面。

步骤 3 单击右上角的  。

步骤 4 浏览器会自动下载桶清单 Excel 表。

----结束

2.9 权限控制

2.9.1 概述

OBS 支持通过以下方式进行权限控制：

- IAM 策略：IAM 策略是作用于云资源的，IAM 策略定义了允许和拒绝的访问操作，以此实现云资源权限访问控制。
- 桶策略和对象策略：

  桶策略是作用于所配置的 OBS 桶及桶内对象的。OBS 桶拥有者通过桶策略可为 IAM 用户或其他帐号授权桶及桶内对象的操作权限。

  对象策略是桶策略中针对对象的策略。
- ACL：OBS ACL 是基于帐号级别的读写权限控制，提供桶和对象的 ACL 配置。

2.9.2 权限控制方式介绍

2.9.2.1 IAM 策略

通过 IAM，您可以在云帐号中创建 IAM 用户，并使用策略来控制 IAM 用户对云资源的访问范围。

IAM 策略是作用于云资源的，IAM 策略定义了允许和拒绝的访问操作，以此实现云资源权限访问控制。

对于 OBS，IAM 策略的 OBS 权限是作用于 OBS 所有的桶和对象的。如果要授予 IAM 用户操作 OBS 资源的权限，则需要向用户所属的用户组授予一个或多个 OBS 权限集。

IAM 策略的 OBS 权限详情请参见权限管理。

IAM 策略应用场景

IAM 策略主要面向对同帐号下 IAM 用户授权的场景：

- 使用策略控制帐号下整个云资源的权限时，使用 IAM 策略授权。

- 使用策略控制帐号下 OBS 所有的桶和对象的权限时，使用 IAM 策略授权。

策略结构&语法

策略结构包括：Version（策略版本号）和 Statement（策略权限语句），其中 Statement 可以有多个，表示不同的授权项。

图2-13 策略结构

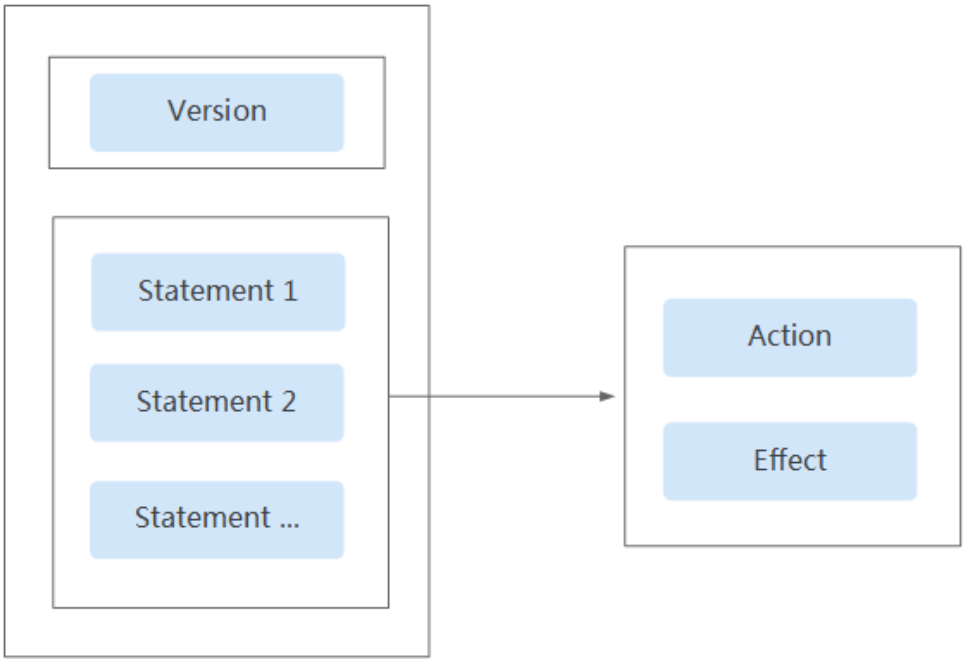


表2-9 策略语法参数

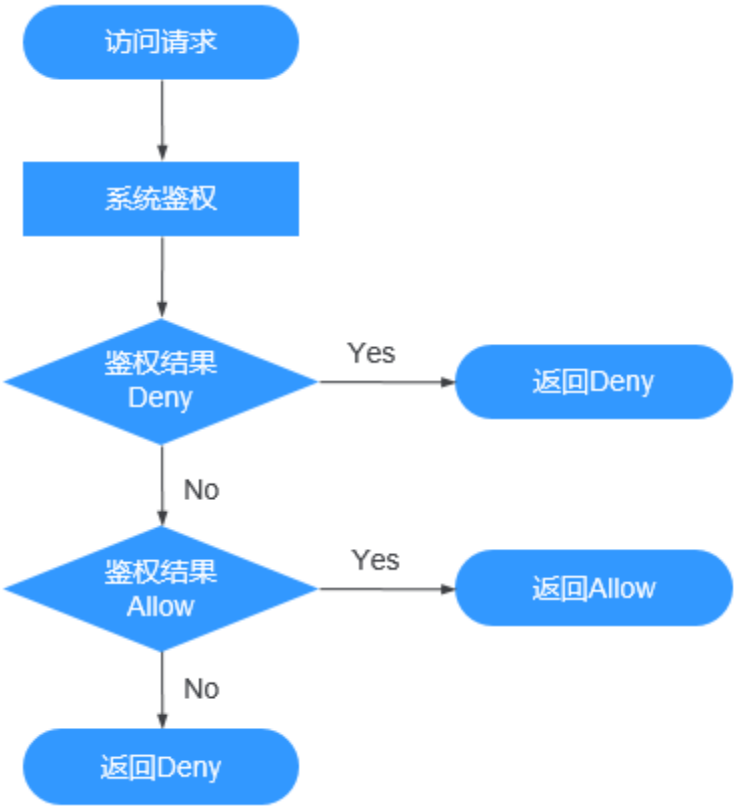
参数	说明
Version	标识策略的版本号： • 1.0：RBAC 策略。RBAC 策略是将服务作为一个整体进行授权，授权后，用户可以拥有这个服务的所有权限。
Statement	策略授权语句，描述策略的详细信息，包含 Effect（作用）和 Action（授权项）。 • Effect（作用） 作用包含两种：Allow（允许）和 Deny（拒绝），系统预置策略仅包含允许的授权语句。 • Action（授权项） 对资源的具体操作权限，支持单个或多个操作权限，支持通配符号*，通配符号表示所有。 • Resource（资源） 策略所作用的资源，格式为：**服务名:region:domainId:资源类**

参数	说明
	型:资源路径，支持通配符号*，通配符号表示所有。在 JSON 视图中，不带 Resource 表示对所有资源生效。 Resource 支持以下字符：-_0-9a-zA-Z*.\，如果 Resource 中包含不支持的字符，请采用通配符号*。 OBS 是全局级服务，**region** 填“*”；domainId 表示资源拥有者的帐号 ID，建议填写“*”简单地表示所填资源的帐号 ID。 示例： – "obs:*:*:bucket:*": 表示所有的 OBS 桶。 – "obs:*:*:object:my-bucket/my-object/*": 表示桶 my-bucket 中“my-object”目录下的所有对象。 • Condition（条件） 使策略生效的特定条件，可选。格式为：**条件运算符: {条件名:[条件值 1, 条件值 2]}** 条件包含全局条件名和云服务条件名，OBS 支持的条件名与桶策略中的 Condition 一致，在 IAM 配置时，需要加上“obs:”。详细的 Condition 介绍如条件所示。 Condition 的条件值仅支持以下字符：-,./ a-zA-Z0-9_@#$%&，如果条件值中包含不支持的字符，请考虑使用模糊匹配的条件运算符，如：StringLike，StringStartWith 等。 示例： – "StringEndWithIfExists":{"g:UserName":["specialCharacter"]}：表示当用户输入的用户名以"specialCharacter"结尾时该条 statement 生效。 "StringLike":{"obs:prefix":["private/"]}：表示在列举桶内对象时，需要指定 prefix 为 private/或者包含 private/这一子字符串。

IAM 策略鉴权

IAM 策略遵循 Deny 优先的原则。在用户访问资源时，权限检查逻辑如下：

图2-14 系统鉴权逻辑图



说明

每条策略做评估时，Action 之间是“或(or)”的关系。

1. 用户访问系统，发起操作请求。
2. 系统评估用户被授予的访问策略，鉴权开始。
3. 在用户被授予的访问策略中，系统将优先寻找显式拒绝指令。如找到一个适用的显式拒绝，系统将返回 Deny 决定。
4. 如果没有找到显式拒绝指令，系统将寻找适用于请求的任何 Allow 指令。如果找到一个显式允许指令，系统将返回 Allow 决定。
5. 如果找不到显式允许，最终决定为 Deny，鉴权结束。

2.9.2.2 桶策略和对象策略

桶和对象的拥有者

桶的拥有者是创建桶的帐号。一个帐号下的 IAM 用户创建的桶，桶拥有者为该 IAM 用户的父级帐号。

对象的拥有者是上传对象的帐号，而不是对象所属的桶的拥有者。例如，如果帐号 B 被授予访问帐号 A 的桶的权限，然后帐号 B 上传一个文件到桶中，则帐号 B 是对象的拥有者，而不是帐号 A。

桶策略

桶策略是作用于所配置的 OBS 桶及桶内对象的。OBS 桶拥有者通过桶策略可为 IAM 用户或其他帐号授权桶及桶内对象的操作权限。

桶策略的应用场景：

- 不用 IAM 策略控制访问权限的情况下，允许其他帐号访问 OBS 资源，可以使用桶策略的方式授权其他帐号对应的权限。
- 当不同的桶对于不同的 IAM 用户有不同的访问控制需求时，需使用桶策略分别授权 IAM 用户不同的权限。
- 桶拥有者允许其他帐号访问自己的桶时，可使用桶策略授权其他帐号对应的权限。

桶策略模板：

OBS 控制台预置了六种常用典型场景的桶策略模板，用户可以使用模板创建桶策略，快速完成桶策略配置。

选择使用模板创建时，部分模板需要指定被授权用户或资源范围，您也可以在原模板基础上修改被授权用户、资源范围、模板动作以及增加桶策略执行的条件。

表2-10 桶策略模板

模板名称	被授权用户	资源范围	模板动作
桶只读	待指定	包含当前桶和桶内所有对象	**允许指定用户对当前桶和桶内所有对象执行以下动作：** Get*（所有获取操作） List*（所有列举操作）
桶读写	待指定	包含当前桶和桶内所有对象	**允许指定用户对当前桶和桶内所有对象执行除以下动作以外的所有动作：** DeleteBucket（删除桶） PutBucketPolicy（设置桶策略） PutBucketAcl（设置桶 ACL）
目录只读	待指定	待指定（需指定对象前缀）	**允许指定用户对当前桶和桶内指定资源执行以下动作：** ListBucket（列举桶内对象、获取桶元数据） GetBucketLocation（获取桶位置） ListBucketVersions（列举桶内多版本对象） GetObject（获取对象内容、获取对象元数据） RestoreObject（恢复归档存储对象）

模板名称	被授权用户	资源范围	模板动作
			GetObjectAcl（获取对象 ACL） GetObjectVersion（获取指定版本对象内容、获取指定版本对象元数据） GetObjectVersionAcl（获取指定版本对象 ACL）
目录读写	待指定	待指定（需指定对象前缀）	**允许指定用户对当前桶和桶内指定资源执行以下动作：** ListBucket（列举桶内对象、获取桶元数据） GetBucketLocation（获取桶位置） ListBucketVersions（列举桶内多版本对象） ListBucketMultipartUploads（列举多段上传任务） GetObject（获取对象内容、获取对象元数据） PutObject（PUT 上传，POST 上传，上传段，初始化上传段任务，合并段） RestoreObject（恢复归档存储对象） GetObjectAcl（获取对象 ACL） PutObjectAcl（设置对象 ACL） GetObjectVersion（获取指定版本对象内容、获取指定版本对象元数据） GetObjectVersionAcl（获取指定版本对象 ACL） AbortMultipartUpload（取消多段上传任务） ListMultipartUploadParts（列举已上传段） ModifyObjectMetaData（修改对象元数据）
公共读	匿名用户（表示所有互联网用户）	包含当前桶和桶内所有对象	**允许匿名用户（所有互联网用户）对当前桶和桶内所有对象执行以下动作：** GetBucketLocation（获取桶位置） ListBucketVersions（列举桶内多版本对象） GetObject（获取对象内容、获取对象元数据） RestoreObject（恢复归档存储对象）

模板名称	被授权用户	资源范围	模板动作
			GetObjectVersion（获取指定版本对象内容、获取指定版本对象元数据）
公共读写	匿名用户（表示所有互联网用户）	包含当前桶和桶内所有对象	**允许匿名用户（所有互联网用户）对当前桶和桶内所有对象执行以下动作：** ListBucket（列举桶内对象、获取桶元数据） GetBucketLocation（获取桶位置） ListBucketVersions（列举桶内多版本对象） ListBucketMultipartUploads（列举多段上传任务） GetObject（获取对象内容、获取对象元数据） PutObject（PUT 上传，POST 上传，上传段，初始化上传段任务，合并段） RestoreObject（恢复归档存储对象） GetObjectAcl（获取对象 ACL） PutObjectAcl（设置对象 ACL） GetObjectVersion（获取指定版本对象内容、获取指定版本对象元数据） GetObjectVersionAcl（获取指定版本对象 ACL） AbortMultipartUpload（取消多段上传任务） ListMultipartUploadParts（列举已上传段） ModifyObjectMetaData（修改对象元数据）

自定义桶策略：

您也可以根据实际业务场景的定制化需求，不使用预置桶策略模板，自定义创建桶策略。自定义桶策略由允许/拒绝、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。详细请参见桶策略参数说明。

对象策略

对象策略即为桶策略中针对对象的策略，桶策略中针对对象的策略是通过配置资源来实现对象匹配的，资源可配置“*”（表示所有对象）或对象前缀（表示对象集）。对象策略则是直接选定对象后，配置到选定的对象资源的策略。

对象策略模板：

OBS 控制台预置了四种常用典型场景的对象策略模板，用户可以使用模板创建对象策略，快速完成对象策略配置。

选择使用模板创建时，部分模板需要指定被授权用户，您也可以在原模板基础上修改被授权用户、模板动作以及增加对象策略执行的条件。资源范围即为所需配置对象策略的对象，系统自动指定，无需修改。

表2-11 对象策略模板

模板名称	被授权用户	资源范围	模板动作
只读模式	待指定	系统自动指定为已选对象，无需修改	**允许指定用户对当前对象执行以下动作：** GetObject（获取对象内容、获取对象元数据） GetObjectVersion（获取指定版本对象内容、获取指定版本对象元数据） GetObjectVersionAcl（获取指定版本对象ACL） GetObjectAcl（获取对象 ACL） RestoreObject（恢复归档存储对象）
读写模式	待指定	系统自动指定为已选对象，无需修改	**允许指定用户对当前对象执行以下动作：** PutObject（PUT 上传，POST 上传，上传段，初始化上传段任务，合并段） GetObject（获取对象内容、获取对象元数据） GetObjectVersion（获取指定版本对象内容、获取指定版本对象元数据） ModifyObjectMetaData（修改对象元数据） ListMultipartUploadParts（列举已上传段） AbortMultipartUpload（取消多段上传任务） GetObjectVersionAcl（获取指定版本对象ACL） GetObjectAcl（获取对象 ACL） PutObjectAcl（设置对象 ACL） RestoreObject（恢复归档存储对象）
公共读	匿名用户	系统自动指定	**允许匿名用户（所有互联网用户）对当**

模板名称	被授权用户	资源范围	模板动作
	（表示所有互联网用户）	为已选对象，无需修改	**前对象执行以下动作：** GetObject（获取对象内容、获取对象元数据） RestoreObject（恢复归档存储对象） GetObjectVersion（获取指定版本对象内容、获取指定版本对象元数据）
公共读写	匿名用户（表示所有互联网用户）	系统自动指定为已选对象，无需修改	**允许匿名用户（所有互联网用户）对当前对象执行以下动作：** PutObject（PUT 上传，POST 上传，上传段，初始化上传段任务，合并段） GetObject（获取对象内容、获取对象元数据） ModifyObjectMetaData（修改对象元数据） ListMultipartUploadParts（列举已上传段） AbortMultipartUpload（取消多段上传任务） RestoreObject（恢复归档存储对象） GetObjectVersion（获取指定版本对象内容、获取指定版本对象元数据） PutObjectAcl（设置对象 ACL） GetObjectVersionAcl（获取指定版本对象 ACL） GetObjectAcl（获取对象 ACL）

自定义对象策略：

你也可以根据实际业务场景的定制化需求，不使用预置对象策略模板，自定义创建对象策略。自定义对象策略由允许/拒绝、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，与桶策略类似，详细请参见桶策略参数说明。其中资源为已选择的对象，系统自动配置。

2.9.2.3 桶 ACL 和对象 ACL

访问控制列表（Access Control List，ACL）是一个指定被授权用户和所授予权限的授权列表，它可以帮助您管理桶和对象的访问权限。每一个桶和对象都有其对应的 ACL，它定义了哪些帐号或群组被授予访问权限以及其拥有的权限类型。当收到对资源的请求时，OBS 会检查资源的 ACL 来验证请求者是否具有必要的访问权限。

