对象存储服务

用户指南 (巴黎区域)

文档版本 06

发布日期 2024-02-29

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

安全声明

漏洞处理流程

华为公司对产品漏洞管理的规定以“漏洞处理流程”为准，该流程的详细内容请参见如下网址：
https://www.huawei.com/cn/psirt/vul-response-process
如企业客户须获取漏洞信息，请参见如下网址：
https://securitybulletin.huawei.com/enterprise/cn/security-advisory

目 录

1 产品介绍

1.1 什么是对象存储服务

对象存储服务简介

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。

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管理控制台或各种OBS工具访问和管理存储在OBS中的数据。此外，OBS支持SDK和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。

产品架构

OBS的基本组成是**桶**和**对象**。

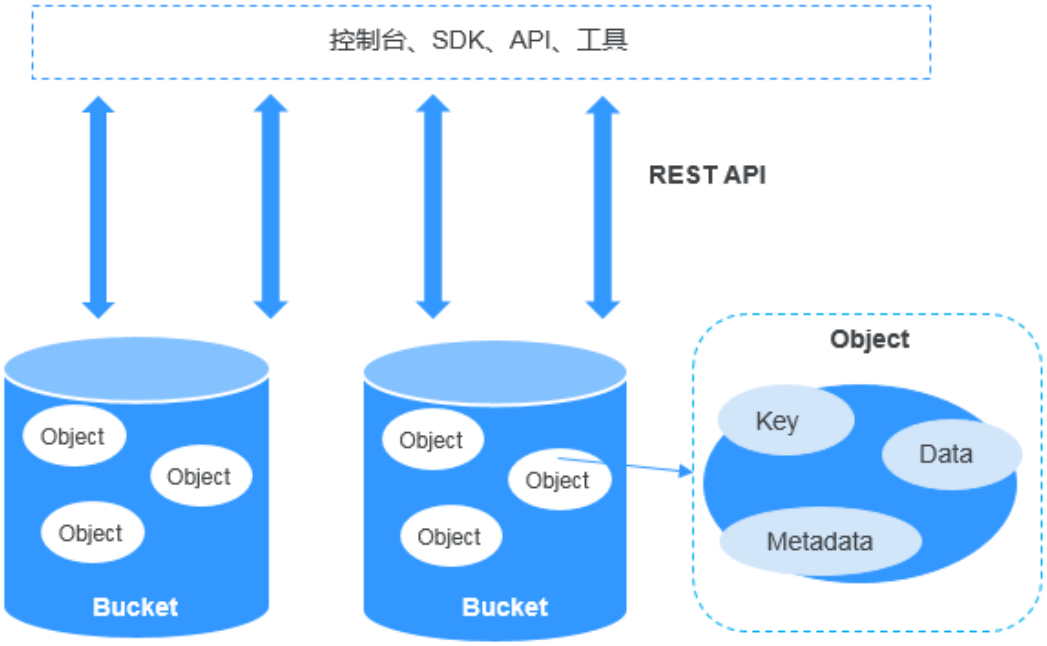
桶是OBS中存储对象的容器，每个桶都有自己的存储类别、访问权限、所属区域等属性，用户在互联网上通过桶的**访问域名**来定位桶。

对象是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的集合体，包括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。

针对OBS提供的REST API进行了二次开发，为您提供了控制台、SDK和各类工具，方便您在不同的场景下轻松访问OBS桶以及桶中的对象。您也可以利用OBS提供的SDK和API，根据您业务的实际情况自行开发，以满足不同场景的海量数据存储诉求。

图 1-1 产品架构



存储类别

对象存储提供了三种存储类别：标准存储、温存储、冷存储，从而满足客户业务对存储性能、成本的不同诉求。

- 标准存储访问时延低和吞吐量高，因而适用于有大量热点文件（平均一个月多次）或小文件（小于1MB），且需要频繁访问数据的业务场景，例如：大数据、移动应用、热点视频、社交图片等场景。
- 温存储适用于不频繁访问（平均一年少于12次）但在需要时也要求快速访问数据的业务场景，例如：文件同步/共享、企业备份等场景。与标准存储相比，温存储有相同的数据持久性、吞吐量以及访问时延，且成本较低，但是可用性略低于标准存储。
- 冷存储适用于很少访问（平均一年访问一次）数据的业务场景，例如：数据归档、长期备份等场景。冷存储安全、持久且成本极低，可以用来替代磁带库。为了保持成本低廉，数据恢复时间可能长达数分钟到数小时不等。

上传对象时，对象的存储类别默认继承桶的存储类别。您也可以重新指定对象的存储类别。

修改桶的存储类别，桶内已有对象的存储类别不会修改，新上传对象时的默认对象存储类别随之修改。

表 1-1 存储类别对比

对比项目	标准存储	温存储	冷存储
特点	高性能、高可靠、高可用的对象存储服务	高可靠、较低成本的实时访问存储服务	归档数据的长期存储，存储单价更优惠

对比项目	标准存储	温存储	冷存储
应用场景	云应用、数据分享、内容分享、热点对象	网盘应用、企业备份、活跃归档、监控数据	档案数据、医疗影像、视频素材、带库替代
最低存储时间	无	30天	90天
最小计量单位[a]	64KB	64KB	64KB
数据恢复	不涉及	按实际恢复数据量收费，单位GB	分加急、标准恢复方式 按实际恢复数据量收费，单位GB

如何访问对象存储服务

对象存储服务提供了多种资源管理工具，您可以选择表1-2中的任意一种方式访问并管理对象存储服务上的资源。

表 1-2 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。
obsutil	obsutil是一款用于访问管理OBS的命令行工具，您可以使用该工具对OBS进行常用的配置管理操作。对于熟悉命令行程序的用户，obsutil是执行批量处理、自动化任务的最佳选择。
obsfs	obsfs是对象存储提供的一款基于FUSE的文件系统工具，主要用于将并行文件系统挂载至Linux系统，让用户能够在本地像操作文件系统一样直接使用对象存储海量的存储空间。
SDK	SDK是对OBS服务提供的REST API进行的封装，以简化用户的开发工作。用户直接调用SDK提供的接口函数即可实现使用OBS业务能力的目的。

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1-3向您详细展示了OBS与自建存储服务器的优劣势对比。

表 1-3 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。	需自行承担网络信息安全、技术漏洞、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，并结合事件通知、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