默认情况下，创建桶和对象时会同步创建 ACL，授予资源拥有者对桶和对象的完全控制权限（FULL_CONTROL）。

一个桶的 ACL 最多支持 100 条授权，一个对象的 ACL 也最多支持 100 条授权。

谁是被授权用户

被授权用户可以是使用云服务的帐号或 OBS 预定义的群组，详细信息如表 2-12 所示。

表2-12 OBS 支持的被授权用户

被授权用户	描述
特定用户	ACL 支持通过帐号授予桶/对象的访问权限。授予帐号权限后，帐号下所有具有 OBS 资源权限的 IAM 用户都可以拥有此桶/对象的访问权限。 当需要为不同 IAM 用户授予不同的权限时，可以通过桶策略配置，具体操作请参见为 IAM 用户授予指定桶的操作权限。
拥有者	桶的拥有者是指创建桶的帐号。桶拥有者默认拥有所有的桶访问权限，其中桶 ACL 的读取和写入这两种权限永远拥有，且不支持修改。 对象的拥有者是上传对象的帐号，而不是对象所属的桶的拥有者。对象拥有者默认永远拥有对象读取权限、ACL 的读取和写入权限，且不支持修改。 **须知** 不建议修改桶拥有者的对桶读取和写入权限。
匿名用户	未注册云服务的普通访客群组。如果匿名用户被授予了访问桶/对象的权限，则表示所有人都可以访问对应的桶/对象，并且不需要经过任何身份认证。
日志投递用户组 **说明** 仅桶 ACL 支持。	日志投递用户组用于投递 OBS 桶及对象的访问日志。由于 OBS 本身不能在帐号的桶中创建或上传任何文件，因此在需要为桶记录访问日志时，只能由帐号授予日志投递用户组一定权限后，OBS 才能将访问日志写入指定的日志存储桶中。该用户组仅用于 OBS 内部的日志记录。 **须知** 当日志记录开启后，目标存储桶的日志投递用户组会同步开启桶的写入权限和 ACL 读取权限。若手动将日志投递用户组的桶写入权限和 ACL 读取权限关闭，桶的日志记录会失败。

通过 ACL 可以授予什么权限

桶 ACL 的可以授予的权限如表 2-13 所示：

表2-13 桶 ACL 访问权限

权限	选项	描述
桶访问权限	读取权限	此权限可以获取该桶内对象列表和桶的元数据。

权限	选项	描述
	READ	
	写入权限 WRITE	此权限可以上传、覆盖和删除该桶内任何对象。
ACL 访问权限	读取权限 READ_ACP	此权限可以获取对应桶的 ACL 权限控制列表。 桶的拥有者默认永远具有 ACL 的读取权限。
	写入权限 WRITE_ACP	此权限可以更新对应桶的 ACL 权限控制列表。 桶的拥有者默认永远具有 ACL 的写入权限。

对象 ACL 可以授予的权限如表 2-14 所示：

表2-14 对象 ACL 访问权限

权限	选项	描述
对象访问权限	读取权限 READ	此权限可以获取该对象内容和元数据。
ACL 访问权限	读取权限 READ_ACP	此权限可以获取对应对象的 ACL 权限控制列表。 对象的拥有者默认永远具有 ACL 的读取权限
	写入权限 WRITE_ACP	此权限可以更新对应对象的 ACL 权限控制列表。 对象的拥有者默认永远具有 ACL 的写入权限。

说明

每一次对桶/对象的授权操作都将覆盖桶/对象已有的权限列表，而不会对其新增权限。

此外，可以在调用创建桶或上传对象 API 时通过头域设置 ACL，可以设置六种预定义的权限，这六种权限对桶或对象的拥有者不产生影响，即拥有者仍然拥有完全控制的权限（FULL_CONTROL）。其详细情况如表 2-15 所示。

表2-15 OBS 预定义的权限控制策略

预定义的权限控制策略	描述
private	桶或对象的拥有者拥有完全控制的权限，其他任何人都没有访问权限。此为系统默认的权限控制策略。
public-read	设在桶上，所有人可以获取该桶内对象列表、桶内多段任务、桶的元数据、桶的多版本。 设在对象上，所有人可以获取该对象内容和元数据。

预定义的权限控制策略	描述
public-read-write	设在桶上，所有人可以获取该桶内对象列表、桶内多段任务、桶的元数据、桶的多版本、上传对象删除对象、初始化段任务、上传段、合并段、拷贝段、取消多段上传任务。 设在对象上，所有人可以获取该对象内容和元数据。
public-read-delivered	设在桶上，所有人可以获取该桶内对象列表、桶内多段任务、桶的元数据、桶的多版本，可以获取该桶内对象的内容和元数据。 不能应用在对象上。
public-read-write-delivered	设在桶上，所有人可以获取该桶内对象列表、桶内多段任务、桶的元数据、桶的多版本、上传对象删除对象、初始化段任务、上传段、合并段、拷贝段、取消多段上传任务，可以获取该桶内对象的内容和元数据。 不能应用在对象上。
bucket-owner-full-control	设在桶上，桶的拥有者拥有完全控制的权限，其他任何人都没有访问权限。 设在对象上，桶或对象的拥有者拥有完全控制的权限，其他任何人都没有访问权限。

桶 ACL 使用场景

OBS ACL 是基于帐号和群组级别的读写权限控制，权限控制细粒度不如桶策略和 IAM 策略。一般情况下，建议使用 IAM 策略和桶策略进行访问控制。

在以下场景，建议您使用桶 ACL：

- 授予指定帐号桶读取权限和桶写入权限，用以共享桶数据或挂载外部桶。

对象 ACL 使用场景

OBS ACL 是基于帐号和群组级别的读写权限控制，权限控制细粒度不如桶策略和 IAM 策略。一般情况下，建议使用 IAM 策略和桶策略进行访问控制。

在以下场景，建议您使用对象 ACL：

- 需要对象级的访问权限控制时。桶策略可以授予对象或对象集访问权限，当授予一个对象集权限后，想对对象集中某一个对象再进行单独授权，通过配置桶策略的方法显然不太实际。此时建议使用对象 ACL，使得单个对象的权限控制更加方便。
- 使用对象链接访问对象时。一般使用对象 ACL，将某一个对象通过对象链接开放给匿名用户进行读取操作。

2.9.2.4 桶策略和 ACL 的关系

桶 ACL 和桶策略的映射关系

桶 ACL 用于授予桶基本的读写权限，桶策略高级设置中支持更多在桶上可以执行的动作。桶策略是对桶 ACL 的补充，除了限定的只能由桶 ACL 授予日志投递用户组权限外，更多时候桶策略可以替代桶 ACL 管理桶的访问权限。桶 ACL 访问权限和桶策略动作的映射关系如表 2-16 所示。

表2-16 桶 ACL 和桶策略的映射关系

ACL 权限	选项	对应桶策略高级设置中的动作
桶访问权限	读取权限	• ListBucket • ListBucketVersions • ListBucketMultipartUploads
	写入权限	• PutObject • DeleteObject • DeleteObjectVersion
ACL 访问权限	读取权限	GetBucketAcl
	写入权限	PutBucketAcl

对象 ACL 和桶策略的映射关系

对象 ACL 用于授予对象基本的读写权限。桶策略高级设置中支持更多在对象上可以执行的动作。对象 ACL 访问权限和桶策略动作的映射关系如表 2-17 所示。

表2-17 对象 ACL 和桶策略的映射关系

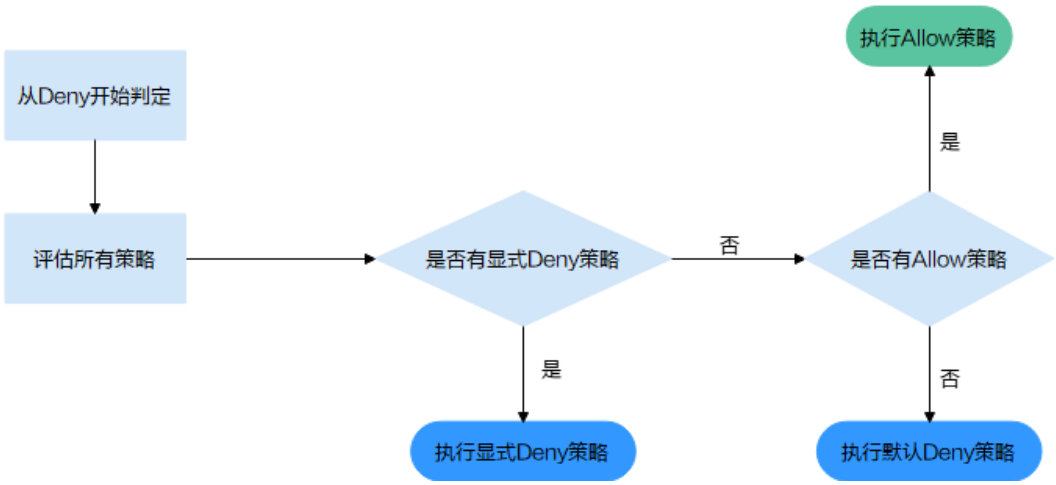
对象 ACL 权限	选项	对应桶策略高级设置中的动作
对象访问权限	读取权限	• GetObject • GetObjectVersion
ACL 访问权限	读取权限	• GetObjectAcl • GetObjectVersionAcl
	写入权限	• PutObjectAcl • PutObjectVersionAcl

2.9.2.5 访问控制机制冲突时，如何工作？

基于最小权限原则，权限控制策略的结果默认为 Deny， 显式的 Deny 始终优先于 Allow。例如，IAM 策略授权了用户对对象的访问权限，但是桶策略拒绝了该用户访问对象的权限，且没有 ACL 时，该用户不能访问对象。

没有策略授权 Allow 权限时，默认情况即为拒绝访问权限。当有策略授权 Allow 权限，且没有其他策略 Deny 该权限时，Allow 的权限才能允许访问。例如，某个桶已经存在多条 Allow 权限的桶策略，再新增 Allow 权限的桶策略，会在原权限的基础上进行叠加，增大用户的权限；如果新增 Deny 权限的桶策略，则会根据 Deny 优先原则调整用户的权限，即使 Deny 策略中定义的动作在其他桶策略中 Allow。

图2-15 访问策略授权过程



桶策略、IAM 策略和 ACL 的 Allow 和 Deny 作用结果如图 2-16 所示。

图2-16 桶策略、IAM 策略和 ACL 的 Allow 和 Deny 作用结果

桶策略	IAM策略			ACL
	Deny	Allow	Default Deny	
Deny	Deny			Allow
				Default Deny
Allow	Deny	Allow		Allow
				Default Deny
Default Deny		Allow	Deny	Allow
		Deny	Deny	Default Deny

2.9.3 桶策略参数说明

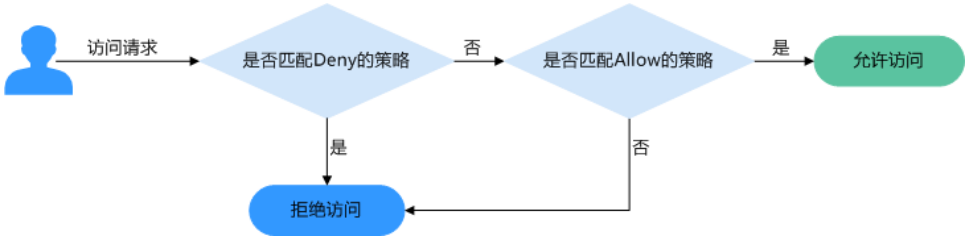
2.9.3.1 允许/拒绝

桶策略可以配置为允许或拒绝请求。

- Allow：指定本条桶策略描述的权限为接受请求。
- Deny：指定本条桶策略描述的权限为拒绝请求。

当桶策略中既有 Allow 又有 Deny 的授权语句时，遵循 Deny 优先的原则，其判定逻辑如下：

图2-17 高级桶策略 Allow 和 Deny 冲突时逻辑判定



1. 用户发起访问请求。
2. OBS 从桶策略中优先寻找设置为拒绝（显式拒绝）的策略。如果找到一个显式拒绝该访问请求的策略，OBS 将直接返回拒绝访问的决定，访问请求结束。
3. 如果没有显式拒绝该访问的策略，OBS 将寻找允许该访问请求的策略。
   - 如果找到显式允许的策略，OBS 返回允许访问的决定，随后由 OBS 继续处理该请求。
   - 如果找不到显式允许的策略，最终返回拒绝访问的决定，访问请求结束。
4. 如果在判定过程中遇到错误，将生成异常信息返回给发起访问请求的用户。

2.9.3.2 被授权用户

被授权用户指桶策略作用的用户，这里的用户可以是帐号，也可以是 IAM 用户。被授权用户可以通过包含和排除两种方式来指定：

- 包含：桶策略对指定的用户生效。
- 排除：桶策略对除指定用户外的其他用户生效。

2.9.3.3 资源

在指定资源时，资源可以是当前整个桶，也可以是桶内对象。

资源可以通过包含和排除两种方式来指定：

- 包含：桶策略对指定的 OBS 资源生效。
- 排除：桶策略对除设置外的其他 OBS 资源生效。

指定资源为桶

指定资源为当前整个桶时，桶策略动作需配置为桶相关的动作，配置方法为“资源范围”选择“当前桶”。

指定资源为对象

指定资源为桶内对象时，桶策略动作需配置为对象相关的动作，配置格式如下：

- 对象：直接输入对象名称（包括文件夹名称）。例如，指定的资源是桶中 imgs-folder 文件夹下的 example.jpg 文件，则在资源输入框中输入以下内容。

  imgs-folder/example.jpg
- 对象集：当指定给对象集时，使用通配符“*”。通配符“*”表示 0 个或多个字符的任意组合。其输入格式为：
  - 仅使用一个通配符“*”，表示桶中所有对象。
  - 使用*“对象名称前缀”*+“*”，表示桶中所有以此前缀开头的对象。示例：

    imgs*
  - 使用“*”+“对象名后缀”，表示桶中所有以此后缀结尾的对象。示例：

    *.jpg

说明

多个对象或对象集使用英文逗号“,”分隔。

2.9.3.4 动作

桶策略动作与资源相关，当资源为当前整个桶时，桶策略动作需配置为桶相关的动作；当资源为桶内对象时，桶策略动作需配置为对象相关的动作。

桶策略动作可以通过包含和排除两种方式来指定：

- 包含：桶策略对指定的动作生效。
- 排除：桶策略对除指定动作外的其他动作生效。

与桶相关的动作

表2-18 桶相关动作含义

类型	值	描述
通用（General）	*	通配符，表示该资源能进行的所有操作。
	Get*	表示该资源能进行的所有的获取操作。
	Put*	表示该资源能进行的所有的设置操作。
	List*	表示该资源能进行的所有的列举操作。
桶（Bucket）	DeleteBucket	删除桶。
	ListBucket	列举桶内对象，获取桶元数据。

类型	值	描述
	ListBucketVersions	列举桶内多版本对象。
	ListBucketMultipartUploads	列举多段上传任务。
	GetBucketAcl	获取桶 ACL 的相关信息。
	PutBucketAcl	设置桶 ACL。
	GetBucketCORS	获取桶 CORS 配置的相关信息。
	PutBucketCORS	设置桶 CORS。
	GetBucketVersioning	获取桶多版本的相关信息。
	PutBucketVersioning	设置多版本。
	GetBucketLocation	获取桶位置。
	GetBucketLogging	获取桶日志记录的相关信息。
	PutBucketLogging	设置桶日志记录。
	GetBucketWebsite	获取桶的静态网站配置的相关信息。
	PutBucketWebsite	设置桶的静态网站托管。
	DeleteBucketWebsite	删除桶的静态网站托管配置。
	GetLifecycleConfiguration	获取桶生命周期规则。
	PutLifecycleConfiguration	设置桶生命周期规则。

与对象相关的动作

表2-19 对象相关动作含义

类型	值	描述
通用（General）	*	通配符，表示该资源能进行的所有操作。
	Get*	表示该资源能进行的所有的获取操作。
	Put*	表示该资源能进行的所有的设置操作。
	List*	表示该资源能进行的所有的列举操作。
对象（Object）	GetObject	可用作于获取对象内容，获取对象元数据。
	GetObjectVersion	可用作于获取指定版本对象内容，获取指定版本对象元数据。

类型	值	描述
	PutObject	可用作于 PUT 上传，POST 上传，上传段，初始化上传段任务，合并段。
	GetObjectAcl	获取对象 ACL 的相关信息。
	GetObjectVersionAcl	获取指定版本对象 ACL。
	PutObjectAcl	设置对象 ACL。
	PutObjectVersionAcl	设置指定版本对象 ACL。
	DeleteObject	删除对象。
	DeleteObjectVersion	删除对象（针对特定版本的对象）。
	ListMultipartUploadParts	列举已上传段。
	AbortMultipartUpload	取消多段上传任务。

2.9.3.5 条件

除了指定允许/拒绝、被授权用户、资源、动作外，桶策略还可以指定生效条件。只有当条件设置的表达式与访问请求中的值匹配时，桶策略才生效。条件是可选参数，用户可以根据业务需要选择是否使用。

例如，帐号 A 想要拥有帐号 B 向其 example 桶中上传的对象的完全控制权限（因为默认情况下对象由上传该对象的帐号 B 拥有），则可以指定上传请求中必须包含 acl 键，以及显式授予完全控制权限，完整的条件表达式如下：

条件运算符	键	值
StringEquals	acl	bucket-owner-full-control

条件由条件运算符、键、值三部分组成，最终组成一个条件表达式，决定桶策略生效的条件。条件运算符、键两者之间存在互相限制的关联关系，例如：

- 条件运算符选择了一个 String 类型的，比如 StringEquals，键就只能选择 String 类型的，比如 UserAgent。
- 键选择了一个 Date 类型，比如 CurrentTime，条件运算符就只能选择 Date 类型的，比如 DateEquals。

OBS 提供如表 2-20 所示的预定义条件运算符。

表2-20 各条件运算符含义

类型	关键字	说明
String	StringEquals	字符串匹配，简化为：streq。

类型	关键字	说明
	StringNotEquals	字符串不匹配，简化为：strneq。
	StringEqualsIgnoreCase	忽略大小写的字符串匹配，简化为：streqi。
	StringNotEqualsIgnoreCase	忽略大小写的字符串不匹配，简化为：strneqi。
	StringLike	宽松的区分大小写的匹配。这些值可以在字符串中的任何地方包括一个多字符匹配的通配符(*)和单字符匹配通配符(?)。简化为：strl。
	StringNotLike	非宽松区分大小写的匹配。这些值可以在字符串中的任何地方包括一个多字符匹配的通配符(*)和单字符匹配通配符(?)。简化为：strnl。
Numeric	NumericEquals	相等，简化为：numeq。
	NumericNotEquals	不相等，简化为：numneq。
	NumericLessThan	小于，简化为：numlt。
	NumericLessThanEquals	小于等于，简化为：numlteq。
	NumericGreaterThan	大于，简化为：numgt。
	NumericGreaterThanEquals	大于等于，简化为：numgteq。
Date	DateEquals	日期时间相等，简化为：dateeq。
	DateNotEquals	日期时间不相等，简化为：dateneq。
	DateLessThan	日期时间小于，简化为：datelt。
	DateLessThanEquals	日期时间小于等于，简化为：datelteq。
	DateGreaterThan	日期时间大于，简化为：dategt。
	DateGreaterThanEquals	日期时间大于等于，简化为：dategteq。
Boolean	Bool	严格布尔值相等。
IP address	IpAddress	指定的 IP 或 IP 范围，例如 x.x.x.x/24。
	NotIpAddress	除指定的 IP 或 IP 范围外所有 IP，例如 x.x.x.x/24。