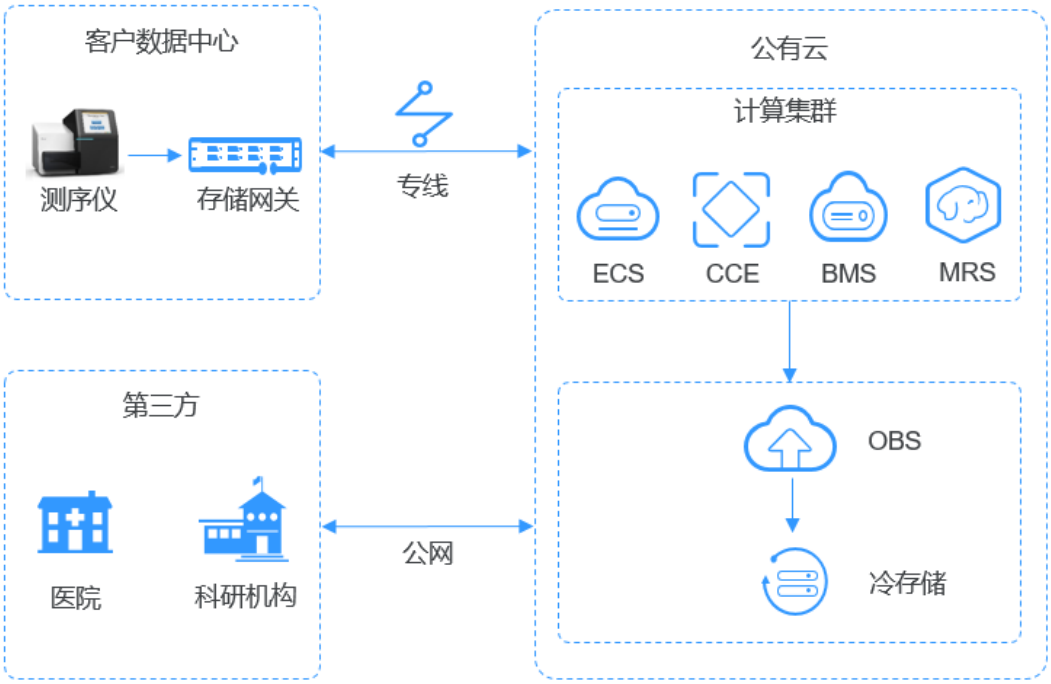
基因测序

场景描述

OBS提供高并发、高可靠、低时延、低成本的海量存储系统，结合计算服务可快速搭建高扩展性、低成本、高可用的基因测序平台。

客户数据中心测序仪上的数据通过云专线自动快速上传到云上，通过由ECS、CCE、MRS等服务搭建的计算集群进行分析计算，分析计算产生的数据和计算结果存储到OBS中，其中上传到云上的基因数据自动转为低成本的冷对象保存在OBS提供的冷存储中，计算得出的测序结果通过公网在线分发到医院和科研机构。

图 1-2 基因测序



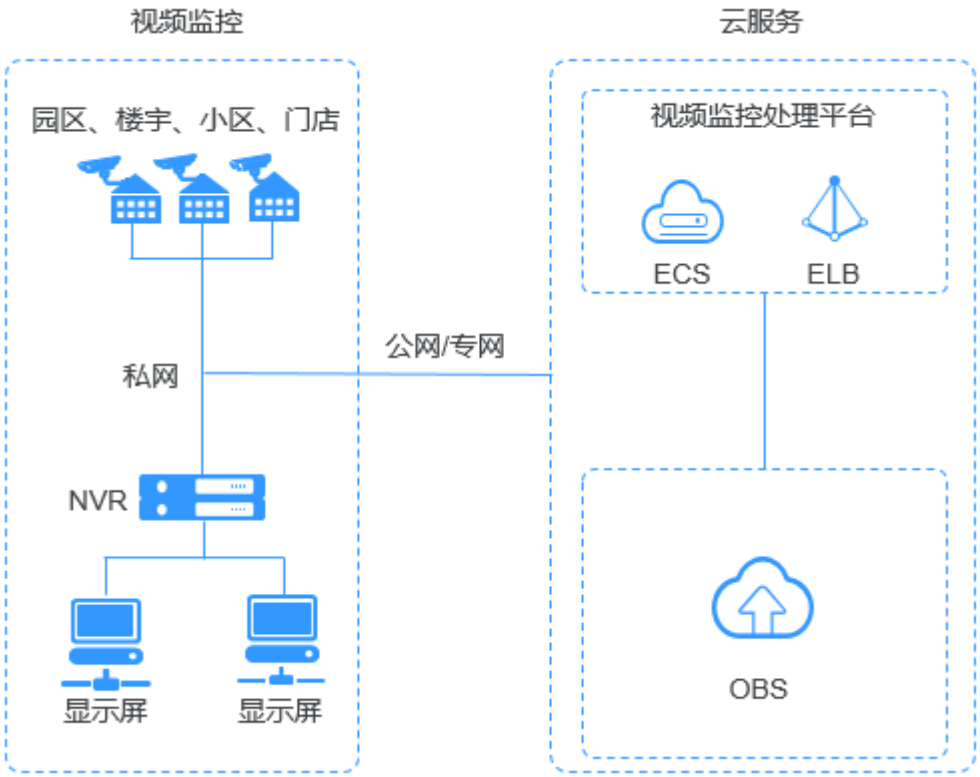
智能视频监控

场景描述

OBS为视频监控解决方案提供高性能、高可靠、低时延、低成本的海量存储空间，同时提供标准存储、温存储和冷存储分类存储数据，降低存储成本。

摄像头拍摄的监控视频通过公网或专线传输至云上，在弹性云服务器ECS和弹性负载均衡ELB组成的视频监控处理平台将视频流切片后存入OBS，后续再从OBS下载历史视频对象传输到观看视频的终端设备。

图 1-3 视频监控

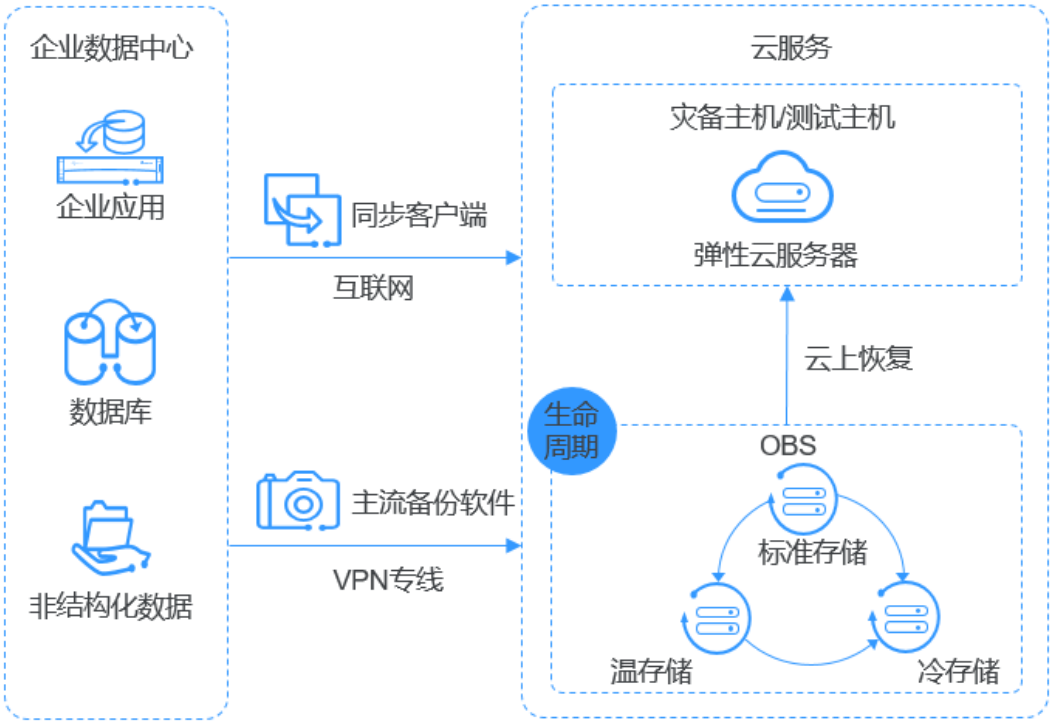


备份归档

场景描述

OBS提供高并发、高可靠、低时延、低成本的海量存储系统，满足各种企业应用、数据库和非结构化数据的备份归档需求。

图 1-4 备份归档



企业云盘（网盘）

场景描述

OBS配合弹性云服务器ECS、弹性负载均衡ELB、关系型数据库RDS和云硬盘备份VBS为企业云盘提供高并发、高可靠、低时延、低成本的存储系统，存储容量可随用户数据量的提高而自动扩容。

用户手机、电脑、PAD等终端设备上的动态数据与搭建在云上的企业云盘业务系统进行交互，动态数据请求发送到企业云盘业务系统处理后直接返回给终端设备。静态数据保存在OBS中，业务系统通过内网对静态数据进行处理，用户终端直接向OBS请求和恢复静态数据。同时，OBS提供生命周期功能，实现不同对象存储类别之间的自动转换，以节省存储成本。

图 1-5 企业云盘（网盘）

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，您可以在账号中给员工创建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。

如果账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，您只需要为您账号中的资源进行付费。关于IAM的详细介绍，请参见《IAM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1-4为OBS的所有系统策略。

表 1-4 OBS 系统策略

策略名称	描述	策略类别
Tenant Administrator	操作权限：对账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：对账号拥有的所有云资源的只读权限。 OBS策略在“全局服务>对象存储服务”下配置。	RBAC策略
OBS Buckets Viewer	操作权限：可以执行列举桶、获取桶基本信息、获取桶元数据的操作。 OBS策略在“全局服务>对象存储服务”下配置。	RBAC策略

用户拥有OBS资源权限后，对应在OBS上可以执行的具体操作如下表所示。

表 1-5 OBS 操作与资源权限关系

操作名称	Tenant Administrator	Tenant Guest	OBS Buckets Viewer
列举桶	可以	可以	可以
创建桶	可以	不可以	不可以
删除桶	可以	不可以	不可以
获取桶基本信息	可以	可以	可以
管理桶访问权限	可以	不可以	不可以
管理桶策略	可以	不可以	不可以

操作名称	Tenant Administrator	Tenant Guest	OBS Buckets Viewer
修改桶存储类别	可以	不可以	不可以
列举对象	可以	可以	不可以
列举多版本对象	可以	可以	不可以
上传文件	可以	不可以	不可以
新建文件夹	可以	不可以	不可以
删除文件	可以	不可以	不可以
删除文件夹	可以	不可以	不可以
下载文件	可以	可以	不可以
删除多版本文件	可以	不可以	不可以
下载多版本文件	可以	可以	不可以
修改对象存储类别	可以	不可以	不可以
恢复文件	可以	不可以	不可以
取消删除文件	可以	不可以	不可以
删除碎片	可以	不可以	不可以
管理对象访问权限	可以	不可以	不可以
设置对象元数据	可以	不可以	不可以
获取对象元数据	可以	可以	不可以
管理多版本控制	可以	不可以	不可以
管理日志记录	可以	不可以	不可以
管理事件通知	可以	不可以	不可以
管理生命周期规则	可以	不可以	不可以
管理静态网站托管	可以	不可以	不可以
管理CORS规则	可以	不可以	不可以
管理防盗链	可以	不可以	不可以
域名管理	可以	不可以	不可以
管理跨区域复制	可以	不可以	不可以
设置对象ACL	可以	不可以	不可以
设置指定版本对象ACL	可以	不可以	不可以
获取对象ACL	可以	可以	不可以

操作名称	Tenant Administrator	Tenant Guest	OBS Buckets Viewer
获取指定版本对象ACL	可以	可以	不可以
多段上传	可以	不可以	不可以
列举已上传段	可以	可以	不可以
取消多段上传任务	可以	不可以	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 约束与限制

本章介绍OBS一些主要特性的使用限制。

表 1-6 OBS 使用限制

限制项	说明
带宽	单个账号默认的读写（GET/PUT）带宽上限是16Gbit/s。如果带宽达到该阈值，请求会触发流控。
每秒请求数（Query Per Second, QPS）	• 单个账号默认的写请求（PUT Object）上限是6000请求每秒。 • 单个账号默认的读请求（GET Object）上限是10000请求每秒。 • 单个账号默认的列举类请求（LIST）上限是1000请求每秒。 **说明** 如果用户在对象命名规则上使用了顺序前缀（如时间戳或字母顺序），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。会使热点分区上的请求速率受限，访问时延上升。 推荐使用随机前缀对象名，这样请求就会均匀分布在多个分区，达到水平扩展的效果。
访问规则	OBS基于DNS解析性能和可靠性的考虑，要求凡是携带桶名的请求，在构造URL的时候都必须将桶名放在domain前面，形成三级域名形式，又称为虚拟主机访问域名。 例如，如果您有一个位于eu-west-0区域的名为test-bucket的桶，期望访问桶中一个名为test-object对象的acl，正确的访问URL为https://test-bucket.oss.eu-west-0.prod-cloud-ocb.orange-business.com/test-object?acl

限制项	说明
桶	• 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，也不能与其他用户创建的桶名称相同。 • 桶创建成功后，桶名、所属区域和数据冗余存储策略均不允许修改。 • 一个账号及账号下的所有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。 • 默认情况下，OBS系统和单个桶都没有总数据容量和对象数量的限制。 • 删除桶之前必须确保桶内所有对象已彻底删除。 • 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。
上传对象	• 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。如果只上传1个文件，则这个文件最大为5GB。 • OBS Browser+、obsutil、API和SDK上传的单个对象最大是48.8TB。 • 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。 • 对象键（对象名）虽然可以使用任何UTF-8字符，但是建议按照**对象键命名指导原则**进行命名，有助于最大程度符合DNS、Web安全字符、XML分析器和其他API的要求。
删除对象	桶没有开启多版本控制功能时，对象删除后不可恢复，请谨慎操作。
恢复冷存储对象	• 冷存储的对象正在恢复的过程中，不允许暂停或删除恢复任务。 • 对象的恢复状态为恢复中时，对象不能再次恢复。 • 数据恢复后，会产生一个标准存储类别的对象副本，即对象同时存在标准存储类别的对象副本和冷存储类别的对象。恢复有效期到期后标准存储类别的对象副本会自动删除。
生命周期管理	单个桶的生命周期规则条数没有限制，但一个桶中所有生命周期规则的XML描述总大小不能超过20KB。
跨区域复制	详见**跨区域复制简介**

限制项	说明
自定义域名绑定	• 桶版本号为3.0及以上的桶支持自定义绑定域名功能。 • OBS自定义域名绑定暂时不支持HTTPS访问自定义域名，只支持HTTP访问自定义域名。 • 一个自定义域名只能绑定到一个桶域名上。 • 绑定的自定义域名后缀目前支持的范围为2~6个英文大小写字母。
ACL	• 一个桶的桶ACL最多支持100条授权，所有桶ACL策略大小总和不超过50KB。 • 一个对象的对象ACL最多支持100条授权，所有对象ACL策略大小不超过50KB。
桶策略	单个桶的桶策略条数（statement）没有限制，但一个桶中所有桶策略的JSON描述总大小不能超过20KB。
并行文件系统	详见《对象存储并行文件系统特性指南》

1.6 与其他服务的关系

表 1-7 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**
通过CES服务监控桶的上传流量、下载流量、GET类请求次数、PUT类请求次数、GET类请求首字节平均时延、4xx异常次数和5xx异常次数。	云监控服务（Cloud Eye Service）	**对象存储服务监控指标说明**
通过事件通知发送警报或触发工作流，并通过消息通知服务（SMN）发送通知。	消息通知服务（Simple Message Notification，SMN）	**SMN通知简介**
通过密钥管理KMS功能对上传到OBS中的文件进行加密。	密钥管理服务（Key Management Service，KMS）	**服务端加密简介**
通过DNS服务为托管在OBS上的静态网站做域名解析。	云解析服务（Domain Name Service，DNS）	**使用自定义域名托管静态网站**

OBS可以作为其他云服务的存储资源池，例如关系型数据库（Relational Database Service，RDS），云审计服务（Cloud Trace Service，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”。

上传对象时，可以指定对象的存储类别，如果不指定，默认与桶的存储类别一致。上传后，对象的存储类别可以修改。

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。

对象键命名指导原则

虽然您可以在对象键名称中使用任何UTF-8字符，但是按照以下规则命名有助于确保与其他应用程序的最大兼容性。每个应用程序对特殊字符的分析方式可能不同。以下指导原则有助于最大程度符合DNS、Web安全字符、XML分析器和其他API的要求。

以下字符集通常可安全地用于键名称：

字母数字字符（通常也被称为非保留字符）	[0-9a-zA-Z]