条件中可选的键包括以下三种：动作无关的通用键、与桶动作有关的键和与对象动作有关的键。

表2-21 通用键

键	类型	描述
CurrentTime	Date	服务器接收请求的时间，格式满足 ISO 8601 标准。
EpochTime	Numeric	服务器接收请求的时间，格式为 1970.01.01 00:00:00 UTC 开始所经过的秒数，不考虑闰秒。
SecureTransport	Bool	请求是否使用 SSL 加密。
SourceIp	IP address	请求发起的源 IP。
UserAgent	String	请求的客户端软件代理程序。
Referer	String	请求从哪个链接发起。

表2-22 与桶动作有关的键

Action	可选键	描述	说明
ListBucket	prefix	String 类型，列举以指定的字符串 prefix 开头的对象。	配置 prefix、delimiter、max-keys 后，执行 List 操作时需要带上符合条件的键值对信息，桶策略才生效。 例如，某桶配置了匿名用户可读的桶策略，且条件运算符 =NumericEquals，键=max-keys，值=100。则匿名用户列举对象时需要在桶访问域名末尾加上?max-keys=100，才能完成对象列举，且列举的对象将是按照字典顺序的前 100 个对
	max-keys	Numeric 类型，指定返回的最大数，返回的对象列表将是按照字典顺序的最多前 max-keys 个对象。	
ListBucketVersions	prefix	String 类型，列举以指定的字符串 prefix 开头的多版本对象。	
	max-keys	Numeric 类型，指定返回的最大数，返回的对象列表将是按照字典顺序的最多前 max-keys 个对象。	

Action	可选键	描述	说明
			象。
PutBucketAcl	acl	String 类型，设置桶 ACL。修改桶 ACL 时在头域中可以包含的 Canned ACL，取值范围为 private|public-read|public-read-write|authenticated-read|bucketowner-read|bucket-owner-full-control|log-delivery-write。	无

表2-23 与对象动作相关的键

Action	可选键	描述
PutObject	acl	String 类型，设置对象 ACL。上传对象时在头域中可以包含的 Canned ACL，取值范围为 private|public-read|public-read-write|authenticated-read|bucketowner-read|bucket-owner-full-control|log-delivery-write。
	copysource	String 类型，用来指定复制对象时对象操作的源桶名以及源对象名。格式如 /bucketname/keyname。
	metadata-directive	String 类型，用来指定新对象的元数据是从元对象中复制，还是用请求中的元数据替换，取值范围为 COPY|REPLACE。
PutObjectAcl	acl	String 类型，设置对象 ACL。上传对象时在头域中可以包含的 Canned ACL，取值范围为 private|public-read|public-read-write|authenticated-read|bucketowner-read|bucket-owner-full-control|log-delivery-write。
GetObjectVersion	VersionId	String 类型，获取 VersionId 为 xxx 版本的对象。
GetObjectVersionAcl	VersionId	String 类型，获取 VersionId 为 xxx 版本的对象 ACL。
PutObjectVersionAcl	VersionId	String 类型，设置 VersionId。
	acl	String 类型，设置 VersionId 为 xxx 版本的对象 ACL。上传对象时在头域中可以包含的 Canned ACL，取值范围为 private|public-read|public-read-write|authenticated-read|bucketowner-

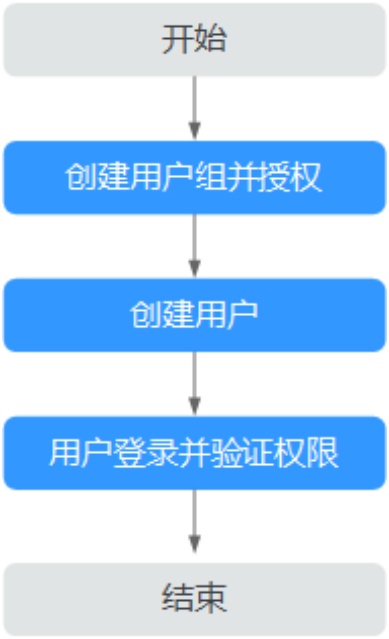
Action	可选键	描述
		read|bucket-owner-full-control|log-delivery-write。
DeleteObjectVersion	VersionId	String 类型，删除 VersionId 为 xxx 版本的对象。

2.9.4 配置 IAM 策略

2.9.4.1 创建 IAM 用户并授权使用 OBS

示例流程

图2-18 为 IAM 用户授权 OBS 资源权限



操作步骤

步骤 1 使用云服务帐号登录管理控制台。

步骤 2 在顶部导航栏选择“服务列表>管理与部署>统一身份认证服务”，进入“统一身份认证服务”管理控制台。

步骤 3 创建用户组并授予 OBS 资源权限。

用户组是用户的集合，IAM 通过用户组功能实现用户的授权。您在 IAM 中创建的用户，需要加入特定用户组后，用户才具备用户组所拥有的权限。

1. 在左侧导航栏单击“用户组”，进入“用户组”界面。

2. 单击“创建用户组”。
3. 在“创建用户组”界面，输入“用户组名称”和“描述”，单击“创建”。
   用户组创建完成，界面自动返回用户组列表，列表中显示新建的用户组。
4. 单击所创建的用户组右侧操作列的“权限配置”。
5. 在用户组详情页，选择“权限管理”页签，单击“配置权限”。
6. 作用范围选择“全局服务”，根据需求选中权限，单击“确定”。

步骤 4 创建用户操作详见创建 IAM 用户。

步骤 5 使用 IAM 用户登录 OBS 管理控制台，验证用户权限。

----结束

2.9.5 配置桶策略

2.9.5.1 使用模板创建桶策略

OBS 控制台预置了六种常用典型场景的桶策略模板，用户可以使用模板创建桶策略，快速完成桶策略配置。

操作步骤

步骤 1 在桶列表单击待操作的桶，进入“对象”页面。

步骤 2 在左侧导航栏，单击“访问权限控制 > 桶策略”。

步骤 3 单击“创建”。

步骤 4 单击对应模板右侧的“使用模板创建”。

图2-19 使用模板创建桶策略

步骤 5 完善桶策略配置信息。

部分桶策略模板需要指定被授权用户或资源范围，请根据界面提示完成桶策略配置。您也可以在原有模板基础上修改策略名称、被授权用户、资源范围、动作以及条件。相关说明请参见桶策略参数说明。

图2-20 配置桶策略

步骤 6 单击界面右下角的“配置确认”，确认桶策略信息是否正确。

图2-21 确认策略

步骤 7 单击界面右下角的“创建”，完成桶策略创建。

----结束

2.9.5.2 自定义创建桶策略（可视化视图）

您可以根据实际业务场景的定制化需求，不使用预置桶策略模板，自定义创建桶策略。自定义桶策略由允许/拒绝、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。

操作步骤

步骤 1 在桶列表单击待操作的桶，进入“对象”页面。

步骤 2 在左侧导航栏，单击“访问权限控制 > 桶策略”。

步骤 3 单击“创建”。

步骤 4 在桶策略模板第一行，单击右侧的“自定义创建”。

图2-22 自定义创建桶策略

步骤 5 配置桶策略。

图2-23 配置桶策略

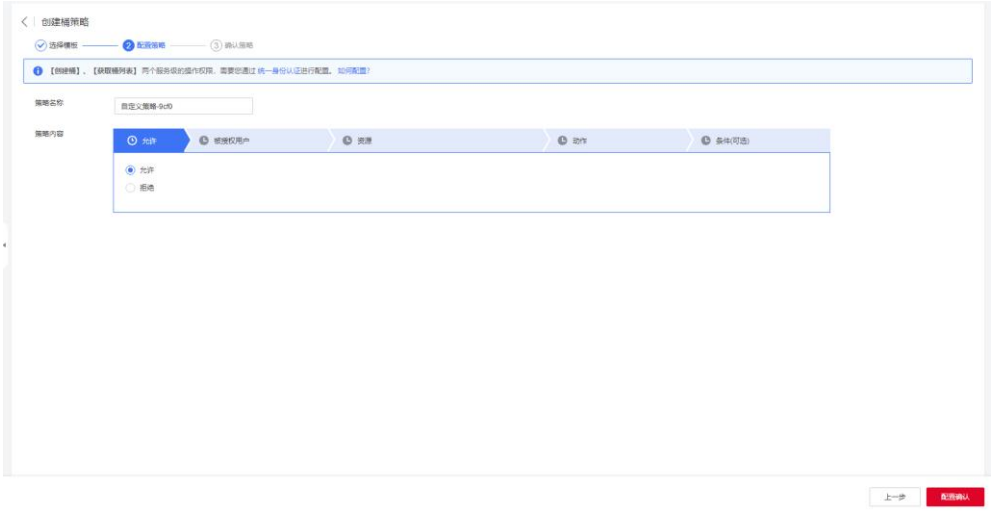


表2-24 自定义桶策略参数配置说明

参数		说明
策略名称		输入自定义桶策略的名称。
策略内容	允许/拒绝	• 允许：指定本条桶策略描述的权限为接受请求。 • 拒绝：指定本条桶策略描述的权限为拒绝请求。
	被授权用户	• 选择被授权用户： – 当前帐号：可以选择当前帐号下的一个或多个 IAM 用户。 – 其他帐号：可以设置一个或多个其他帐号 ID。若是只想为其他帐号下的 IAM 用户授权，则需再配置 IAM 用户 ID，可以指定多个 IAM 用户。 – 匿名用户：表示桶策略授权给互联网上的所有人。

参数		说明
		• 选择用户策略： – 包含以上用户：桶策略对指定的用户生效。 – 排除以上用户：桶策略对除指定用户外的其他用户生效。
	资源	• 选择资源范围： – 当前桶：表示当前桶，可以在动作中配置桶相关动作。 – 桶内对象：表示桶内所有对象或指定对象，可以在动作中配置对象相关动作。 指定对象的资源路径中支持填写对象或对象集 对象：对象名称 对象集：“对象名称前缀”+“*”、“*”+“对象名后缀”或“*” • 选择资源策略： – 包含以上资源：桶策略对指定的资源生效。 – 排除以上资源：桶策略对除指定资源外的其他资源生效。
	动作	• 指定被授权的动作：详细的动作信息，请参见桶策略参数说明。 – 若“资源”仅选择“当前桶”，可选择配置“通用动作”和“桶动作”。 – 若“资源”仅选择“桶内对象”，可选择配置“通用动作”和“对象动作”。 – 若“资源”同时选择“当前桶”和“桶内对象”，可选择配置“通用动作”、“桶动作”和“对象动作”。 • 选择操作策略： – 包含以上动作：桶策略对指定的动作生效。 – 排除以上动作：桶策略对除指定动作外的其他动作生效。
	条件（可选）	• 条件运算符：请参见桶策略参数说明。 • 键：请参见桶策略参数说明。 • 值：输入的值与键相关。

步骤 6 单击界面右下角的“配置确认”，确认桶策略信息是否正确。

步骤 7 单击界面右下角的“创建”，完成桶策略创建。

----结束

2.9.5.3 复制桶策略

操作场景

OBS 提供桶策略复制功能，帮助您快速将已有桶策略一键复制到新的桶。桶策略复制时，OBS 会自动将源桶桶策略中的桶名替换为新桶桶名，即实现新的桶策略对新桶生效。

约束与限制

- 从源桶复制桶策略的操作为增量复制，不会删除当前桶已存在的桶策略。
- 与当前桶中相同名称的桶策略不会复制。
- 源桶和目标桶的桶版本号都必须是 3.0。

操作步骤

步骤 1 在桶列表单击待操作的桶，进入“对象”页面。

步骤 2 在左侧导航栏，单击“访问权限控制 > 桶策略”。

步骤 3 单击“复制”。

步骤 4 选择复制源，即桶策略所在的源桶。

源桶中所有与当前桶不同名的桶策略将在复制列表中展示，您可以按需移除不需要复制的桶策略。

图2-24 复制桶策略

步骤 5 单击“确定”，将源桶的桶策略复制到当前桶。

----结束

2.9.6 配置对象策略

对象策略是桶策略针对对象的策略，选中对象后配置该对象的对象策略。对象策略的资源为选中的对象，对应的动作和条件为桶策略中针对对象的动作和条件。

操作步骤

步骤 1 在桶列表单击待操作的桶，进入“对象”页面。

步骤 2 在待操作的对象的后面，单击“更多>配置对象策略”，进入“配置对象策略”页面。

支持使用模板创建和自定义创建两种方式，您可以根据需要进行选择。

- 使用模板创建：系统预置了四种常用典型场景的对象策略模板，您可以使用模板快速完成对象策略配置。
- 自定义创建：您也可以根据实际业务场景的定制化需求，不使用预置对象策略模板，自定义创建对象策略。自定义对象策略由允许/拒绝、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，与桶策略类似，详细请参见桶策略参数说明。其中资源为已选择的对象，系统自动配置。自定义创建的方法，可参见自定义创建桶策略（可视化视图），与自定义桶策略相比有如下两点区别：
  a. 资源不需要指定，系统默认指定为已选择对象。
  b. 配置的动作仅支持对象相关动作。

----结束

2.9.7 配置桶 ACL

前提条件

配置桶 ACL 的帐号需要是桶的拥有者，或者具备该桶的 ACL 写权限。

操作步骤

步骤 1 在桶列表单击待操作的桶，进入“对象”页面。

步骤 2 在左侧导航栏，单击“访问权限控制 > 桶 ACLs”。

步骤 3 在“桶 ACLs”中，单击“编辑”可按照需求通过勾选相应权限对拥有者、匿名用户以及日志投递用户组赋予目标桶的 ACL 权限。

步骤 4 单击“增加”，可对特定帐号添加 ACL 权限，如图 2-25 所示。

输入特定账号的“帐号 ID”，并为其设定相应的 ACL 权限。“帐号 ID”可通过“我的凭证”页面查看。

图2-25 添加权限

步骤 5 单击“确定”。

----结束

2.9.8 配置对象 ACL

前提条件

配置对象 ACL 的帐号需要是对象的拥有者，或者具备该对象的 ACL 写权限。

对象的拥有者是上传对象的帐号，而不是对象所属的桶的拥有者。例如，如果帐号 B 被授予访问帐号 A 的桶的权限，帐号 B 上传一个文件到桶中，则帐号 B 是对象的拥有者，而不是帐号 A。默认情况下，帐号 A 没有该对象的访问权限，也无法读取和修改该对象的 ACL。

操作步骤

步骤 1 在桶列表单击待操作的桶，进入“对象”页面。

步骤 2 单击待操作的对象。

步骤 3 在“对象 ACL”中，单击“编辑”可按需求通过勾选相应权限对拥有者以及匿名用户赋予目标对象的 ACL 权限。

说明

不能对已加密的对象设置注册用户和匿名用户的 ACL 权限。

步骤 4 单击“增加”，可对特定帐号添加 ACL 权限，如图 2-26 所示。

输入特定账号的“帐号 ID”，并为其设定相应的 ACL 权限。“帐号 ID”可通过“我的凭证”页面查看。

图2-26 添加对象的 ACL 权限

步骤 5 单击“确定”。

----结束

2.9.9 应用示例

2.9.9.1 为 IAM 用户授予指定桶的操作权限

在主帐号下创建一个 IAM 用户，IAM 用户不加入任何用户组，该 IAM 用户没有任何权限。桶拥有者（主帐号）或者拥有设置桶策略权限的帐号及 IAM 用户可以通过配置桶策略授予 IAM 用户桶的权限。

下面示例以授予 IAM 用户访问桶和上传对象的权限为例。

操作步骤

步骤 1 在桶列表单击待操作的桶，进入“对象”页面。

步骤 2 在左侧导航栏，单击“访问权限控制 > 桶策略”。

步骤 3 单击“创建”。

步骤 4 在桶策略模板第一行，单击右侧的“自定义创建”。

步骤 5 配置如下参数，授予 IAM 用户访问桶（列举对象）和上传对象的权限。

表2-25 授予访问桶和上传对象的权限参数配置

参数	说明
策略配置方式	可视化视图
策略名称	自定义

参数		说明
策略内容	允许/拒绝	允许
	被授权用户	• 授权用户：当前帐号 • 子用户：选择需要授权的 IAM 用户 • 用户策略：包含以上用户
	资源	• 资源范围：同时选择当前桶和桶内对象，桶内对象选择所有对象 • 资源策略：包含以上资源
	动作	• 选择动作：ListBucket 和 PutObject • 操作策略：包含以上动作 **说明** 本例对象动作仅授予上传对象权限。可以根据业务需要选择多个动作，同时授予其他操作权限。“*”代表所有操作。 支持的动作及含义请参见动作。