特殊字符（通常也被称为保留字符）	感叹号（“!”） 连字符（“-”） 下划线（“_”） 句点（“.”） 星号（“*”） 单引号（“'”） 左括号（“(”） 右括号（“)”）

以下是有效对象键名称的示例：

```
4my-organization
my.great_photos-2014/jan/myvacation.jpg
videos/2014/birthday/video1.wmv
```

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。

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

对象存储服务设置有三类桶存储类别，分别为：标准存储、温存储、冷存储，从而满足客户业务对存储性能、成本的不同诉求。创建桶时可以指定桶的存储类别，桶的存储类别可以修改。

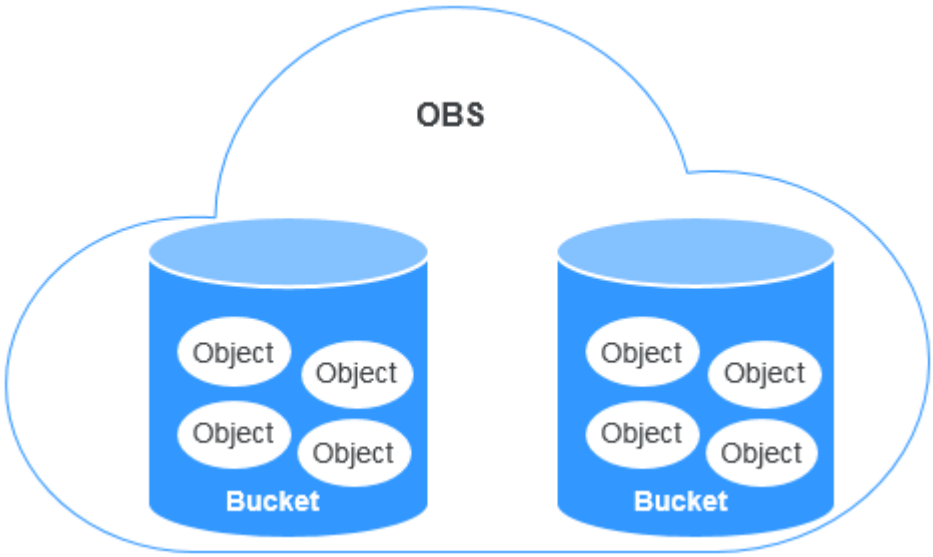
在OBS中，桶名必须是全局唯一的且不能修改，即用户创建的桶不能与自己已创建的其他桶名称相同，也不能与同账号、其他账号及账号下的所有IAM用户创建的桶名称相同。桶所属的区域在创建后也不能修改。每个桶在创建时都会生成默认的桶ACL（Access Control List，访问控制列表），桶ACL的每项包含了对被授权用户授予什么样的权限，如读取权限、写入权限等。用户只有对桶有相应的权限，才可以对桶进行操作，如创建、删除、显示、设置桶ACL等。

一个账号及账号下的所有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1-6**所示：

图 1-6 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《对象存储服务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

说明

访问“欧洲-巴黎”区域的OBS，需要联系管理员获取访问密钥（AK/SK），单击**这里**查看获取方法。

- 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，可以访问指定账号下所有资源。

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 1-8 OBS 资源管理工具

工具	AK/SK配置方式
OBS Browser+	在配置账号时配置AK和SK。
obsutil	在初始化配置时配置AK和SK。
obsfs	在初始化配置时配置AK和SK。
SDK	在初始化阶段设置AK和SK。

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。

不同服务不同区域的终端节点不同，OBS的终端节点信息如下表所示。

表 1-9 OBS 终端节点信息

区域名称	区域	终端节点（Endpoint）	协议类型
欧洲-巴黎	eu-west-0	oss.eu-west-0.prod-cloud-ocb.orange-business.com	HTTPS/HTTP

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1-10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 1-10 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。 OBS的终端节点信息如**表 1-9**所示。	HTTPS HTTP
桶访问域名	**BucketName.Endpoint**	桶创建成功后，可以使用桶访问域名来访问桶。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。	HTTPS 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，或在SDK上通过调用GetObjectUrl接口获取。	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
自定义域名	用户在域名提供商注册的自有域名	你可以为桶绑定用户自定义的域名，通过用户自定义的域名访问桶。	HTTP

1.7.6 区域和可用区

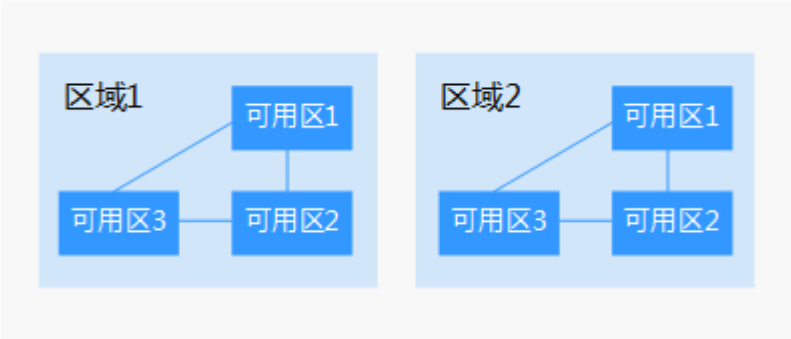
什么是区域、可用区?

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1-7阐明了区域和可用区之间的关系。

图 1-7 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。OBS的终端节点信息如**表1-9**所示。

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）创建不同存储类别的桶、删除桶、修改桶的存储类别等。
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、修改对象的存储类别、恢复冷存储对象等。
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。
监控	• Cloud Eye可监控OBS服务如下指标： – 下载流量 – 上传流量 – GET类请求次数 – PUT类请求次数 – GET类请求首字节平均时延 – 4xx错误次数 – 5xx错误次数
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。

功能	说明
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。
事件通知	方便用户接收OBS对象存储的消息通知。
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或者定时转换对象的存储类别。
跨区域复制	跨区域复制是指通过创建跨区域复制规则，在同一个账号下，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。
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。
配置自定义域名	用户可以将自己的网站域名绑定到桶域名上。适用于以下场景：当用户需要将网站中的文件迁移到OBS，并且不想修改网页的代码，即保持网站的链接不变。
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。

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

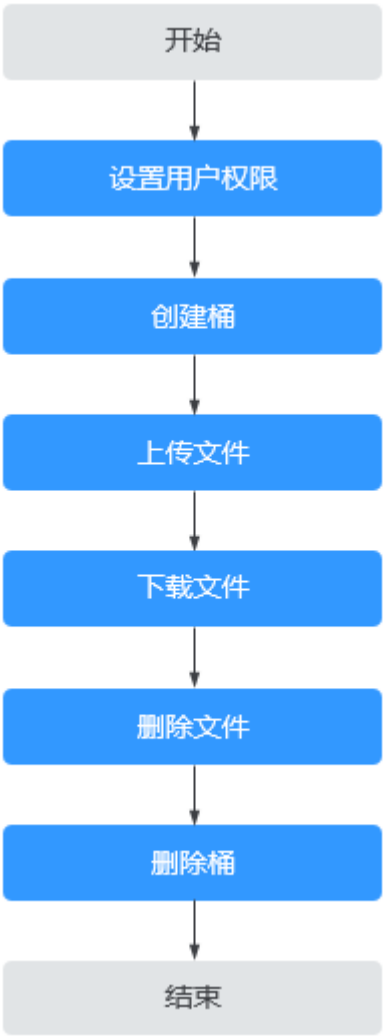
2.3 入门

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



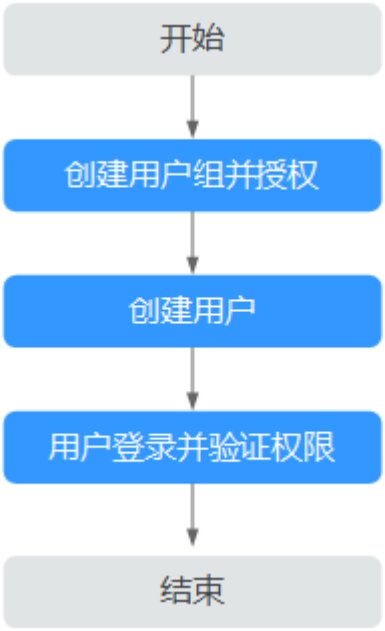
2.3.2 设置用户权限

如果云服务账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。

如果您使用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 使用云服务账号登录管理控制台。

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”，单击“确定”。
   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“修改”。
5. 在“用户组权限”区域中，单击“全局服务 > 对象存储服务”操作列的“修改”，选中策略名称，单击“确定”完成用户组授权。

说明

在“策略内容”中您可以查看到授权的详细信息。

步骤4 创建用户操作详见《统一身份认证服务用户指南》的“创建IAM用户”章节。

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

一个账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”。

步骤2 配置桶参数。

表 2-3 桶参数说明

参数	描述
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。 • 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（.）。
存储类别	桶的存储类别。不同的存储类别可以满足客户业务对存储性能、成本的不同诉求。 • 标准存储：适用于有大量热点文件或小文件，且需要频繁访问（平均一个月多次）并快速获取数据的业务场景。 • 温存储：适用于不频繁访问（平均一年少于12次），但需要快速获取数据的业务场景。 • 冷存储：适用于很少访问（平均一年一次），且对数据获取速率要求不高的业务场景。 更多详情请参见**存储类别简介**。

参数	描述
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。
默认加密	开启桶默认加密后，上传到桶中的对象都会被加密，KMS密钥会默认选中“obs/default”。您也可以通过单击“创建KMS密钥”进入密钥管理服务页面创建自定义的密钥加密上传对象，然后通过KMS密钥的下拉框选中您创建的KMS密钥。 如果桶已开启了默认加密，上传对象会继承桶的KMS加密特性。
多AZ	开启多AZ后，数据冗余存储至多个AZ中。 • 请根据业务情况提前规划是否开启多AZ功能，桶一旦创建成功，后续无法修改多AZ功能的启停状态。 • 冷存储的桶不支持多AZ功能。

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工具（OBS Browser+、obsutil）或OBS SDK和API的多段上传接口上传，大小上限为48.8TB。

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。
- 如果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OBS管理控制台桶列表中，单击待操作的桶，进入“概览”页面。

步骤2 在左侧导航栏，单击“对象”。

步骤3 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4 指定对象的存储类别。如果不指定，默认与桶的存储类别一致。

说明

对象存储类别和桶存储类别可以不一致。上传对象时，对象的存储类别默认继承桶的存储类别，您也可以重新指定对象的存储类别，同时也支持在对象上传完成后修改对象的存储类别。

步骤5 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6 **可选**：勾选“KMS加密”，用于加密上传文件。详情请参见**使用服务端加密方式上传对象**。

说明

如果桶已开启了默认加密，上传对象会继承桶的KMS加密特性。

步骤7 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。

约束与限制

对于存储类别为冷存储的对象，需要确认对象的状态为“已恢复”才能对其进行下载。

操作步骤

步骤1 在OBS管理控制台桶列表中，单击待操作的桶，进入“概览”页面。

步骤2 在左侧导航栏，单击“对象”。

步骤3 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OBS管理控制台桶列表中，单击待操作的桶，进入“概览”页面。

步骤2 在左侧导航栏，单击“对象”。

步骤3 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4 单击“是”，确认删除文件。

----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。建议通过给目录**配置生命周期规则**来删除，符合生命周期规则的目录下的文件会在到期后被删除。

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 存储类别简介

OBS支持桶级和对象级存储类别。

存储类别可以分为：标准存储、温存储、冷存储。

不同的存储类别可以满足客户业务对存储性能、成本的不同诉求。

- 标准存储访问时延低和吞吐量高，因而适用于有大量热点文件（平均一个月多次）或小文件（小于1MB），且需要频繁访问数据的业务场景，例如：大数据、移动应用、热点视频、社交图片等场景。
- 温存储适用于不频繁访问（平均一年少于12次）但在需要时也要求快速访问数据的业务场景，例如：文件同步/共享、企业备份等场景。
- 冷存储适用于很少访问（平均一年访问一次）数据的业务场景，例如：数据归档、长期备份等场景。冷存储安全、持久且成本极低，可以用来替代磁带库。为了保持成本低廉，数据恢复时间可能长达数分钟到数小时不等。

桶存储类别和对象存储类别的关系

上传对象时，对象的存储类别默认继承桶的存储类别。您也可以重新指定对象的存储类别。

修改桶的存储类别，桶内已有对象的存储类别不会修改，新上传对象时的默认对象存储类别随之修改。

存储类别对比

对比项目	标准存储	温存储	冷存储
特点	高性能、高可靠、高可用的对象存储服务	高可靠、较低成本的实时访问存储服务	冷数据的长期存储，存储单价更优惠
应用场景	云应用、数据分享、内容分享、热点对象	网盘应用、企业备份、活跃归档、监控数据	档案数据、医疗影像、视频素材、带库替代
最小计量单位[a]	64KB	64KB	64KB
最低存储时间[b]	无	30天	90天

2.5 桶管理

2.5.1 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

一个账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”。

步骤2 配置桶参数。

表 2-4 桶参数说明

参数	描述
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。 ● 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（.）。
存储类别	桶的存储类别。不同的存储类别可以满足客户业务对存储性能、成本的不同诉求。 ● 标准存储：适用于有大量热点文件或小文件，且需要频繁访问（平均一个月多次）并快速获取数据的业务场景。 ● 温存储：适用于不频繁访问（平均一年少于12次），但需要快速获取数据的业务场景。 ● 冷存储：适用于很少访问（平均一年一次），且对数据获取速率要求不高的业务场景。 更多详情请参见**存储类别简介**。
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。
默认加密	开启桶默认加密后，上传到桶中的对象都会被加密，KMS密钥会默认选中“obs/default”。您也可以通过单击“创建KMS密钥”进入密钥管理服务页面创建自定义的密钥加密上传对象，然后通过KMS密钥的下拉框选中您创建的KMS密钥。 如果桶已开启了默认加密，上传对象会继承桶的KMS加密特性。

参数	描述
多AZ	开启多AZ后，数据冗余存储至多个AZ中。 ● 请根据业务情况提前规划是否开启多AZ功能，桶一旦创建成功，后续无法修改多AZ功能的启停状态。 ● 冷存储的桶不支持多AZ功能。

步骤3 单击“立即创建”。

----结束

相关操作

您可以在创建桶时指定桶的存储类别，也可以在创建后修改桶的存储类别。修改步骤如下：

步骤1 在OBS管理控制台桶列表中，选择待操作的桶，并单击右侧的“修改存储类别”。

步骤2 选择目标存储类别，并单击“确定”。

说明

- 修改桶的存储类别后，不会影响已存储在桶内的对象的存储类别。
- 上传对象时，默认的对象存储类别与桶的存储类别一致。当桶存储类别修改后，新上传对象时的默认对象存储类别随之修改。

----结束

2.5.2 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OBS管理控制台桶列表中，单击待操作的桶，进入“概览”页面。

步骤2 在“基本信息”下查看桶的基本信息。

表 2-5 桶信息参数说明

参数	说明
桶名称	桶的名称。
存储类别	桶的存储类别，有标准存储、温存储、冷存储三种类别。
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。

参数	说明
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。
拥有者	拥有者是指创建桶的账号。
账号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*
多AZ	多AZ功能的状态。 开启多AZ后，数据冗余存储至多个AZ中。

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

2.5.3 搜索桶

OBS管理控制台支持按桶名所包含的字符串搜索桶。

操作步骤

步骤1 在OBS管理控制台页面右上角的搜索框中输入需要查找的桶。

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”、“存储类别”、“区域”、“存储用量”、“对象数量”和“创建时间”进行排序，您可以单击参数后的 按钮进行排序。