步骤 6 单击右下角的“配置确认”。

步骤 7 单击右下角的“创建”，完成桶策略创建。

----结束

验证

使用 OBS Browser+用来验证以上授权。

步骤 1 在管理控制台上创建被授权用户的访问密钥（AK/SK）。

步骤 2 打开 OBS Browser+，配置已获取到的 AK/SK，并设置“访问路径”为授权的桶名称。

步骤 3 当主帐号未授权给用户访问桶权限时，用户用 OBS Browser+访问桶时，被拒绝访问。

步骤 4 主帐号配置授予给用户访问桶权限后，用户可以用 OBS Browser+登录访问桶，桶界面正常显示桶中对象。

步骤 5 此时上传对象到桶中，上传失败。

步骤 6 主帐号配置授予给用户上传对象权限后，用户用 OBS Browser+上传对象成功，对象在对象列表中显示。

----结束

2.9.9.2 为其他帐号授予指定桶的操作权限

桶拥有者（主帐号）或者拥有设置桶策略权限的帐号及 IAM 用户可以通过配置桶策略授予其他帐号或其他帐号下 IAM 用户桶的权限。

下面示例以授予其他帐号访问桶和上传对象的权限为例。

说明

如果是给其他帐号下的 IAM 用户授权，需要同时配置桶策略和 IAM 策略。

1. 配置桶策略允许 IAM 用户访问桶。
2. 被授权 IAM 用户所属帐号配置 IAM 策略，允许 IAM 用户访问此桶。

桶策略和 IAM 策略中同时允许的权限才能生效。

操作步骤

步骤 1 在桶列表单击待操作的桶，进入“对象”页面。

步骤 2 在左侧导航栏，单击“访问权限控制 > 桶策略”。

步骤 3 单击“创建”。

步骤 4 在桶策略模板第一行，单击右侧的“自定义创建”。

步骤 5 配置如下参数，授予其他帐号访问桶（列举对象）和上传对象的权限。

表2-26 授予访问桶和上传对象的权限参数配置

参数		说明
策略配置方式		可视化视图
策略名称		自定义
策略内容	允许/拒绝	允许
	被授权用户	• 授权用户：其他帐号 • 其他帐号：填写帐号 ID 和 IAM 用户 ID **说明** 帐号 ID 和用户 ID 通过“我的凭证”页面可以获取。不同授权场景的设置说明： • **授权给所有帐号及 IAM 用户**：帐号 ID 和 IAM 用户 ID 填写通配符（*）； • **仅授权给某个帐号**：填写被授权帐号的帐号 ID 和用户 ID； • **授权给某个帐号及帐号下所有 IAM 用户**：帐号 ID 填写被授权帐号的帐号 ID，用户 ID 填写通配符（*）； • **授权给 IAM 用户**：填写被授权 IAM 用户的帐号 ID 和用户 ID，支持添加多个 IAM 用户。 • 用户策略：包含以上用户
	资源	• 资源范围：同时选择当前桶和桶内对象，桶内对象选择所有对象 • 资源策略：包含以上资源
	动作	• 选择动作：ListBucket 和 PutObject • 操作策略：包含以上动作 **说明**

参数		说明
		本例对象动作仅授予上传对象权限。可以根据业务需要选择多个动作，同时授予其他操作权限。“*”代表所有操作。 支持的动作及含义请参见动作。

步骤 6 单击右下角的“配置确认”。

步骤 7 单击右下角的“创建”，完成桶策略创建。

----结束

验证

使用 OBS Browser+用来验证以上授权。

步骤 1 在管理控制台上创建被授权用户的访问密钥（AK/SK）。

步骤 2 打开 OBS Browser+，配置已获取到的 AK/SK，并设置“访问路径”为授权的桶名称。

步骤 3 当主帐号未授权给用户访问桶权限时，用户用 OBS Browser+访问桶时，被拒绝访问。

步骤 4 主帐号配置授予给用户访问桶权限后，用户可以用 OBS Browser+登录访问桶，桶界面正常显示桶中对象。

步骤 5 此时上传对象到桶中，上传失败。

步骤 6 主帐号配置授予给用户上传对象权限后，用户用 OBS Browser+上传对象成功，对象在对象列表中显示。

----结束

2.9.9.3 限制特定地址对桶的访问权限

通过桶策略可以限制特定地址对指定桶的访问权限。本示例演示拒绝来源 IP 为“114.115.1.0/24”网段的客户端访问桶。

操作步骤

步骤 1 在桶列表单击待操作的桶，进入“对象”页面。

步骤 2 在左侧导航栏，单击“访问权限控制 > 桶策略”。

步骤 3 单击“创建”。

步骤 4 在桶策略模板第一行，单击右侧的“自定义创建”。

步骤 5 配置如下参数。

表2-27 限制特定地址对桶的访问权限

参数	说明

参数		说明
策略配置方式		可视化视图
策略名称		自定义
策略内容	允许/拒绝	拒绝
	被授权用户	• 授权用户：匿名用户 • 用户策略：包含以上用户
	资源	• 资源范围：同时选择当前桶和桶内对象，桶内对象选择所有对象 • 资源策略：包含以上资源
	动作	• 选择动作：*（表示所有动作） • 操作策略：包含以上动作
	条件	• 条件运算符：IpAddress • 键：SourceIP • 值：114.115.1.0/24

步骤 6 单击右下角的“配置确认”。

步骤 7 单击右下角的“创建”，完成桶策略创建。

----结束

验证

使用 114.115.1.0/24 网段内的 IP 地址的客户端访问桶，访问被拒绝。使用 114.115.1.0/24 网段外的 IP 地址的客户端可以访问桶。

2.9.9.4 限制桶中对象的访问起始时间和结束时间

通过桶策略可以限制桶中对象的访问起始时间和结束时间。下面示例配置在 2019-03-26T12:00:00Z 到 2019-03-26T15:00:00Z 期间允许访问操作桶内资源。

操作步骤

步骤 1 在桶列表单击待操作的桶，进入“对象”页面。

步骤 2 在左侧导航栏，单击“访问权限控制 > 桶策略”。

步骤 3 单击“创建”。

步骤 4 在桶策略模板第一行，单击右侧的“自定义创建”。

步骤 5 配置如下参数。

表2-28 限制桶中对象的访问起始时间和结束时间

参数		说明
策略配置方式		可视化视图
策略名称		自定义
策略内容	允许/拒绝	允许
	被授权用户	• 授权用户：匿名用户 • 用户策略：包含以上用户
	资源	• 资源范围：桶内对象，选择所有对象 • 资源策略：包含以上资源 **说明** 本示例仅配置桶内资源的权限，如果还需要配置桶的权限（如列举桶内对象），则需要再额外创建一条配置到当前桶的自定义桶策略。
	动作	• 选择动作：*（表示所有动作） • 操作策略：包含以上动作 **说明** 配置所有权限可能有资源被删除的风险，如果想规避此风险，建议配置动作名称为“Get*”，表示所有读权限。
	条件	• 条件 1： – 条件运算符：DateGreaterThan – 键：CurrentTime – 值：2019-03-26T12:00:00Z（取值为 UTC 格式） • 条件 2： – 条件运算符：DateLessThan – 键：CurrentTime – 值：2019-03-26T15:00:00Z（取值为 UTC 格式）

步骤 6 单击右下角的“配置确认”。

步骤 7 单击右下角的“创建”，完成桶策略创建。

----结束

验证

在设定的允许访问时间，任何用户都可以访问操作桶内资源。在允许时间范围外，除了桶拥有者，其他用户不能访问操作桶内资源。

2.9.9.5 为匿名用户设置对象的访问权限

使用 OBS 存储了大量全球各地的地图数据，这些数据需要对外开放供所有人查阅的。在这种情况下，该公司便可以为这部分数据设置匿名用户的读取权限，然后将这些数据对应的 URL 公开在英特网上，所有人就可以使用这个 URL 访问或下载这些公开数据了。

操作步骤

步骤 1 登录 OBS 管理控制台，在页面右上角单击“创建桶”创建一个新的桶。

步骤 2 在桶列表中单击新创建的桶的“桶名称”，进入对象页面，然后将需要存储的地图数据作为对象上传至新创建好的桶中。

步骤 3 单击待操作的对象的“名称”，进入对象详情页。

步骤 4 在“对象 ACL>公共访问权限”中，单击“编辑”为匿名用户设置对象的读取权限，如图 2-27 所示。

图2-27 为匿名用户设置对象的读取权限

步骤 5 单击“确定”。

----结束

验证

步骤 1 权限设置成功后单击对象，页面上“链接”显示该对象的共享链接地址。将“链接”中对象对应的 URL 公布到英特网上，英特网所有用户便可以访问或下载该对象。

步骤 2 匿名用户将对应的 URL 复制到浏览器，则可以访问到对象。

----结束

2.9.9.6 为匿名用户设置文件夹的访问权限

当一个文件夹下的对象都需要授权匿名用户访问权限时，可以通过桶策略和对象策略配置授予匿名用户访问文件夹内对象的权限。本示例以桶策略为例，对象策略方法的区别在于，对象策略是直接选中待配置的文件夹配置对象策略，其他参数设置一致。

操作步骤

步骤 1 在桶列表单击待操作的桶，进入“对象”页面。

步骤 2 在左侧导航栏，单击“访问权限控制 > 桶策略”。

步骤 3 单击“创建”。

步骤 4 在桶策略模板第一行，单击右侧的“自定义创建”。

步骤 5 配置如下参数。

表2-29 为匿名用户设置文件夹的访问权限

参数		说明
策略配置方式		可视化视图
策略名称		自定义
策略内容	允许/拒绝	允许
	被授权用户	• 授权用户：匿名用户 • 用户策略：包含以上用户
	资源	• 资源范围：桶内对象，选择指定对象 • 资源路径：配置为需要访问的文件夹内的所有对象，如文件夹名称为“folder-001”时，资源路径为“folder-001/*”。 • 资源策略：包含以上资源
	动作	• 选择动作：GetObject • 操作策略：包含以上动作

步骤 6 单击右下角的“配置确认”，确认桶策略信息是否正确。

步骤 7 单击右下角的“创建”，完成桶策略创建。

----结束

验证

步骤 1 权限设置成功后，在文件夹中选择一个对象，单击对象，页面上“链接”显示该对象的共享链接地址。将“链接”中对象对应的 URL 公布到英特网上，英特网所有用户便可以访问或下载该对象。

步骤 2 匿名用户将对应的 URL 复制到浏览器，则可以访问到对象。

----结束

2.10 多版本控制

2.10.1 多版本控制简介

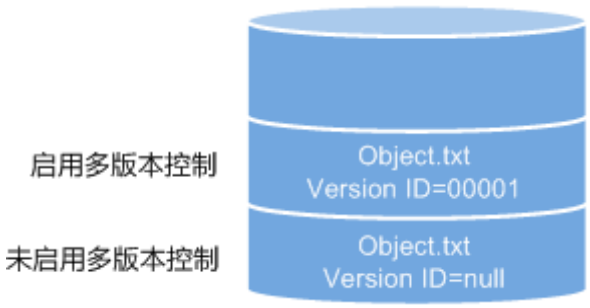
利用多版本控制，您可以在一个桶中保留多个版本的对象，使您更方便地检索和还原各个版本，在意外操作或应用程序故障时快速恢复数据。

默认情况下，OBS 中新创建的桶不会开启多版本功能，向同一个桶上传同名的对象时，新上传的对象将覆盖原有的对象。

开启多版本控制

- 桶中已有对象版本 ID（空）和内容都不会变化。再次上传该同名对象，对象版本示意图如图 2-28 所示。

图2-28 多版本对象示意图（已有对象）



- 新上传对象，OBS 自动为每个对象创建唯一的版本号。上传同名的对象将以不同的版本号同时保存在 OBS 中，如图 2-29 所示。

图2-29 多版本对象示意图（新对象）

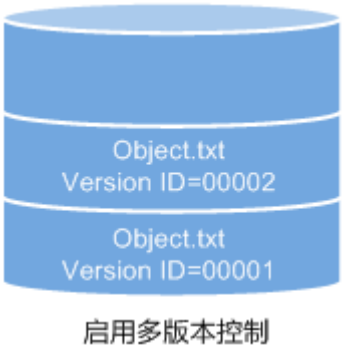
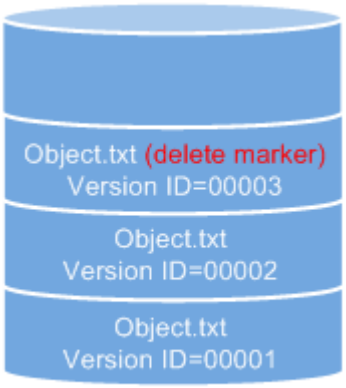


表2-30 版本说明

版本	描述
最新版本	多版本控制开启后，同名对象多次操作，每次操作都会对应一个版本号进行保存。最后一次操作保存的版本号，为最新版本。
历史版本	多版本控制开启后，同名对象多次操作，每次操作都会对应一个版本号进行保存。除最后一次外的，其他保存的版本号为历史版本。

- 列出桶内对象列表时默认列出最新对象列表。
- 可以指定版本号下载对象，不指定版本号默认下载最新的对象。详细操作请参见配置多版本控制的相关操作。
- 可以选中目标对象，并单击右侧的“删除”删除对象。对象被删除后，OBS 将插入一个删除标记，对象在“已删除对象”列表中呈现。详细操作请参见删除对象或文件夹。此时若访问该对象，会返回 404 错误。

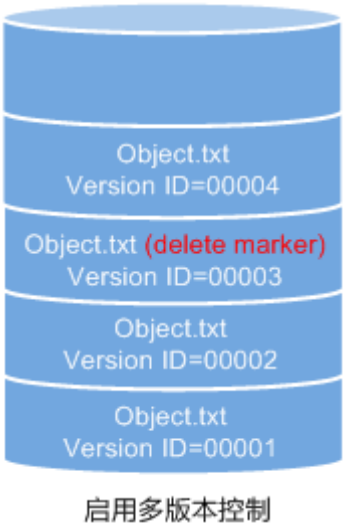
图2-30 删除标记示意图



- 删除带删除标记的对象可恢复该对象。详细操作请参见取消删除对象的相关操作。
- 在“已删除对象”列表，选中对象，可指定版本号彻底删除指定版本对象。详细操作请参见删除对象或文件夹的相关操作。
- 一个对象只会显示在对象列表或已删除对象列表中，不会同时出现。

  例如，上传一个对象 A 后，将其删除，对象 A 将显示在已删除对象列表中。若再次上传同名对象 A，同名对象 A 会显示在对象列表中，显示在已删除对象列表中的原对象 A 将不会存在。对象 A 版本示意图如图 2-31 所示。

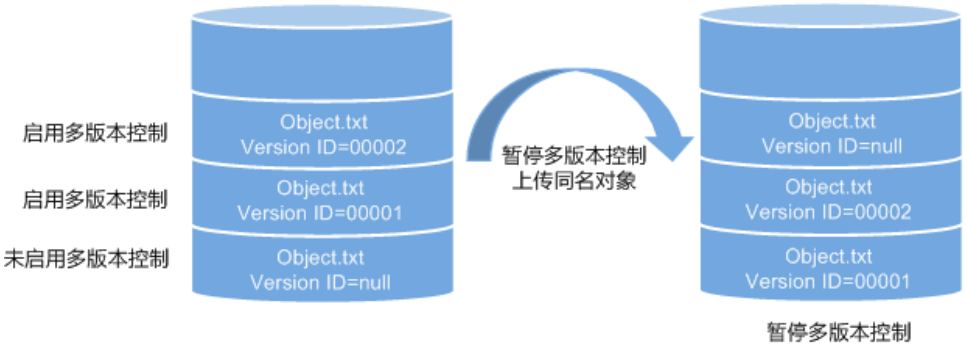
图2-31 删除后再上传同名对象的版本示意图



暂停多版本控制

多版本控制一旦启动，不可以关闭，只能暂停使用。暂停后，新上传的对象版本号为空。若之前有空版本号的同名对象，则会覆盖该带空版本号的对象。

图2-32 暂停多版本控制后的对象版本示意图



当不需要对桶内对象进行版本控制时，可以暂停多版本控制：

- 历史版本将继续保留在 OBS 中，若这些历史版本你不再需要，请手动删除。
- 仍可以指定版本号下载对象，不指定版本号默认下载最新的对象。

暂停与未启用的区别

暂停多版本控制后，删除对象时，无论此对象是否存在历史版本，将会产生一个删除标记。而未启用多版本控制时，则不会产生删除标记。

2.10.2 配置多版本控制

操作步骤

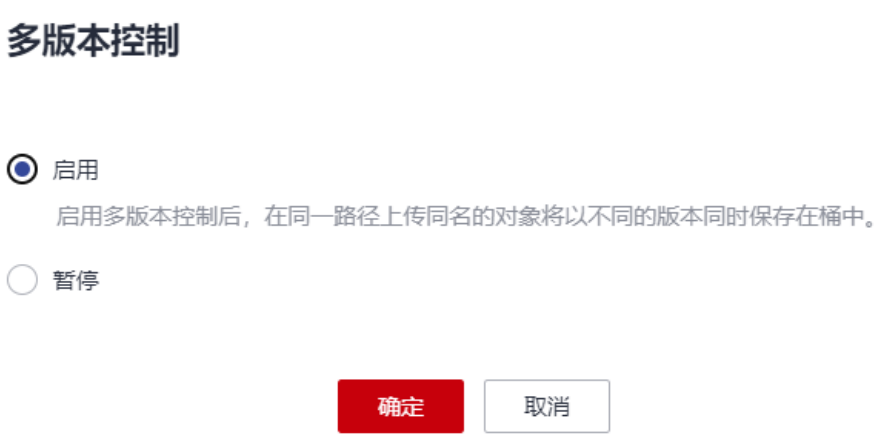
步骤 1 在桶列表单击待操作的桶，进入“对象”页面。

步骤 2 在左侧导航栏，单击“概览”进入“概览”页面。

步骤 3 单击“基本信息”区域“多版本控制”参数后面的“编辑”，系统弹出多版本控制对话框。

步骤 4 选择“启用”，如图 2-33 所示。

图2-33 多版本控制



步骤 5 单击“确定”，启用目标桶中对象的多版本控制。

步骤 6 单击待查看的对象，进入对象详情页面。在“版本”页签，查看一个对象的多个版本。

----结束

相关操作

开启多版本控制后，进入对象详情页面，在“版本”页签，可以对多版本对象进行删除、下载操作。

步骤 1 在桶列表单击待操作的桶，进入“对象”页面。

步骤 2 在“对象”列表，单击待操作的对象，进入对象详情页面。

步骤 3 在“版本”页签，显示该对象的所有版本。

步骤 4 对多版本对象可做以下操作。

1. 在待操作版本对象右侧，单击“下载”，可下载该版本对象。

2. 在待操作版本对象右侧，单击“删除”，将永久删除该版本对象，不可恢复。若删除的是最新版本的对象，那么时间最近的历史版本将变成新的最新版本。

----结束

2.11 日志记录

2.11.1 访问日志记录简介

出于分析或审计等目的，用户可以开启日志记录功能。通过访问日志记录，桶的拥有者可以深入分析访问该桶的用户请求性质、类型或趋势。当用户开启一个桶的日志记录功能后，OBS 会自动对这个桶的访问请求记录日志，并生成日志文件写入用户指定的桶（即目标桶）中。

当日志记录开启后，目标存储桶的日志投递用户组会同步开启桶的写入权限和 ACL 读取权限。若手动将日志投递用户组的桶写入权限和 ACL 读取权限关闭，桶的日志记录会失败。

OBS 支持对桶的访问请求创建并保存访问日志记录，可用于进行请求分析或日志审计。

由于日志存储在 OBS 中也会占用用户的 OBS 存储空间，即意味着将产生额外的存储费用，默认情况下，OBS 不会为用户的桶收集访问日志。

由于日志文件是 OBS 产生，并且由 OBS 上传到存放日志的桶中，因此 OBS 需要获得委托授权，用于上传生成的日志文件。所以在配置桶日志记录前，需要先到统一身份认证服务生成一个对 OBS 服务的委托，并在配置日志记录时添加该委托。默认情况下，在为委托配置权限时只需设置日志存储桶的上传对象（PutObject）权限，示例如下（其中 mybucketlogs 为日志存储桶的桶名）。如果日志存储桶开启了默认加密功能，还需要委托同时具有日志存储桶所在区域的 KMS Administrator 权限。

```
{
   "Version": "1.1",
   "Statement": [
      {
         "Action": [
            "obs:object:PutObject"
         ],
         "Resource": [
            "OBS:*:*:object:mybucketlogs/*"
         ],
         "Effect": "Allow"
      }
   ]
}
```

日志记录设置成功后，大约 15 分钟后可在日志存储目标桶中查看到桶的操作日志。

以下所示为在目标桶生成的桶访问日志文件记录：

```
787f2f92b20943998a4fe2ab75eb09b8 bucket [13/Aug/2015:01:43:42 +0000] xx.xx.xx.xx
787f2f92b20943998a4fe2ab75eb09b8 281599BACAD9376ECE141B842B94535B
```

```
REST.GET.BUCKET.LOCATION
- "GET /bucket?location HTTP/1.1" 200 - 211 - 6 6 "-"  "HttpClient" - -
```

每个桶访问日志都包含以下信息：

表2-31 Bucket Logging 格式

名称	示例	含义
BucketOwner	787f2f92b20943998a4fe2ab75eb09b8	桶的 ownerId
Bucket	bucket	桶名
Time	[13/Aug/2015:01:43:42 +0000]	请求时间戳（UTC）
Remote IP	xx.xx.xx.xx	请求 IP
Requester	787f2f92b20943998a4fe2ab75eb09b8	请求者 ID
RequestID	281599BACAD9376ECE141B842B94535B	请求 ID
Operation	REST.GET.BUCKET.LOCATION	操作名称
Key	-	对象名
Request-URI	GET /bucket?location HTTP/1.1	请求 URI
HTTPStatus	200	返回码
ErrorCode	-	错误码
BytesSent	211	HTTP 响应的字节大小
ObjectSize	-	对象大小（bytes）
TotalTime	6	服务端处理时间（ms）
Turn-AroundTime	6	总请求时间（ms）
Referer	-	请求的 referrer 头域
User-Agent	HttpClient	请求的 user-agent 头域
VersionID	-	请求中带的 versionId
STSLogUrn	-	联邦认证及委托授权信息

2.11.2 配置桶的日志记录

当一个桶开启了日志记录功能后，OBS 自动将该桶的日志按照固定的命名规则，生成一个对象写入用户指定的桶。

操作步骤

步骤 1 在桶列表单击待操作的桶，进入“对象”页面。

步骤 2 在左侧导航栏，单击“概览”，进入“概览”页面。

步骤 3 在“基础配置”区域下，单击“日志记录”卡片，系统弹出“日志记录”对话框。

步骤 4 选择“启用”，如图 2-34 所示。

图2-34 日志记录

步骤 5 选择“日志存储桶”（已经存在的桶），指定日志文件生成后将上传到哪个桶中。选定的日志存储桶的日志投递用户组会自动被赋予读取 ACL 权限和桶的写入权限。

步骤 6 设置“日志文件前缀”，指定日志文件的前缀。

启用日志记录功能后，生成的日志文件根据如下规则命名：

<*日志文件前缀*>YYYY-mm-DD-HH-MM-SS-<*UniqueString*>

- <*日志文件前缀*>为用户指定的日志文件日志存储前缀。
- **YYYY-mm-DD-HH-MM-SS** 为日志生成的日期与时间，各字段依次表示年、月、日、时、分、秒。
- <*UniqueString*>为 OBS 自动生成的字符串。

在管理控制台上，如果配置的目标前缀<*日志文件前缀*>以斜杠/结尾，则该桶生成的日志文件在目标桶中将统一存放在以<*日志文件前缀*>命名的文件夹中，方便您进行管理。

例如：

- 如果配置日志存储桶为 **bucket**，日志文件前缀为 **bucket-log/**，则所有日志都将保存在 **bucket** 内的文件夹 **bucket-log** 中。日志命名举例：**2015-06-29-12-22-07-N7MXLAF1BDG7MPDV**。
- 如果配置日志存储桶为 **bucket**，日志文件前缀为 **bucket-log**，则所有日志都将直接保存在 **bucket** 中。日志命名举例：**bucket-log2015-06-29-12-22-07-N7MXLAF1BDG7MPDV**。

步骤 7 选择“IAM 委托”，给 OBS 授予上传日志文件到日志存储桶的权限。

默认情况下，在为委托配置权限时只需设置日志存储桶的上传对象（PutObject）权限，示例如下（其中 mybucketlogs 为日志存储桶的桶名）。如果日志存储桶开启了默认加密功能，还需要委托同时具有日志存储桶所在区域的 KMS Administrator 权限。

```
{
   "Version": "1.1",
   "Statement": [
      {
         "Action": [
            "obs:object:PutObject"
         ],
         "Resource": [
            "OBS:*:*:object:mybucketlogs/*"
         ],
         "Effect": "Allow"
      }
   ]
}
```

您可以从下拉列表选择帐号下已有的 IAM 委托，也可以单击“创建委托”去创建一个新的委托。创建委托的方法，请参见创建 IAM 委托。

步骤 8 单击“确定”。

日志记录设置成功后，大约 15 分钟后可在日志存储桶中查看到桶的操作日志。

----结束

相关操作

若您不再需要记录日志，在“日志记录”对话框，勾选“关闭”后，单击“确定”。关闭“日志记录”后，日志不再保存，之前保存的日志仍然在目标桶。

2.12 标签

2.12.1 标签简介

标签用于标识 OBS 中的桶，以此来达到对 OBS 中的桶进行分类的目的。

当为桶添加标签时，该桶上所有请求产生的计费话单里都会带上这些标签，从而可以针对话单报表做分类筛选，进行更详细的成本分析。例如：某个应用程序在运行过程会往桶里上传数据，我们可以用应用名称作为标签，设置到被使用的桶上。在分析话单时，就可以通过应用名称的标签来分析此应用的成本。

OBS 以键值对的形式来描述标签。一个桶默认最大拥有 10 个标签。每个标签有且只有一对键值。

键和值可以任意顺序出现在标签中。同一个桶标签的键不能重复，但是值可以重复，并且可以为空。

2.12.2 配置桶标签

您可以在创建桶时，配置其标签，详见创建桶。您也可以在桶创建后，再配置其标签。本章节介绍桶创建后标签的配置方法。

操作步骤

步骤 1 在桶列表单击待操作的桶，进入“对象”页面。

步骤 2 在左侧导航栏，单击“概览”，进入“概览”页面。

步骤 3 在“基础配置”区域下，单击“标签”卡片，系统跳转至“标签”界面。

或您可以直接在左侧导航栏单击“基础配置>标签”，进入“标签”界面。

步骤 4 单击“添加标签”，系统弹出“添加标签”对话框。

图2-35 添加标签

步骤 5 按照表 2-32 要求输入标签的键和值。

表2-32 参数说明

参数	说明
标签键	输入标签的键，同一个桶标签的键不能重复。可以自定义，也可以选择预先在标签管理服务（TMS）创建好的标签。 命名规则如下： • 长度范围为 1 到 36 个字符。区分大小写。 • 不能以空格开头或结尾，不能包含以下字符：=*<>\,|/
标签值	输入标签的值，标签的值可以重复，并且可以为空。 命名规则如下： • 长度范围为 0 到 43 个字符。区分大小写。 • 不能包含以下字符：=*<>\,|/

步骤 6 单击“确定”。

设置桶标签后，大约需要等待 3 分钟才能生效。

----结束

相关操作

您可以单击“编辑”，修改标签的“值”；也可以单击“删除”，删除标签。

2.13 跨区域复制（适用存量客户）

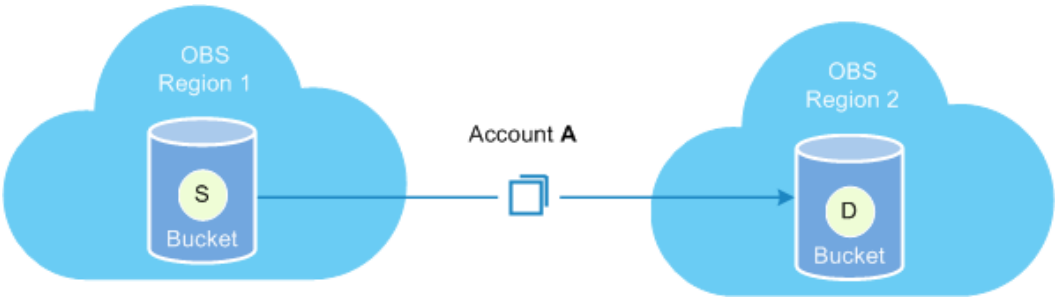
2.13.1 跨区域复制简介

跨区域复制能够为用户提供跨区域数据容灾的能力，满足用户数据复制到异地进行备份的需求。

跨区域复制是指通过创建跨区域复制规则，将一个桶（源桶）中的数据自动、异步地复制到不同区域的另外一个桶（目标桶）中，源桶和目标桶必须属于同一个帐号，暂不支持跨帐号复制。

在配置跨区域复制规则时，您可以按前缀匹配请求复制部分对象，也可以请求复制桶中的所有对象。复制到目标桶的对象是源桶中对象的精确副本。它们具有相同的对象名称和元数据，包括：对象内容、大小、最后修改时间、创建者、版本号、用户定义的元数据以及 ACL。

图2-36 跨区域复制示意图



复制的内容

启用跨区域复制规则后，符合以下条件的对象会复制到目标桶中：

- 新上传的对象。
- 有更新的对象，比如对象内容有更新，或者某一对象跨区域复制成功后源桶对象ACL 设置有更新。

适用场景

- 客户需要在多地访问相同的 OBS 资源。为了最大限度缩短访问对象时的延迟，您可以使用跨区域复制，在离客户较近的区域中创建对象副本。
- 由于业务原因，您需要将 OBS 数据从一个区域的数据中心迁移至另一个区域的数据中心。
- 出于对数据安全性以及可用性的考虑，您希望对所有写入 OBS 的数据，都在另一个区域的数据中心显式地创建一个备份，以防止在数据发生不可逆损毁时，有安全、可用的备份数据。

约束与限制

在使用跨区域复制过程中，存在如下的约束与限制：

- 桶版本号为 3.0 及以上的桶支持跨区域复制功能。桶版本号可以在 OBS 管理控制台上，进入桶概览页后，在“基本信息”中查看。
- 启用跨区域复制功能之前上传的对象，不会被复制到目标桶。
- 源桶和目标桶必须属于不同的区域，同区域的桶不能进行数据复制。
- 源桶和目标桶的多版本控制状态必须保持一致。
- 源桶中的对象只能被复制到一个目标桶中，且复制过去的对象不能再被复制到另外一个目标桶。例如有两个不同区域的桶 A 和桶 B，桶 A 数据可以复制到桶 B 中，桶 B 数据也可以复制到桶 A 中，但桶 B 中存储的桶 A 数据的副本不会复制，同理桶 A 中存储的桶 B 数据的副本也不会复制。
- 当且仅当源桶、目标桶多版本控制状态开启，在源桶中不指定版本删除对象时，目标桶会同步删除此对象；除此之外，删除源桶对象时，目标桶默认不会同步删除操作。

- 在启用跨区域复制过程中，若您修改目标桶的多版本控制状态，会导致对象复制失败；若您尝试修改源桶多版本控制状态，必须先删除复制配置，然后才能进行修改。
- 源桶或目标桶都需要一直保证桶拥有者具有读写权限，以确保数据能够成功同步。如果源桶或目标桶的读写权限错误，导致系统没有读源对象或者写目标对象的权限，这种对象将一直复制不成功，即使将权限修改正确后，也不会重新复制。
- 同一个源桶只能创建一条复制所有对象的跨区域复制规则，或多条（最多 100 条）按前缀匹配的跨区域复制规则。
- OBS 目前仅支持一个源桶同时复制到一个目标桶，不支持一个源桶同时复制到多个目标桶。允许修改目标桶，但修改目标桶会更改所有已创建规则的目标桶。
- 在启用跨区域复制过程中，若您删掉 OBS 云服务委托，会导致对象复制状态为 FAILED。
- 不建议您对目标桶中的副本对象进行删除、覆盖或者修改 ACL 操作，此类操作可能导致目标桶中对象最新版本或者对象访问控制权限与源区域不一致。
- 如果已复制成功的源对象的 ACL 发生变化，在该对象匹配的复制策略未发生变化的情况下，这些变化会同步复制到对象副本，但已复制成功的历史对象不会同步源对象的 ACL 变化。

2.13.2 配置跨区域复制

当前，OBS 支持一个源桶到一个目标桶配置一条复制所有对象的跨区域复制规则，或多条按前缀匹配的跨区域复制规则。

说明

跨区域复制不保证时效性，配置跨区域复制规则后，可能会出现对象不会立即进行复制的情况，请耐心等待。

前提条件

源桶的版本号为 3.0 及以上，并且源桶所在区域支持跨区域复制功能。

操作步骤

步骤 1 在桶列表单击待操作的桶，进入“对象”页面。

步骤 2 在左侧导航栏，单击“跨区域复制”。

步骤 3 单击“创建规则”，系统将弹出“创建跨区域复制规则”对话框。

图2-37 创建跨区域复制规则

步骤 4 根据业务规划配置跨区域复制规则，参数的详细说明如表 2-33 所示。

表2-33 跨区域复制规则参数

参数		说明
状态		选择启用或者禁用当前规则。源桶和目标桶的多版本控制状态必须保持一致。
源桶	复制对象	在源桶中选择要复制的对象。 • 所有对象：复制所有对象到目标桶。 • 按前缀匹配：复制具有相同前缀的对象到目标桶。
	前缀	• 按前缀匹配对象时，输入的对象名前缀不能为空，长度限制为 1024 个字符。 • 当按前缀配置时，如果指定的前缀名与某条已配置的规则指定的前缀名存在包含关系，OBS 会将两条规则视为同一条，而禁止您配置本条规则。例如，系统中已存在指定前缀名为“abc”的规则，则不允许再配置指定前缀以“abc”字段开头的规则。 • 如果要复制文件夹，对象名前缀需要使用/作为最后一个字符（例如，imgs/）。
	同步历史对象	选择是否将创建本规则前已经存在于桶中的对象同步复制到目标桶，默认不同步。

参数		说明
目标桶	区域	选择目标桶所在区域，目标桶需要与源桶处于不同区域。
	桶	选择目标桶。
	修改复制对象的存储类别	默认不勾选，即保持与源桶中对象的存储类别一致。勾选后可以配置复制到目标桶的对象的存储类别。
权限	复制使用 KMS 加密的对象	不论是否勾选，OBS 均会尝试复制 KMS 加密对象。 • 若勾选该项，下方的“IAM 委托”仅会展示全局项目下配置了任意权限，并且源桶和目标桶区域均配置了 KMS Administrator 或 Tenant Administrator 权限的 OBS 云服务委托。 • 若不勾选该项，下方的“IAM 委托”仅会展示全局项目下配置了任意权限，且源桶或目标桶区域不包含 KMS Administrator 或 Tenant Administrator 权限的 OBS 云服务委托。 如果目标区域没有启用 KMS 服务或者委托中没有赋予源桶和目标桶所在区域“KMS Administrator”权限，则源桶中 KMS 加密对象会复制失败，导致对象复制状态为 FAILED。 源桶中以任意 KMS 密钥加密的对象，复制到目标桶后都会以目标桶所在区域的默认密钥“obs/default”进行加密。
	IAM 委托	将您资源的操作权限委托给 OBS，OBS 使用此委托执行对象的跨区域复制。 第一次使用时，您需要单击“查看 IAM 委托”去创建一个新的委托用于跨区域复制。如果已经创建，可以从下拉列表中选择。 **说明** 委托要求： 此 IAM 委托必须为“对象存储服务 OBS”的云服务委托。其中“对象存储服务”项目需要具有“OBS Administrator”权限。如果勾选了“复制使用 KMS 加密的对象”，源桶和目标桶所在区域还需要具有“KMS Administrator”权限。

步骤 5 （可选）创建 IAM 委托，参见创建 IAM 委托。

步骤 6 单击“确定”，完成跨区域复制规则创建。

----结束

2.14 生命周期管理

2.14.1 生命周期管理简介

生命周期管理是指通过配置指定的规则，实现定时删除桶中的对象。

生命周期管理可适用于以下典型场景：

- 周期性上传的日志文件，可能只需要保留一个星期或一个月。到期后要删除它们。

对于上述场景中的对象，您可以定义用于识别这些对象的生命周期管理规则，通过这些规则实现对象的生命周期管理。

生命周期管理规则通常包含两个关键要素：

- 策略：即您可以指定对象名前缀来匹配受约束的对象，则匹配该前缀的对象将受规则影响；也可以指定将生命周期管理规则配置到整个桶，则桶内所有对象都将受规则影响。
- 过期删除：即您可以指定在对象最后一次更新后多少天，受规则影响的对象将过期并自动被 OBS 删除。