2.5.4 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

2.6 对象管理

2.6.1 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OBS管理控制台桶列表中，单击待操作的桶，进入“概览”页面。

步骤2 在左侧导航栏，单击“对象”。

步骤3 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4 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5 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。

2.6.2 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工具（OBS Browser+、obsutil）或OBS SDK和API的多段上传接口上传，大小上限为48.8TB。
- 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。
- 如果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OBS管理控制台桶列表中，单击待操作的桶，进入“概览”页面。

步骤2 在左侧导航栏，单击“对象”。

步骤3 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4 指定对象的存储类别。如果不指定，默认与桶的存储类别一致。

说明

对象存储类别和桶存储类别可以不一致。上传对象时，对象的存储类别默认继承桶的存储类别，您也可以重新指定对象的存储类别，同时也支持在对象上传完成后修改对象的存储类别。

步骤5 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6 **可选**：勾选“KMS加密”，用于加密上传文件。详情请参见**使用服务端加密方式上传对象**。

说明

如果桶已开启了默认加密，上传对象会继承桶的KMS加密特性。

步骤7 单击“上传”。

----结束

相关操作

您可以在上传对象时指定对象的存储类别，也可以在上传后修改对象的存储类别，修改步骤如下：

步骤1 在OBS管理控制台桶列表中，单击待操作的桶，进入“概览”页面。

步骤2 在左侧导航栏，单击“对象”。

步骤3 选中目标对象，并单击右侧“更多>修改存储类别”。

步骤4 选择目标存储类别，并单击“确定”。

----结束

说明

- 标准存储的对象可以修改为温存储或冷存储的对象。温存储的对象可以修改为标准存储或冷存储的对象。冷存储的对象要先恢复，才可以修改为标准存储或温存储。后两种修改会涉及恢复费用，请根据对象的使用频率和场景择优选择。
- 对象存储类别修改为冷存储时，恢复状态为未恢复。
- 您也可以通过配置生命周期规则转换对象的存储类别，详情请参见**配置生命周期规则**。

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。

2.6.3 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。

约束与限制

对于存储类别为冷存储的对象，需要确认对象的状态为“已恢复”才能对其进行下载。

操作步骤

步骤1 在OBS管理控制台桶列表中，单击待操作的桶，进入“概览”页面。

步骤2 在左侧导航栏，单击“对象”。

步骤3 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

2.6.4 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。
- 冷存储对象需恢复后才能分享。

相关操作

步骤1 在OBS管理控制台桶列表中，单击待操作的桶，进入“概览”页面。

步骤2 在左侧导航栏，单击“对象”。

步骤3 在待分享文件的操作列，单击“更多 > 复制对象URL”。

此时，临时URL便已经生效并开始计时，有效期固定为900s。在有效期内，任何人均可以通过此临时URL访问文件。

----结束

2.6.5 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OBS管理控制台桶列表中，单击待操作的桶，进入“概览”页面。

步骤2 在左侧导航栏，单击“对象”。

步骤3 在对象列表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4 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。

2.6.6 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OBS管理控制台桶列表中，单击待操作的桶，进入“概览”页面。

步骤2 在左侧导航栏，单击“对象”。

步骤3 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。

说明

- 对于存储类别为冷存储的对象，如果要让匿名用户通过URL访问，则需要先确认对象的状态是否为“已恢复”。

----结束

2.6.7 恢复冷存储文件

对于存储类别为冷存储的对象，用户需要先恢复才能下载、通过对象URL访问对象、配置对象的ACL权限、设置对象元数据。

约束与限制

- 冷存储的对象正在恢复的过程中，不允许暂停或删除恢复任务。
- 对象的恢复状态为恢复中时，对象不能再次恢复。
- 数据恢复恢复后，会产生一个标准存储类别的对象副本，即对象同时存在标准存储类别的对象副本和冷存储类别的对象，恢复有效期到期后标准存储类别的对象副本会自动删除。

操作步骤

步骤1 在OBS管理控制台桶列表中，单击待操作的桶，进入“概览”页面。

步骤2 在左侧导航栏，单击“对象”。

步骤3 选中待恢复的文件，并单击右侧的“恢复”。

也可以选中多个文件，单击文件列表上方的“恢复”恢复多个文件。

说明

恢复中的对象不能加入批量恢复文件中。

步骤4 恢复对象需要设置对象的有效期和恢复速率，参数解释如下表所示：

表 2-6 恢复对象

参数	说明
有效期	对象恢复后，保持为“已恢复”状态的时长，从对象恢复完成开始计时。有效期时长可设置1-30天的整数。系统默认有效期为30天。 例如：恢复对象时，有效期设置为20天，则从对象恢复成功后开始算起，20天后，该对象则会从“已恢复”状态变成“未恢复”状态。
速率	对象的恢复速度。 ● 加急：可在1-5分钟内恢复冷存储数据。 ● 标准：可在3-5小时内恢复冷存储数据。 ● 慢速：可在5-12小时内以较低的成本恢复大量（千兆字节）数据。

步骤5 单击“确定”。

对象恢复状态可在对象列表中查看。

单击页面右上角的“刷新”按钮 可手动刷新恢复任务状态。

说明

系统每天会在UTC 00:00点检查一次文件恢复情况，过期时间是根据最近一次系统检查时间开始计算的。

----结束

相关操作

在对象有效期内，用户可以重复做对象恢复操作。对象的有效期会以最新一次的恢复完成时间为开始算起，以此可以达到延长对象有效期的目的。

说明

重复恢复对象时，其过期时间应该在上一次恢复对象的过期时间之后。例如，1月1号恢复对象并设置30天后过期，过期时间是1月30号。1月10号时重复恢复对象，过期时间设置如果早于30号（天数小于20天），那么此恢复操作是非法的。

2.6.8 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OBS管理控制台桶列表中，单击待操作的桶，进入“概览”页面。

步骤2 在左侧导航栏，单击“对象”。

步骤3 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4 单击“是”，确认删除文件或文件夹。

注意

如果您的删除对象所在的OBS桶启用了多版本控制功能，那么删除的对象不会被立即删除，而是保留在“已删除对象”列表中，该对象的历史版本仍然会被保存下来且会占用存储空间，因此OBS仍然会对所有版本收取存储费用。如果您不再需要该对象，为避免删除后持续计费，请再按照以下步骤进行彻底删除。

步骤5 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。

----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：

- 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。

2.6.9 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。
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OBS管理控制台桶列表中，单击待操作的桶，进入“概览”页面。

步骤2 在左侧导航栏，单击“对象”。

步骤3 单击“已删除对象”。

步骤4 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OBS管理控制台桶列表中，单击待操作的桶，进入“概览”页面。

步骤2 在左侧导航栏，单击“对象”。

步骤3 单击“已删除对象”。

步骤4 单击要找回的文件名称，系统显示该文件信息。

步骤5 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

2.6.10 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OBS管理控制台桶列表中，单击待操作的桶，进入“概览”页面。

步骤2 在左侧导航栏，单击“对象”。

步骤3 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4 单击“是”，确认删除碎片。

----结束

2.7 服务端加密

2.7.1 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)和客户提供加密密钥的服务端加密（SSE-C）两种方式，SSE-C方式是指OBS使用用户提供的密钥和密钥的MD5值进行服务端加密。上述两种方式都采用行业标准的AES256加密算法。

2.7.2 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OBS管理控制台桶列表中，单击待操作的桶，进入“概览”页面。

步骤2 在概览页的“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3 选择“开启”。

开启“KMS加密”后，KMS密钥会默认选中“obs/default”。您也可以通过单击“创建KMS密钥”进入密钥管理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4 单击“确定”。