2.14.2 配置生命周期规则

您可以为某个桶或某些对象设置生命周期规则。同时，您也可以指定对象过期删除。

操作步骤

步骤 1 在桶列表单击待操作的桶，进入“对象”页面。

步骤 2 在左侧导航栏，单击“概览”，进入“概览”页面。

步骤 3 在“基础配置”区域下，单击“生命周期规则”卡片，系统跳转至“生命周期规则”界面。

或您可以直接在左侧导航栏单击“基础配置>生命周期规则”，进入“生命周期规则”界面。

步骤 4 单击“创建”，系统弹出如图 2-38 所示对话框。

图2-38 创建生命周期规则

步骤 5 配置生命周期管理规则。

基本信息：

- “状态”：选中“启用”，启用本条生命周期规则。
- “规则名称”：用于识别不同的生命周期配置，其长度需不超过 255 字符。
- “前缀”：可选。
  - 填写前缀：满足该前缀的对象将受生命周期规则管理，输入的对象前缀不能包括\:*?"<>|特殊字符，不能以/开头，不能两个/相邻。
  - 未填写前缀：桶内所有对象都将受生命周期规则管理。

说明

- 当按前缀配置时，如果指定的前缀名与某条已配置的生命周期规则指定的前缀名存在包含关系，OBS 会将两条规则视为同一条，而禁止您配置本条规则。例如，系统中已存在指定前缀名为“abc”的规则，则不允许再配置指定前缀以“abc”字段开头的规则。
- 如果已存在按前缀配置的生命周期规则，则不允许再新增配置到整个桶的规则。

当前版本或历史版本：

- 若桶未启用“多版本控制”，仅可配置“当前版本”。
- 若桶开启过“多版本控制”，配置界面可见“当前版本”和“历史版本”。

  “历史版本”配置项默认不展示，只有当桶开启过“多版本控制”，即多版本控制状态为“已启用”或“暂停”时才会展示。

说明

- “当前版本”与“历史版本”是针对“多版本控制”而言的。若开启了“多版本控制”功能，同名的对象上传到同一路径下时，则会产生不同的版本号。最新版本的对象称之为“当前版本”，历史时间上传的对象称之为“历史版本”。
- “当前版本”与“历史版本”至少配置一个，也可以两个版本同时配置。

- 转换为低频访问存储天数：指定在对象最后一次更新后多少天，受规则影响的对象将转换为低频访问存储。至少设置为 30 天。
- 对象过期删除天数：指定在对象最后一次更新后多少天，受规则影响的对象将过期并自动被 OBS 删除。

例如，您于 2015 年 1 月 7 日在 OBS 中存储了以下几个文件：

- log/test1.log
- log/test2.log
- doc/example.doc
- doc/good.txt

您于 2015 年 1 月 10 日在 OBS 中存储了以下几个文件：

- log/clientlog.log
- log/serverlog.log
- doc/work.doc
- doc/travel.txt

若您在 2015 年 1 月 10 日设置前缀为“log”的对象，过期删除的时间设置为一天，可能出现如下情况：

- 1 月 7 日上传的两个对象“log/test1.log”和“log/test2.log”，会在最近一次系统自动扫描后被删除，可能在 1 月 10 日当天，也可能在 1 月 11 日，这取决于系统的下一次扫描在何时进行。
- 1 月 10 日上传的两个对象“log/clientlog.log”和“log/serverlog.log”，每下一次系统扫描均会判断距上一次对象更新是否已满一天。如果已满一天，则在本次扫描时删除；如果未满一天，则会等到下次扫描再判断，直到满一天时删除，一般可能在 1 月 11 日或 1 月 12 日删除。

说明

对象上传后，系统会将下一个 UTC 零点作为对象存储的起始时间开始计算生命周期。生命周期规则执行最长耗时 24 小时。因此，过期被删除可能会存在延时，且一般不会超过 48 小时。配置生命周期规则后，如果期间修改了生命周期配置，会重新计算生效时间。

步骤 6 单击“确定”，完成生命周期规则配置。

----结束

复制生命周期规则

步骤 1 在桶列表单击待操作的桶，进入“对象”页面。

步骤 2 在左侧导航栏，单击“概览”，进入“概览”页面。

步骤 3 在“基础配置”区域下，单击“生命周期规则”卡片，系统跳转至“生命周期规则”界面。

或您可以直接在左侧导航栏单击“基础配置>生命周期规则”，进入“生命周期规则”界面。

步骤 4 单击“更多 > 复制”。

步骤 5 选择复制源，即生命周期规则所在的源桶。

说明

- 从源桶复制生命周期规则的操作为增量复制，不会删除当前桶已存在的生命周期规则，与已存在的生命周期规则冲突的规则不会复制。
- 源桶和目标桶的桶版本号都必须是 3.0。
- 您可以按需移除不需要复制的生命周期规则。

图2-39 复制生命周期规则

步骤 6 单击“确定”，将源桶的生命周期规则复制到当前桶。

----结束

后续操作

若您需修改生命周期的内容，请单击该生命周期规则所在行右侧的“编辑”进行编辑；单击“禁用”，可以禁用该生命周期规则，单击“启用”，可启用该生命周期规则。

您可以选中多条生命周期规则，单击列表上方的“禁用”或“启用”，批量“禁用”或“启用”生命周期规则。

2.15 静态网站托管

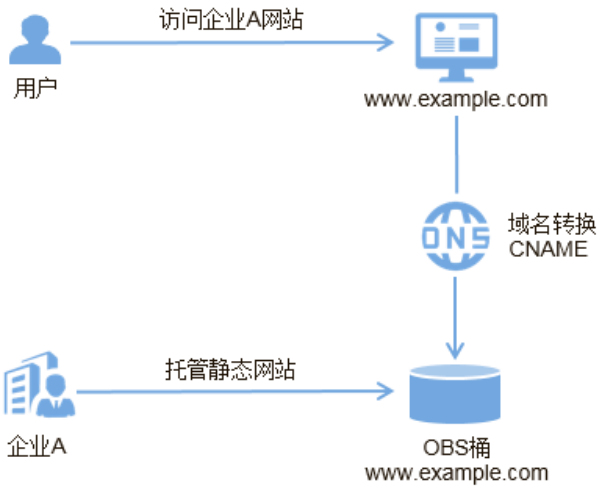
2.15.1 静态网站托管简介

您可以将静态网站文件上传至 OBS 的桶中，并对这些文件赋予匿名用户可读权限，然后将该桶配置成静态网站托管模式，就可以实现在 OBS 上托管静态网站了。

静态网站通常仅包含静态网页，以及可能包含部分可在客户端运行的脚本，如 JavaScript、Flash 等。相比之下，动态网站则依赖于服务器端处理脚本，包括 PHP、JSP 或 ASP.Net 等。OBS 当前尚不支持服务器端运行脚本。

静态网站托管配置会在两分钟内生效。在 OBS 上托管静态网站配置生效后，您可以通过静态网站托管的访问域名访问该静态网站。

图2-40 静态网站示意图



2.15.2 重定向简介

在使用静态网站托管功能时，OBS 还支持配置重定向请求，即您可以将特定的请求或所有请求实施重定向。

当网站结构调整、网站地址变化或者网站的扩展名发生变化时，用户使用旧的网站地址（比如收藏夹中的地址）访问网站会访问失败，用户只能得到 404 页面错误信息。此时网站配置了重定向后，让访问这些域名的用户跳转到设定的页面以避免 404 错误访问。

重定向典型的应用场景包括：

- 重定向所有请求到另外一个站点。
- 设定特定的重定向规则，对特定的请求实施重定向。

2.15.3 配置静态网站托管

用户可将自己的桶配置成静态网站托管模式，并通过桶域名访问该静态网站。

静态网站托管配置会在两分钟内生效。

前提条件

静态网站所需的网页文件已上传到指定桶中。

桶内的静态网站文件必须配置为匿名用户可访问。

操作步骤

步骤 1 在桶列表单击待操作的桶，进入“对象”页面。

步骤 2 **可选**：如果还未将桶内静态网站文件配置为匿名用户可访问，请执行本步骤配置匿名访问权限。如果已经配置，请跳过此步骤。

若桶中只有静态网站文件，则配置桶策略为“公共读”，使桶内所有文件能被公开访问。

1. 单击“访问权限控制>桶策略”。
2. 单击“创建”。
3. 单击“公共读”模板右侧的“使用模板创建”。

图2-41 配置公共读权限

4. 无需修改桶策略模板内容，直接单击“配置确认”后再单击“创建”，完成桶策略创建。

步骤 3 在左侧导航栏，单击“概览”，进入“概览”页面。

步骤 4 在“基础配置”区域下，单击“静态网站托管”卡片，系统跳转至“静态网站托管”界面。

或您可以直接在左侧导航栏单击“基础配置>静态网站托管”，进入“静态网站托管”界面。

步骤 5 单击“配置静态网站托管”，系统弹出“配置静态网站托管”对话框。

步骤 6 “状态”设置为使能状态。

步骤 7 “托管模式”选择“配置到当前桶”，如图 2-42 所示。

图2-42 配置静态网站托管

步骤 8 在“默认首页”、“默认 404 错误页面”中设置默认缺省页面和 404（Not Found）页面。

- 默认首页：即访问静态网站时的默认首页。当使用 OBS 管理控制台配置静态网站托管时，仅支持“html”格式的网页文件；当使用 API 的方式配置时，OBS 不进行限制，用户必须指定对象的“Content-Type”。

  OBS 仅支持配置桶根目录下的文件（如“index.html”）作为默认首页，暂不支持按目录层级的方式（如“/page/index.html”）配置默认首页。
- 默认 404 错误页面：即访问静态网站遇到错误时，OBS 返回给用户的错误页面。当使用 OBS 管理控制台配置静态网站托管时，仅支持桶根目录下 html、jpg、png、bmp、webp 格式的文件；当使用 API 的方式配置时，OBS 不进行限制，用户必须指定对象的“Content-Type”。

步骤 9 **可选**：在“重定向规则”中配置重定向规则。满足重定向规则的请求将被重定向到指定主机或页面。

“重定向规则”采用 JSON 或 XML 格式编写，可以包含多条重定向规则，每条重定向规则包含一个 Condition 和一个 Redirect，参数说明如所示。

表2-34 参数说明

容器	键值	键值说明
Condition	KeyPrefixEquals	重定向生效时的对象名前缀。当向对象发送请求时，如果对象名前缀等于这个值，那么重定向生效。 例如：重定向 ExamplePage.html 对象的请求，KeyPrefixEquals 设为 ExamplePage.html。
	HttpErrorCodeReturnedEquals	重定向生效时的 HTTP 错误码。当发生错误时，如果错误码等于这个值，那么重定向生效。 例如：当返回的 HTTP 错误码为 404 时重定向到 NotFound.html，可以将 Condition 中的 HttpErrorCodeReturnedEquals 设置为 404，Redirect 中的 ReplaceKeyWith 设置为 NotFound.html。
Redirect	Protocol	重定向请求生效时使用的协议。取值为 **http** 或 **https**，如不设置，默认为 **http**。
	HostName	重定向请求生效时使用的主机名。如不设置，代表重定向至原请求的 HostName。
	ReplaceKeyPrefixWith	重定向请求生效时使用的对象名前缀。
	ReplaceKeyWith	重定向请求生效时使用的对象名。
	HttpRedirectCode	响应中的 HTTP 状态码。默认值为 301，表示永久重定向到 Redirect 指定的位置，也可根据业务实际情况设置。

重定向规则示例

- 示例一：对所有前缀为“folder1/”对象的请求，自动重定向至主机“www.example.com”上前缀为“target.html”的页面，并使用 https 协议。

```
[
    {
    "Condition": {
         "KeyPrefixEquals": "folder1/"
         },
    "Redirect":{
         "Protocol": "https",
         "HostName": "www.example.com",
         "ReplaceKeyPrefixWith": "target.html"
         }
    }
]
```

- 示例二：对所有前缀为“folder2/”对象的请求，自动重定向至本 OBS 桶中前缀为“folder/”的对象上。

```
[
    {
    "Condition": {
         "KeyPrefixEquals": "folder2/"
         },
    "Redirect":{
         "ReplaceKeyPrefixWith": "folder/"
         }
    }
]
```

- 示例三：对所有前缀为“folder.html”对象的请求，自动重定向至本 OBS 桶的“folderdeleted.html”对象上。

```
[
    {
    "Condition": {
         "KeyPrefixEquals": "folder.html"
         },
    "Redirect":{
         "ReplaceKeyWith": "folderdeleted.html"
         }
    }
]
```

- 示例四：在未找到请求对象返回 HTTP 状态码 404 时，自动重定向至主机“www.example.com”上前缀为“report-404/” 的页面。

  例如，如果您请求页面 ExamplePage.html，且它导致了 HTTP 404 错误，该请求将重定向至 www.example.com 上的 report-404/ExamplePage.html 页面。如果没有设置 404 的重定向规则，在发生 HTTP 404 错误时将返回上一步中配置的默认 404 错误页面。

```
[
    {
    "Condition": {
         "HttpErrorCodeReturnedEquals": "404"
         },
    "Redirect":{
         "HostName": "www.example.com",
         "ReplaceKeyPrefixWith": "report-404/"
         }
    }
]
```

步骤 10 单击“确定”。

在 OBS 上托管静态网站配置生效后，您可以通过静态网站托管访问域名访问该静态网站。

说明

由于浏览器缓存等原因，您可能需要清除浏览器缓存后才能查看到预期效果。

----结束

2.15.4 配置重定向请求

若需将该桶的所有请求重定向至其他桶或 URL，可以配置重定向请求。

前提条件

静态网站所需的网页文件已上传到指定桶中。

桶内的静态网站文件必须配置为匿名用户可访问。

操作步骤

步骤 1 在桶列表单击待操作的桶，进入“对象”页面。

步骤 2 在左侧导航栏，单击“概览”，进入“概览”页面。

步骤 3 在“基础配置”区域下，单击“静态网站托管”卡片，系统跳转至“静态网站托管”界面。

或您可以直接在左侧导航栏单击“基础配置>静态网站托管”，进入“静态网站托管”界面。

步骤 4 单击“配置静态网站托管”，系统弹出“配置静态网站托管”对话框。

步骤 5 “状态”设置为使能状态。

步骤 6 “托管模式”选择“重定向请求”，如图 2-43 所示。在“重定向页面”中输入桶访问域名或 URL。

图2-43 配置重定向请求

步骤 7 单击“确定”。

步骤 8 在桶列表中选择重定向的桶。

步骤 9 **验证**：在浏览器输入本桶的访问域名，结果显示为重定向的桶或重定向的 URL。

说明

由于浏览器缓存等原因，您可能需要清除浏览器缓存后才能查看到预期效果。

----结束

2.16 跨域资源共享

2.16.1 跨域资源共享简介

跨域资源共享（CORS）是由 W3C 标准化组织提出的一种网络浏览器的规范机制，定义了一个域中加载的客户端 Web 应用程序与另一个域中的资源交互的方式。而在通常的网页请求中，由于同源安全策略（Same Origin Policy，SOP）的存在，不同域之间的网站脚本和内容是无法进行交互的。

OBS 支持 CORS 规范，允许跨域请求访问 OBS 中的资源。

OBS 支持静态网站托管，而只有当对该桶设置了合理的 CORS 配置，OBS 中保存的静态网站才能允许响应另一个跨域网站的请求。

CORS 的典型应用场景包括：

- 通过 CORS 支持，使用 JavaScript 和 HTML5 来构建 Web 应用，直接访问 OBS 中的资源，而不再需要代理服务器做中转。
- 使用 HTML5 中的拖拽功能，直接向 OBS 上传文件，展示上传进度，或是直接从 Web 应用中更新内容。
- 托管在不同域中的外部网页、样式表和 HTML5 应用，现在可以引用存储在 OBS 中的 Web 字体或图片，让这些资源能被多个网站共享。

CORS 配置会在两分钟内生效。

2.16.2 配置跨域资源共享

OBS 提供 HTML5 协议中的 CORS 设置，帮助用户实现跨域访问。

前提条件

已经配置了静态网站托管，配置方法请参见配置静态网站托管。

操作步骤

步骤 1 在桶列表单击待操作的桶，进入“对象”页面。

步骤 2 在左侧导航栏，单击“概览”，进入“概览”页面。

步骤 3 在桶概览信息展示区域“基础配置”下，单击“CORS 规则”卡片，系统跳转至“CORS 规则”界面。

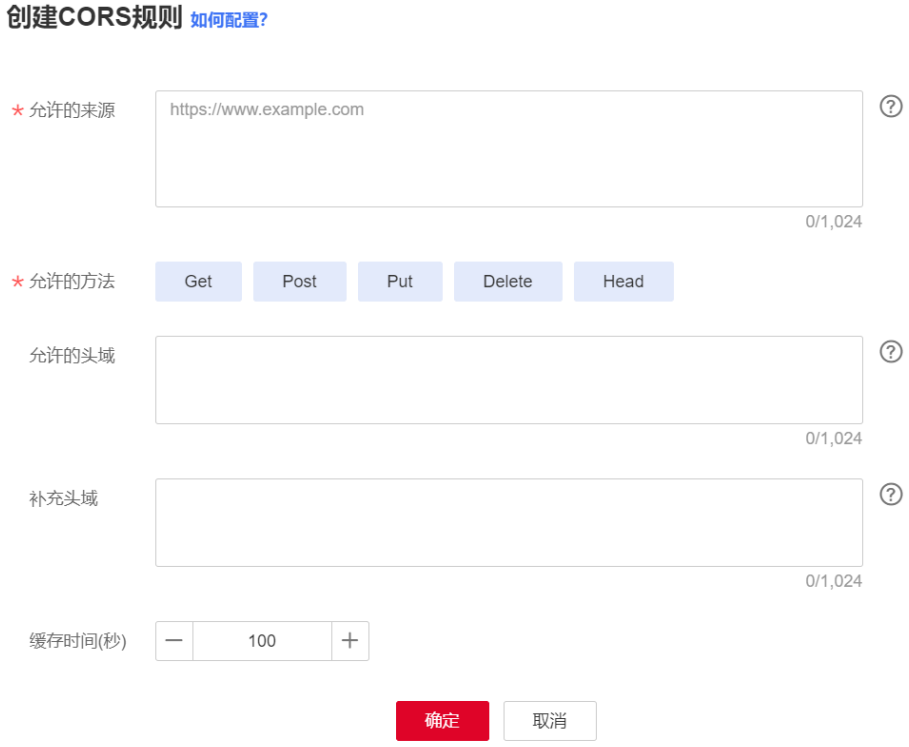
或您可以直接在左侧导航栏单击“访问权限控制>CORS 规则”，进入“CORS 规则”界面。