----结束

关闭桶默认加密

步骤1 在OBS管理控制台桶列表中，单击待操作的桶，进入“概览”页面。

步骤2 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3 选择“关闭 ”。

步骤4 单击“确定”。

----结束

2.7.3 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。
- 服务端加密的对象不支持分享。

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OBS管理控制台桶列表中，单击待操作的桶，进入“概览”页面。

步骤2 在左侧导航栏，单击“对象”。

步骤3 单击“上传对象”，系统弹出“上传对象”对话框。

步骤4 添加待上传的文件。

步骤5 勾选“KMS加密”，在后面的选择框中选择您在密钥管理服务中创建的KMS密钥。

说明

如果桶已开启了默认加密，上传对象会继承桶的KMS加密特性。

当勾选“KMS加密”后，KMS密钥会默认选中“obs/default”。您也可以通过单击“创建KMS密钥”进入密钥管理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6 单击“上传”。

对象上传成功后，可在对象详情中查看对象的加密状态。

----结束

2.8 对象元数据

2.8.1 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 2-7 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。

名称	说明
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。

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。
- 对于存储类别为冷存储的对象，不能对其设置对象的元数据。

2.8.2 配置对象元数据

操作步骤

步骤1 在OBS管理控制台桶列表中，单击待操作的桶，进入“概览”页面。

步骤2 在左侧导航栏，单击“对象”。

步骤3 单击待操作的对象，然后再单击“元数据”。

步骤4 单击“增加”。根据需要填写元数据信息。

步骤5 单击“保存”。

----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用户或其他账号授权桶及桶内对象的操作权限。

  说明

  通过桶策略对VDC只读管理员授予的权限中，只有读类型的权限能生效，例如列举对象、下载对象。VDC只读管理员不能执行资源的修改操作。

  对象策略是桶策略中针对对象的策略。
- ACL：OBS ACL是基于账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，您可以在云账号中创建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策略主要面向对同账号下IAM用户授权的场景：

- 使用策略控制账号下整个云资源的权限时，使用IAM策略授权。
- 使用策略控制账号下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 2-3 策略结构

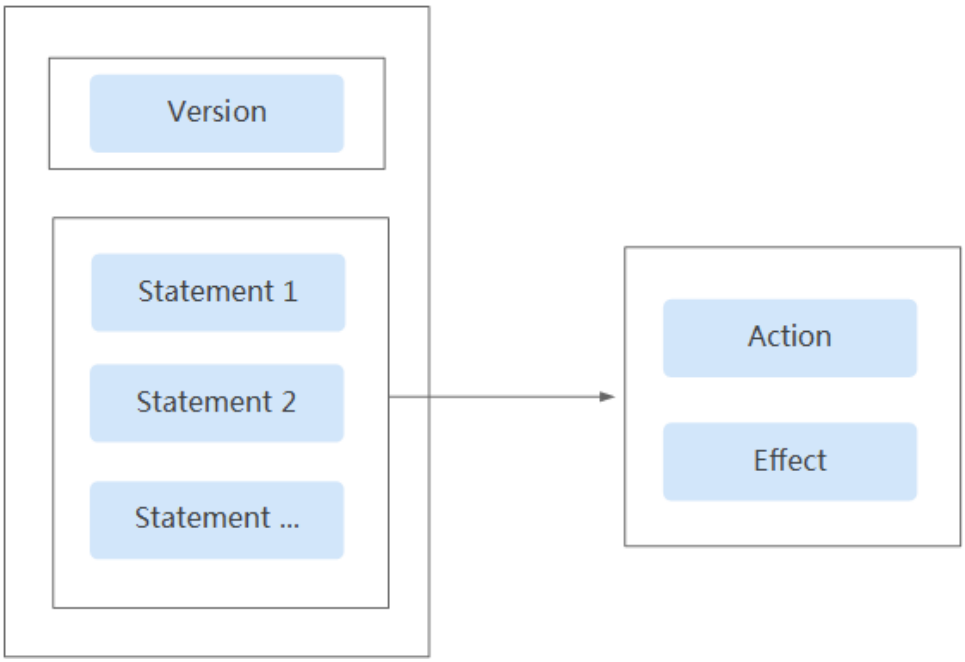


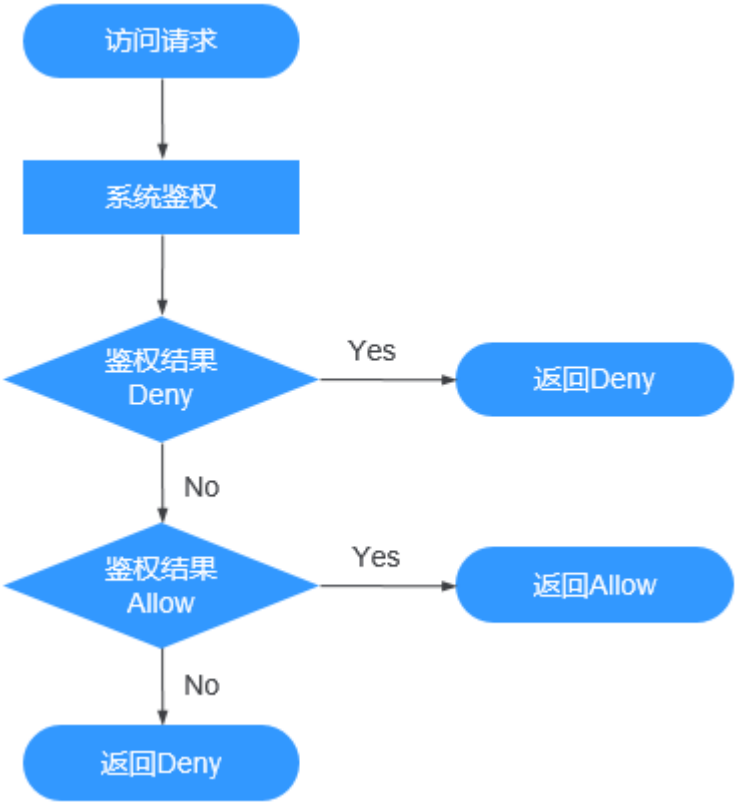
表 2-8 策略语法参数

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。

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 2-4 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账号。一个账号下的IAM用户创建的桶，桶拥有者为该IAM用户的父级账号。

对象的拥有者是上传对象的账号，而不是对象所属的桶的拥有者。例如，如果账号B被授予访问账号A的桶的权限，然后账号B上传一个文件到桶中，则账号B是对象的拥有者，而不是账号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用户或其他账号授权桶及桶内对象的操作权限。

说明

通过桶策略对VDC只读管理员授予的权限中，只有读类型的权限能生效，例如列举对象、下载对象。VDC只读管理员不能执行资源的修改操作。

桶策略的应用场景：

- 不用IAM策略控制访问权限的情况下，允许其他账号访问OBS资源，可以使用桶策略的方式授权其他账号对应的权限。
- 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。
- 桶拥有者允许其他账号访问自己的桶时，可使用桶策略授权其他账号对应的权限。

标准桶策略：

标准桶策略提供三种策略供用户直接设置。

- 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。

桶创建成功后，默认桶策略为私有，仅桶拥有者具有完全控制权限，其他用户在未经授权的情况下均无访问权限。为确保数据安全，不推荐用户使用公共读或公共读写，建议使用私有。

表 2-9 标准桶策略描述

参数	私有	公共读	公共读写
效果	无	允许	允许
被授权用户	无	*（任何用户）	*（任何用户）
资源	无	*（桶内所有对象）	*（桶内所有对象）
动作	无	• GetObject • GetObjectVersion • ListBucket	• GetObject • GetObjectVersion • PutObject • DeleteObject • DeleteObjectVersion • ListBucket
条件	无	无	无