步骤 4 单击“创建”，系统弹出“创建 CORS 规则”对话框，如图 2-44 所示。

说明

一个桶最多可设置 100 条 CORS 规则。

图2-44 创建 CORS 规则



步骤 5 在“CORS 规则”中配置“允许的来源”、“允许的方法”、“允许的头域”、“补充头域”和“缓存时间”。

表2-35 CORS 规则

参数	说明

允许的来源	必选参数，指定允许的跨域请求的来源，即允许来自该域名下的请求访问该桶。
	允许多条匹配规则，以回车换行为间隔。每个匹配规则允许使用最多一个“*”通配符。例如：
	`http://rds.example.com`
	`https://*.vbs.example.com`

允许的方法	必选参数，指定允许的跨域请求方法，即桶和对象的几种操作类型。包括：Get、Post、Put、Delete、Head。
允许的头域	可选参数，指定允许的跨域请求的头域。只有匹配上允许的头域中的配置，才被视为是合法的 CORS 请求。 允许的头域可设置多个，多个头域之间换行隔开，每行最多可填写一个*符号，不支持&、:、<、空格以及中文

参数	说明
	字符。
补充头域	可选参数，指 CORS 响应中带的补充头域，给客户端提供额外的信息。 默认情况下浏览器只能访问以下头域：Content-Length、Content-Type，如果需要访问其他头域，需要在补充头域中配置。 补充头域可设置多个，多个头域之间换行隔开，不支持*、&、:、<、空格以及中文字符。
缓存时间	必选参数，请求来源的客户端可以缓存的 CORS 响应时间，以秒为单位，默认为 100 秒。

步骤 6 单击“确定”。

“CORS 规则”页签显示“创建 CORS 规则成功”提示创建桶的 CORS 配置成功。CORS 配置会在两分钟内生效。

CORS 配置成功后，便仅允许跨域请求来源的地址通过允许的方法访问 OBS 的桶。例如：为桶“testbucket”允许的来源配置为“https://www.example.com”，允许的方法配置为“GET”，允许的头域和补充的头域配置为“*”，缓存时间设置为“100”，则 OBS 仅允许来源为“https://www.example.com”的“GET”请求访问桶“testbucket”，且不限制该请求的头域，请求来源的客户端可缓存的该 CORS 请求的响应时间为 100 秒。

----结束

复制 CORS 规则

步骤 1 在桶列表单击待操作的桶，进入“对象”页面。

步骤 2 在左侧导航栏，单击“概览”，进入“概览”页面。

步骤 3 在桶概览信息展示区域“基础配置”下，单击“CORS 规则”卡片，系统跳转至“CORS 规则”界面。

或您可以直接在左侧导航栏单击“访问权限控制>CORS 规则”，进入“CORS 规则”界面。

步骤 4 单击“复制”。

步骤 5 选择复制源，即 CORS 规则所在的源桶。

说明

- 从源桶复制 CORS 规则的操作为增量复制，不会删除当前桶已存在的 CORS 规则，与已存在的 CORS 规则冲突的规则不会复制。
- 源桶和目标桶的桶版本号都必须是 3.0。
- 您可以按需移除不需要复制的 CORS 规则。
- 单桶 CORS 规则上限为 100 条，如果已有规则+复制规则的数量超过上限，将会复制失败，请先删除多余规则再进行复制。

图2-45 复制 CORS 规则

步骤 6 单击“确定”，将源桶的 CORS 规则复制到当前桶。

----结束

2.17 防盗链

2.17.1 防盗链简介

一些不良网站为了不增加成本而扩充自己站点内容，经常盗用其他网站的链接。一方面损害了原网站的合法利益，另一方面又加重了服务器的负担。因此，产生了防盗链技术。

在 HTTP 协议中，通过表头字段 referer，网站可以检测目标网页访问的来源网页。有了 referer 跟踪来源，就可以通过技术手段来进行处理，一旦检测到来源不是本站即进行阻止或者返回指定的页面。防盗链就是通过设置 Referer，去检测请求来源的 referer 字段信息是否与白名单或黑名单匹配，若与白名单匹配成功则允许请求访问，否则阻止请求访问或返回指定页面。

为了防止用户在 OBS 的数据被其他人盗链，OBS 支持基于 HTTP header 中表头字段 referer 的防盗链方法。OBS 同时支持访问白名单和访问黑名单的设置。

2.17.2 配置防盗链

OBS 提供同时支持允许白名单访问和阻止黑名单访问的配置，防止盗链。

前提条件

已经配置了静态网站托管。

操作步骤

步骤 1 在桶列表单击待操作的桶，进入“对象”页面。

步骤 2 在左侧导航栏，单击“概览”，进入“概览”页面。

步骤 3 在“基础配置”区域下，单击“防盗链”卡片，系统跳转至“防盗链”界面。

步骤 4 单击“白名单 Referer”/“黑名单 Referer”后的 ，输入白名单/黑名单。

Referer 规则如下：

- 白名单 Referer/黑名单 Referer 输入的字节数不能超过 1024 个字符。
- Referer 格式：
  - Referer 可以设置多个，多个 Referer 换行隔开；
  - Referer 参数支持通配符（*）和问号（?），通配符可代替 0 个或多个字符，问号可代替单个字符；
  - 如果下载时 Referer 头域包含了 http 或 https，则 Referer 设置必须包含 http 或 https。
- 白名单 Referer 为空，黑名单 Referer 不空时，允许所有黑名单中指定网站以外的其他网站的请求访问目标桶中的数据。
- 白名单 Referer 不为空，黑名单 Referer 为空或不空时，只允许白名单中指定网站的请求访问目标桶中的数据。

说明

当白名单 Referer 与黑名单 Referer 内容一样时，黑名单生效。例如：当白名单 Referer 与黑名单 Referer 输入框中的 referer 字段都为“https://www.example.com”时，系统是阻止该请求访问的。

- 黑名单 Referer 与白名单 Referer 都为空时，默认允许所有网站的请求访问目标桶中的数据。
- 判断用户是否有对桶及其内容访问的四种权限（读取权限、写入权限、ACL 读取权限、ACL 写入权限）之前，需要首先检查是否符合 referer 字段的防盗链规则。

步骤 5 单击 保存设置。

----结束

2.18 任务管理

当您执行上传对象、删除文件夹、批量恢复和批量修改存储类别时，会在任务中心生成一条任务记录，方便您查看任务进度和状态。

说明

刷新或关闭浏览器，会取消当前任务并清除全部记录。

操作步骤

步骤 1 在桶的对象列表页，单击界面右上角的“任务中心”。

步骤 2 执行上传对象、删除文件夹、批量恢复或批量修改存储类别操作，可查看对应操作的任务记录。

- 可单击“清除记录”，清除所有任务记录。
- 在“上传”页签，可单击“全部暂停”或“全部开始”，批量管理上传任务。

----结束

2.19 相关操作参考

2.19.1 创建 IAM 委托

在使用 OBS 的部分特性时，需要使用 IAM 委托功能给 OBS 授予相关的权限，以委托 OBS 处理您的数据。

创建用于跨区域复制的委托

步骤 1 在 OBS 控制台“创建跨区域复制规则”对话框，单击“创建 IAM 委托”，进入“统一身份认证服务”控制台“委托”页面。

步骤 2 单击“创建委托”，进行委托创建。

步骤 3 输入“委托名称”。

步骤 4 “委托类型”选择“云服务”。

步骤 5 “云服务”选择“OBS”。

步骤 6 选择“持续时间”。

步骤 7 单击“下一步”。

步骤 8 选择“全局服务”，搜索并选择“OBS Administrator”权限。

步骤 9 单击“确定”，完成委托创建。

----结束

创建用于上传日志的委托

步骤 1 在“日志记录”对话框，单击“创建委托”，进入“统一身份认证服务”管理控制台“委托”页面。

步骤 2 单击“创建”，进行委托创建。

步骤 3 输入“委托名称”。

步骤 4 “委托类型”选择“云服务”。

步骤 5 “云服务”选择“OBS”。

步骤 6 选择“持续时间”。

步骤 7 单击“下一步”。

步骤 8 在作用范围区域选择“全局服务”。

步骤 9 在权限区域搜索并选择拥有日志存储桶上传权限的自定义策略，单击下方的“确定”完成委托创建。

如还未创建自定义策略，请先参见创建自定义策略创建。

自定义策略的作用范围选择“全局级服务”，策略配置方式选择“JSON 视图”，策略内容如下：

说明

下方 JSON 中 mybucketlogs 需要替换为实际日志存储桶的桶名。

```
{
   "Version": "1.1",
   "Statement": [
      {
         "Action": [
            "obs:object:PutObject"
         ],
         "Resource": [
            "OBS:*:*:object:mybucketlogs/*"
         ],
         "Effect": "Allow"
      }
   ]
}
```

步骤 10 （可选）如果日志存储桶开启了默认加密，日志存储桶所在区域还需要具有“KMS Administrator”权限。

1. 在“统一身份认证服务”管理控制台“委托”页面，单击上一步创建的委托名称。
2. 选择“委托权限”页签，单击“配置权限”。
3. 在作用范围区域选择“区域级项目”，选择日志存储桶所在区域的项目。
4. 在权限区域搜索并选择“KMS Administrator”权限，单击下方的“确定”完成委托权限修改。

步骤 11 单击“确定”，完成委托创建。

----结束

2.20 异常处理

2.20.1 使用 IE11 浏览器下载对象时提示对象无法下载

问题

用 IE11 浏览器登录 OBS 管理控制台上传一个对象，在未关闭浏览器的情况下，下载该对象到本地原路径下，选择替换原文件保存，浏览器会弹出无法下载的提示。

例如，从本地 C 盘的根目录下上传一个名为“abc”的对象到 OBS 管理控制台的某桶中，在不关闭浏览器的情况下，将该对象再下载到本地 C 盘的根目录下，并选择替换原文件保存，浏览器会弹出无法下载的提示。

回答

此问题是由于浏览器不兼容导致的，使用其他浏览器即可规避此问题。

出现此问题后，关闭浏览器后再重试，也可以规避此问题。

2.20.2 使用 IE9 浏览器无法打开 OBS 管理控制台界面

问题

在 OBS 管理控制台地址能够 Ping 通的情况下，为什么使用 IE9 浏览器无法打开 OBS 管理控制台界面？

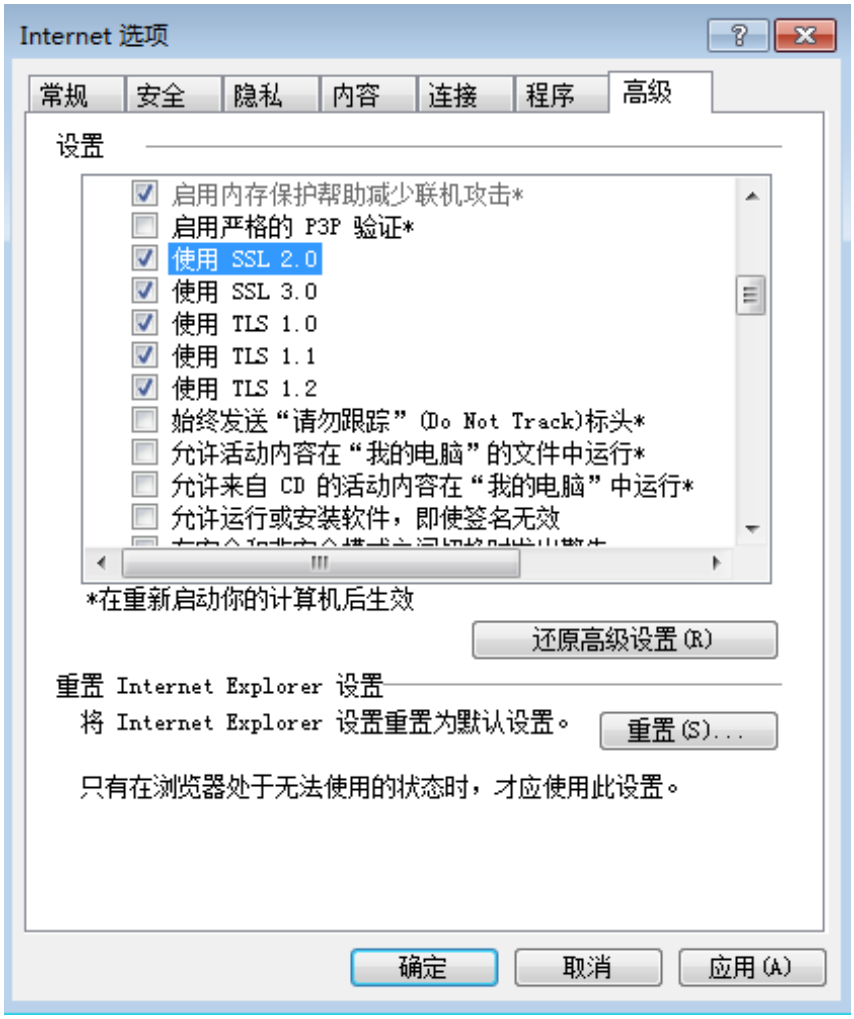
回答

检查浏览器的“Internet 选项”中是否勾选 SSL 和 TLS 选项，若没有，则根据以下步骤处理后再重试。

步骤 1 打开 IE9 浏览器。

步骤 2 单击页面右上角的“设置”按钮，单击“Internet 选项 > 高级”，勾选“使用 SSL 2.0”，“使用 SSL 3.0”，“使用 TLS 1.0”，“使用 TLS 1.1”，“使用 TLS 1.2”，如图 2-46 所示。

图2-46 Internet 选项



步骤 3 单击“确定”。

----结束

2.20.3 下载一个对象名较长的对象到本地后，对象名称改变

问题

使用 OBS 管理控制台下载一个对象名较长的对象到本地后，为什么对象名称发生了改变？

回答

Windows 操作系统下允许的文件名长度最大为 255 字符，包括文件名和扩展名在内。当对象名称长度超过 255 字符时，将该对象下载到本地后，系统便会自动将对象名截取至 255 字符。

2.20.4 出现“客户端与服务器的时间相差 15 分钟”的报错

问题

使用 OBS 时出现报错“客户端与服务器的时间相差大于 15 分钟”或“The difference between the request time and the current time is too large”。

回答

出于安全目的，OBS 会校验客户端与 OBS 服务器的时间差，当该时间差大于 15 分钟时，OBS 服务器会拒绝您的请求，从而出现此报错。请根据本地 UTC 时间调整本地时间后再访问。

2.21 错误码列表

如果请求因错误导致未被处理，则会返回一条错误响应。错误响应中包括错误码和具体错误描述。表 2-34 列出了错误响应中的常见错误码。

表2-36 错误码列表

错误码	描述
Obs.0000	无效的参数。
Obs.0001	所有对这个对象的访问已经无效了。
Obs.0002	文件的绝对路径总长度不能超过 1023 字符，请重试。
Obs.0003	连接超时。
Obs.0004	客户端与服务器的时间相差大于 15 分钟。 出于安全目的，OBS 会校验客户端与 OBS 服务器的时间差，当该时间差大于 15 分钟时，OBS 服务器会拒绝您的请求，从而出现此报错。请根据本地 UTC 时间调整本地时间后再访问。
Obs.0005	服务器负载过高，请稍后重试。
Obs.0006	用户拥有的桶的数量已经达到了系统的上限。 一个帐号及帐号下的所有 IAM 用户可创建的桶+并行文件系统的上限为 100 个。建议结合 OBS 细粒度权限控制能力，合理进行桶规划和使用。
Obs.0007	目标桶不存在或目标桶与当前桶不属于同一区域，请确认后重新操作。
Obs.0008	你的帐号还没有在系统中注册，必须先在系统中注册了才能使用该帐号。
Obs.0009	另外一个冲突的操作当前正作用在这个资源上，请重试。

错误码	描述
	这是由于 OBS 中存在同名桶且该同名桶在短期内因欠费被释放导致的。建议您更换桶名再试。
Obs.0010	删除失败，请检查桶中是否存在对象或历史版本的对象。
Obs.0011	桶策略规则无效，请重新配置。
Obs.0012	请求的桶名已经存在。桶的命名空间是系统中所有用户共用的，选择一个不同的桶名再重试一次。
Obs.0013	请求的文件夹名已经存在。选择一个不同的名字再重试一次。
Obs.0014	文件超过 50MB。请使用 OBS Browser+上传。
Obs.0015	搜索条件的绝对路径总长度超过 1023 字符，请重试。
Obs.0016	上传对象失败。可能原因如下： 1. 网络异常。 2. 无桶的写权限。
Obs.0017	新的有效期对应的过期时间必须晚于当前该对象的过期时间。
Obs.0018	有效期必须大于或等于剩余天数。
Obs.0019	无法判断桶中是否有对象或碎片，请检查您是否有桶的读权限。
Obs.0020	TMS 系统内部错误，请稍后重试。
Obs.0021	您没有权限访问 TMS。TMS 需要的权限请在 IAM 中配置。
Obs.0022	TMS 系统繁忙，请稍后重试。

3 常见问题

3.1 一般性问题

3.1.1 对象存储与 SAN 存储和 NAS 存储相比较有什么优势？

- SAN 存储提供给应用的是一个 LUN 或者是一个卷，LUN 和卷是面向磁盘空间的一种组织方式，上层应用要通过 FC 或者 ISCSI 协议访问 SAN。SAN 存储处理的是管理磁盘的问题，其他事情都要依靠上层的应用程序实现。
- NAS 存储提供给应用的是一个文件系统或者是一个文件夹，上层应用通过 NFS 和 CIFS 协议进行访问。文件系统要维护一个目录树。
- 对象存储更加适合 web 类应用，基于 URL 访问地址提供一个海量的桶存储空间，能够存储各种类型的文件对象，对象存储是一个扁平架构，无需维护复杂的文件目录。无需考虑存储空间的限制，一个桶支持近乎无限大的存储空间。

3.1.2 我可以存储哪种类型的数据？

OBS 可以存储任何格式的任何类型数据。

3.1.3 我可以在 OBS 中存储多少数据？

OBS 系统和单个桶都没有总数据容量和对象/文件数量的限制，但对于单次上传对象的大小有如下限制：

- 管理控制台支持批量上传文件，单次最多支持 100 个文件同时上传，总大小不超过 5GB。如果只上传 1 个文件，则这个文件最大为 5GB。
- OBS Browser+和 API 上传的单个对象最大是 48.8TB。

3.1.4 OBS 的文件夹与文件系统的文件夹是否一样？

不一样。

OBS 并没有文件系统中的文件和文件夹概念。为了使用户更方便进行管理数据，OBS 提供了一种方式模拟文件夹。实际上在 OBS 内部是通过在对象的名称中增加“/”，将该对象在 OBS 管理控制台上模拟成一个文件夹的形式展现。

3.1.5 OBS 的数据存储在哪里？

在 OBS 上创建桶时，您可以指定一个区域。在该区域内，您的数据存储在多台设备上。

3.1.6 OBS 支持 HTTPS 访问吗？

OBS 支持 HTTPS 访问。

- 使用 OBS 分配的域名进行访问时，只要在浏览器中将桶或对象的 URL 的 http 替换成 https 即可。

3.1.7 OBS 中的数据可以让其他用户访问吗？

可以。

- 对于桶，可以通过桶 ACL 和桶策略授予其他用户桶的读取权限，其他用户即可访问该桶。
- 对于对象，可以通过对象 ACL，对象策略和桶策略来授予其他用户对象的读取权限，其他用户即可访问该对象。

3.1.8 OBS 是否支持断点续传功能？

OBS 管理工具断点续传功能的支持情况：

表3-1 OBS 管理工具断点续传功能

OBS 管理工具	断点续传功能
管理控制台	不支持
OBS Browser+	支持
API	不支持

3.1.9 OBS 是否支持批量上传文件？

OBS 管理工具批量上传功能的支持情况：

表3-2 OBS 管理工具批量上传功能

工具	批量上传
管理控制台	OBS 管理控制台支持批量上传文件，单次最多支持 100 个文件同时上传，总大小不超过 5GB。
OBS Browser+	支持上传多个文件或一个文件夹。单次最多支持 500 个文件同时上传。
API	不支持

3.1.10 OBS 是否支持批量下载文件？

OBS 管理工具批量下载功能的支持情况：

表3-3 OBS 管理工具批量下载功能

工具	批量下载
管理控制台	不支持
OBS Browser+	支持
API	不支持

3.1.11 OBS 是否支持批量删除对象？

OBS 管理工具批量删除功能的支持情况：

表3-4 OBS 管理工具批量删除功能

工具	批量删除
管理控制台	支持，一次批量删除的对象数最多为 100 个，若选择文件夹，只能单个删除文件夹。
OBS Browser+	支持，可批量删除多个文件和文件夹，一次删除的数量没有限制。
API	支持，批量删除对象一次能接收最大对象数目为 1000 个。

说明

批量删除的性能和单个请求内的对象数负相关，对于 QPS 的计算，删除 N 个对象，算 N 次操作。如果删除对象数量大并且对象前缀使用了字典序，可能导致大量对象的请求访问集中于某个特定分区，造成访问热点。热点分区上的请求速率受限，访问时延上升。

为解决以上问题，您可以考虑减少单个批量删除请求的对象数量，增加并发请求数，并将对象名的顺序前缀改为随机性前缀。

3.1.12 OBS 上传下载速率的影响因素有哪些？

影响 OBS 上传下载速率的因素有：

- 受单个帐号的读写带宽上限影响。
- 上传下载速率还受网卡、磁盘 io 及是否有其它进程抢占资源的影响。

3.1.13 为什么 OBS 存储的数据丢失了？

- 请检查桶中是否设置了生命周期过期删除规则，符合规则的对象会被删除。

- 请检查桶是否授权了其他用户桶的写权限，被授权的用户都可以删除对象。若您开启了日志记录功能，可以通过日志记录查询到删除对象的用户。

3.1.14 已删除的数据是否可以恢复？

- 桶开启了多版本控制功能时，删除的对象会保存到“已删除对象”列表中，您可以在“已删除对象”列表中恢复对象，详情请参见取消删除对象。
- 桶没有开启多版本控制功能时，已删除的对象不可恢复。

3.1.15 已删除的数据在 OBS 中是否会有残留？

用户选择清除数据之后，系统会保证完全删除数据，不会留下残留信息，无需担心信息泄露。

3.2 权限相关

3.2.1 如何对 OBS 进行访问权限控制？

您可以使用以下几种机制来控制对 OBS 的访问权限。

- IAM 策略

  IAM 策略是作用于云资源的，IAM 策略定义了允许和拒绝的访问操作，以此实现云资源权限访问控制。

  推荐使用 IAM 策略的场景：对同一帐号内的子用户授权。

  IAM 策略的实现机制如下：

  a. 创建用户组，为用户组设定 IAM 权限集。

  b. 创建 IAM 用户，用户加入用户组以获取相关的权限。

- 桶策略

  桶策略是作用于所配置的 OBS 桶及桶内对象的。OBS 桶拥有者通过桶策略可为 IAM 用户或其他帐号授权桶及桶内对象的操作权限。

- 访问控制列表 (ACL)

  ACL 是基于帐号级别的读写权限控制，权限控制细粒度不如桶策略和 IAM 策略。一般情况下，建议使用 IAM 策略和桶策略进行访问控制。

3.2.2 IAM 策略和桶策略访问控制有什么区别？

IAM 策略是作用于云资源的，IAM 的 OBS 策略是作用于 OBS 的所有桶和对象的。

桶策略是作用于配置桶策略的单个桶的。

3.2.3 桶策略和对象策略之间有什么关系？

对象策略即为桶策略中针对对象的策略，区别是对象策略只针对一个对象，桶策略中针对对象的策略可以配置多个对象或桶中所有对象。

3.3 桶和对象相关

3.3.1 创建桶失败

- 若当前用户所创建的桶已达到上限 100 个，删除一些闲置的桶再创建。
- 若是当前桶名已存在，则更换桶名再创建。在 OBS 中，桶名必须是全局唯一的，即用户创建的桶不能与自己已创建的其他桶名称相同，也不能与其他用户创建的桶名称相同。
- 用户删除桶后，立即创建同名桶或并行文件系统会创建失败，需要等待 30 分钟才能创建。
- 检查帐号是否拥有权限，若无权限，请授予对应的操作权限。
- 检查帐号是否已欠费或余额不足。若欠费，请先续费。
- 检查本地与 OBS 的网络是否正常，若存在网络故障，解决网络故障，确保网络正常。
- 若以上都不是，请根据返回的错误码进一步判断。

3.3.2 上传对象失败

- 检查本地与 OBS 的网络是否正常，若存在网络故障，解决网络故障，确保网络正常。
- 上传对象时弹出“Service Unavailable”的错误提示，则可能是因为当前服务器繁忙，请稍后重试。
- 检查帐号是否已欠费或余额不足。若欠费，请先续费。
- 检查帐号是否拥有桶的上传对象权限，请综合 IAM 策略、桶策略和桶 ACL 共同检查。若无权限，请先授权。
- 对于 OBS Browser+，数据库紊乱也会造成上传失败，您可以清空数据库后再次上传文件。

  在数据库路径下，删除所有文件。
- 对于 OBS Browser+，您还要检查您的电脑系统是否使用了搜狗输入法，若是，请升级搜狗输入法到最新版本。
- 若以上都不是，请联系客服进一步解决。

3.3.3 下载对象失败

- 检查本地与 OBS 的网络是否正常，若存在网络故障，解决网络故障，确保网络正常。
- 检查帐号是否已欠费或余额不足。若欠费，请先续费。
- 检查帐号是否拥有桶的下载对象权限，请综合 IAM 策略、桶策略、对象策略、桶 ACL 和对象 ACL 共同检查。若无权限，请先授权。
- 检查当前对象是否采用了 KMS 加密，若对象已加密，使用管理控制台和 OBS Browser+下载对象时会失败；使用 SDK 和 API 下载时，需提供密钥才能下载成功。
- 若以上都不是，请联系客服进一步解决。

3.3.4 删除桶失败

- 检查本地与 OBS 的网络是否正常，若存在网络故障，解决网络故障，确保网络正常。
- 检查桶列表中的对象是否已经全部删除。若没有，请先删除桶列表中的所有对象。
- 检查碎片列表中的对象是否已经全部删除。若没有，请先删除碎片列表中的所有对象。
- 如果已开启多版本控制功能，需要检查已删除对象列表中的对象是否已经全部删除。若没有，请先删除已删除对象列表中的所有对象。
- 确认执行删除操作的帐号是否为桶的拥有者。
- 若以上都不是，请联系客服进一步解决。

3.3.5 我可以修改对象名称吗？

可以。

重命名桶中对象

OBS 客户端支持重命名桶中对象，您可以对单个对象重命名。

3.3.6 我可以修改桶所在的区域吗？

不可以。桶创建后，不能更改区域。

3.3.7 如何获取对象访问路径？

对象访问路径为：https://桶名.域名/对象名。

您可以自己拼接，或通过以下工具方式获取：

表3-5 对象 URL 获取方式

工具	对象 URL
管理控制台	单击对象，从对象属性中 copy 获取到对象 URL 访问路径。
OBS Browser+	单击对象属性按钮，从对象属性中 copy 获取到对象 URL 访问路径。
API	不支持

说明

如果是自己拼接的对象访问路径，用户需要参考 URL 编码（URL encoding）规则对对象名进行转义。

3.3.8 无法搜索到桶中对象

OBS 管理控制台和 OBS Browser+支持通过前缀搜索对象，例如，您搜索“test”，搜索结果为以前缀为“test”的对象。若您输入的不是待搜索对象名称的前缀，则搜索不到对象。例如，您待搜索对象名称为“testabc”，您输入“abc”搜索，则搜索不到“testabc”对象，只能搜索到名称以“abc”开头的对象。

3.4 安全性

3.4.1 我的数据存在 OBS 中，如何保证安全性？

OBS 本身是非常安全的。OBS 本身也提供端到端的安全服务。访问桶或对象时，如果桶或对象未公开，只有桶或对象的拥有者才能够访问，访问时需要提供访问密钥（AK/SK）。您还可以使用各种访问控制机制，例如桶策略和访问控制列表（ACL），选择性地向您的用户和用户组授予权限。传输数据时，OBS 支持 HTTPS/SSL 协议；如果您需要更高安全性，可以开启服务端加密功能。

3.4.2 OBS 会不会扫描我的数据用于其他用途？

系统对数据做的扫描仅限于判断数据块是否存在和被损坏（如有损坏，会启动修复），不会读取具体的内容。

3.4.3 后台工程师能否导出我存在 OBS 中的数据？

后台工程师无法导出用户数据。访问桶或对象时，如果桶或对象未公开，只有桶或对象的拥有者才能够访问，访问时需要提供访问密钥（AK/SK）。

3.4.4 OBS 如何保证我的数据不会被盗用？

只有桶或对象的拥有者才能访问，访问时需要提供访问密钥（AK/SK），并且还有 ACL、桶策略、防盗链等多种访问控制机制保证数据的访问安全。

3.4.5 在使用 AK 和 SK 访问 OBS 过程中，密钥 AK 和 SK 是否可以更换？

可以。在使用过程中，密钥 AK 和 SK 可以随时更换。

3.4.6 多个用户是否可以共享一对 AK 和 SK 来访问 OBS？

可以。不同的用户使用相同的一对 AK 和 SK 可以同时访问 OBS 中的资源，且访问到的资源相同。

3.4.7 我对存储在 OBS 上的数据加密时，可支持哪些加密技术？

您在将数据上传到 OBS 中前，可以事先对数据进行加密，以保证传输和保存的安全性。OBS 不限定客户端加密的技术。

用户可根据需要对对象进行服务端加密，使对象更安全的存储在 OBS 中。

需要上传的对象可以通过数据加密服务器提供密钥的方式进行服务端加密。用户首先需要在 KMS 中创建密钥（或者使用 KMS 提供的默认密钥），当用户在 OBS 中上传对象时使用该密钥进行服务端加密。

当启用服务端加密功能后，用户上传对象时，数据会在服务端加密成密文后存储。用户下载加密对象时，存储的密文会先在服务端解密为明文，再提供给用户。

OBS 支持通过接口提供 KMS 托管密钥的服务端加密(SSE-KMS)。

3.5 碎片管理

3.5.1 为什么会有碎片产生？

桶中不完整的数据称之为碎片，通常是由于数据上传失败而产生的。

OBS 采用分段上传的模式上传数据，在下列情况下（但不仅限于此）通常会导致数据上传失败而产生碎片。

- 网络条件较差，与 OBS 的服务器之间的连接经常断开。
- 上传过程中，人为中断上传任务。
- 设备故障。
- 突然断电等特殊情况。

3.5.2 如何处理碎片？

OBS 中的碎片会占用存储空间，会按照存储空间计费项进行计费。

您可以通过 OBS 管理控制台或 OBS Browser+将桶中碎片清理掉。

若是由于 OBS Browser+分段上传任务中断产生的碎片，继续运行完成任务，碎片将会消失。

3.6 多版本控制

3.6.1 我可以上传同名对象到同一个文件夹中吗？

若开启了多版本控制，上传对象时，OBS 自动为每个对象创建唯一的版本号。上传同名的对象将以不同的版本号同时保存在 OBS 中。

若未开启多版本控制，向同一个文件夹中上传同名的对象时，新上传的对象将覆盖原有的对象。

3.6.2 我可以恢复已删除的对象吗？

启用多版本控制功能后，不带版本号删除对象时，对象产生一个带唯一版本号的删除标记，在已删除对象列表中，您可以从此处恢复您需要的对象。

如果未启用版本控制功能，或启用该功能后指定版本号删除了对象，OBS 将彻底删除这些数据，将无法找回。

详情请参见多版本控制简介。

3.7 标签

3.7.1 我可以通过标签搜索桶吗？

不支持通过标签搜索桶。

3.7.2 我可以使用标签做什么？

当为桶添加标签时，该桶上所有请求产生的计费话单里都会带上这些标签，从而可以针对话单报表做分类筛选，进行更详细的成本分析。例如：某个应用程序在运行过程会往桶里上传数据，我们可以用应用名称作为标签，设置到被使用的桶上。在分析话单时，就可以通过应用名称的标签来分析此应用的成本。

3.8 生命周期管理

3.8.1 我在什么场景下需要使用生命周期管理？

生命周期管理可适用于以下典型场景：

- 周期性上传的日志文件，可能只需要保留一个星期或一个月。到期后要删除它们。

若您需要大量的删除桶内对象，您可以设置生命的周期的过期删除，可定时删除桶内对象。在“生命周期规则”界面，按照表 3-6 参数创建规则：

表3-6 过期删除参数配置

参数	取值
状态	启用
规则名称	例如：rule-delete
策略	可以配置按前缀删除对象，也可以配置到整个桶，删除整个桶内对象。
当前版本	过期删除 天数：1 天
历史版本	过期删除 天数：1 天

1 天后，桶内对象按照规则删除成功。若您以后不再按照该规则删除对象，则停止或删除该生命周期规则。

3.9 静态网站托管

3.9.1 可以在 OBS 上托管我的静态网站吗？

OBS 支持静态网站托管。用户可以通过 OBS 管理控制台将自己的桶配置成静态网站托管模式，当客户端通过桶的 website 接入点访问桶内的对象资源时，浏览器可以直接解析出这些网页资源，呈现给最终用户。

3.9.2 哪些类型的网站适合使用 OBS 进行静态网站托管？

静态网站通常仅包含静态网页，以及可能包含部分可在客户端运行的脚本，如 JavaScript、Flash 等。

3.9.3 如何获取桶的静态网站托管地址？

您可以在控制台的静态网站托管页面上获取到桶的静态网站托管地址。

您也可以拼接桶的静态网站访问地址。拼接地址格式为：*https://桶名.静态网站托管域名*。

3.10 跨区域复制

3.10.1 我在什么场景下需要使用跨区域复制？

- 客户需要在多地访问相同的 OBS 资源。为了最大限度缩短访问对象时的延迟，您可以使用跨区域复制，在离客户较近的区域中创建对象副本。
- 由于业务原因，您需要将 OBS 数据从一个区域的数据中心迁移至另一个区域的数据中心。
- 出于对数据安全性以及可用性的考虑，您希望对所有写入 OBS 的数据，都在另一个区域的数据中心显式地创建一个备份，以防止在数据发生不可逆损毁时，有安全、可用的备份数据。

3.10.2 删除对象操作会同步复制到跨区复制的桶中吗？

不会，删除操作不同步。

启用跨区域复制规则后，符合以下条件的对象会复制到目标桶中：

- 新上传的对象。
- 有更新的对象，比如对象内容有更新，或者某一对象跨区域复制成功后源桶对象 ACL 设置有更新。

3.10.3 创建跨区域复制规则后，为什么对象没有复制到目标桶中？

- 创建跨区复制规则前，桶中已有的对象不会复制到目标桶中。
- 跨区域复制不保证时效性，配置跨区域复制规则后，可能会出现对象不会立即进行复制的情况，请耐心等待。