说明

在桶版本号为3.0的桶中，我们更新了公共读和公共读写的默认权限，以解决在Browser挂载外部桶时权限不足的问题：

- 公共读权限增加了ListBucket权限。
- 公共读写权限增加了ListBucket权限。
- 如果您需要在Browser挂载外部桶，请手动更新标准桶策略配置。

高级桶策略：

高级桶策略提供三种方式，方便用户快速设置桶策略。

- 只读模式：被授权用户将拥有桶内指定对象的读权限，对应可以执行获取对象内容及元数据操作。
- 读写模式：被授权用户将拥有桶内指定对象的读写权限，对应可以执行获取对象内容及元数据、上传对象、删除对象等操作。
- 自定义模式：自定义配置被授权用户可以拥有桶或对象的操作权限，由效果、被授权用户、资源、动作和条件5个桶策略基本参数共同决定。

说明

通常情况下，在控制台上通过高级桶策略给其他用户授予桶中资源的某些操作权限，需要同时授予用户桶的读权限ListBucket（配置策略时资源留空表示对桶授权），否则可能导致用户从控制台进入桶后提示没有权限。

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。

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，它定义了哪些账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账号或OBS预定义的群组，详细信息如**表2-10**所示。

表 2-10 OBS 支持的被授权用户

被授权用户	描述
特定用户	ACL支持通过账号授予桶/对象的访问权限。授予账号权限后，账号下所有具有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账号。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账号，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。
注册用户组	注册用户组代表所有注册了云服务的账号（仅指账号，不包括通过IAM创建的用户组或用户）。注册用户必须要经过身份认证（目前主要通过AK/SK进行身份认证），才可以获取对应的访问权限。例如，当注册用户组被授予桶写入权限后，世界上任何已通过身份验证的云服务账号，都可以向您的桶上传、覆盖和删除对象。
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本身不能在账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，只能由账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。如果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2-11**所示：

表 2-11 桶 ACL 访问权限

权限	选项	描述
桶访问权限	读取权限 READ	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
	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2-12所示：

表 2-12 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2-13所示。

表 2-13 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是基于账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：

- 授予日志投递用户组桶写入权限，用以存储桶访问请求日志。
- 授予指定账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是基于账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2-14所示。

表 2-14 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2-15所示。

表 2-15 对象 ACL 和桶策略的映射关系

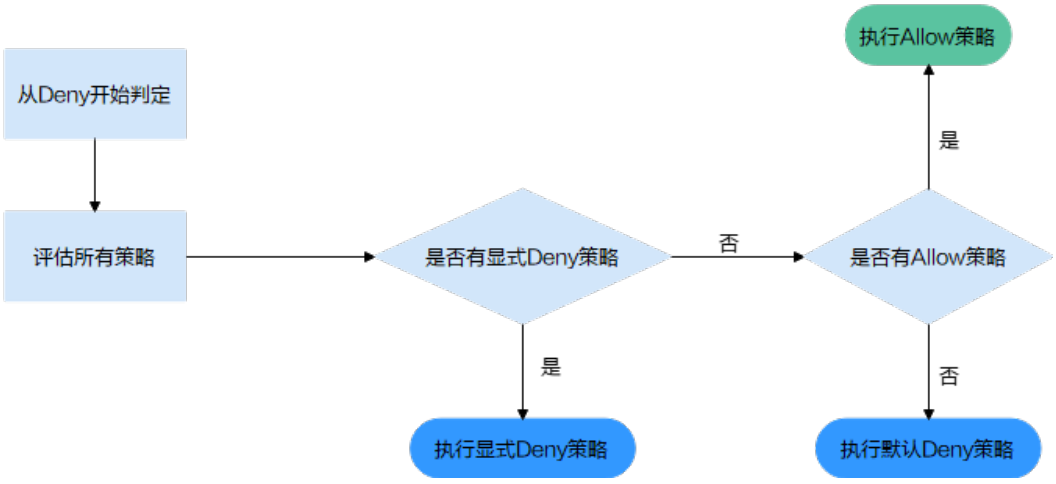
对象ACL权限	选项	对应桶策略高级设置中的动作
对象访问权限	读取权限	• GetObject • GetObjectVersion
ACL访问权限	读取权限	• GetObjectAcl • GetObjectVersionAcl
	写入权限	• PutObjectAcl • PutObjectVersionAcl

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 2-5 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2-6所示。

图 2-6 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

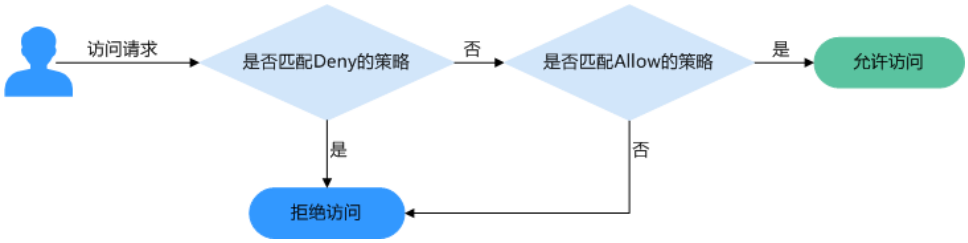
2.9.3.1 效果

桶策略的效果，具体表现为拒绝或允许请求。

- 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 2-7 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效果设置为拒绝（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，这里的用户可以是账号，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。

说明

通过桶策略对VDC只读管理员授予的权限中，只有读类型的权限能生效，例如列举对象、下载对象。VDC只读管理员不能执行资源的修改操作。

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，配置方法为在资源输入框中不输入任何内容。

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 2-16 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。
	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。

类型	值	描述
	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 2-17 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。
	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。

类型	值	描述
	AbortMultipartUpload	取消多段上传任务。

2.9.3.5 条件

除了指定效果、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，账号A想要拥有账号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账号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2-18所示的预定义条件运算符。

表 2-18 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。
	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。

类型	关键字	说明
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 2-19 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。

键	类型	描述
Referer	String	请求从哪个链接发起。

表 2-20 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。	
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。	
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 2-21 与对象动作相关的键

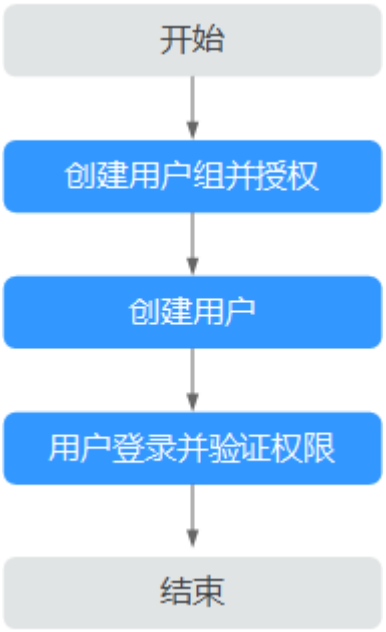
Action	可选键	描述
PutObject	acl	String类型，设置对象ACL。上传对象时在头域中可以包含的Canned ACL，取值范围为private|public-read|public-read-write|authenticated-read|bucketowner-read|bucket-owner-full-control|log-delivery-write。
	copysource	String类型，用来指定复制对象时对象操作的源桶名以及源对象名。格式如/bucketname/keyname。
	metadata-directive	String类型，用来指定新对象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-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 2-8 为 IAM 用户授权 OBS 资源权限



操作步骤

步骤1 使用云服务账号登录管理控制台。

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”，单击“确定”。
   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“修改”。
5. 在“用户组权限”区域中，单击“全局服务 > 对象存储服务”操作列的“修改”，选中策略名称，单击“确定”完成用户组授权。

说明

在“策略内容”中您可以查看到授权的详细信息。

步骤4 创建用户操作详见《统一身份认证服务用户指南》的“创建IAM用户”章节。

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 配置标准桶策略

标准桶策略可一键式为桶配置私有、公共读、或公共读写的通用策略。

操作步骤

步骤1 在OBS管理控制台桶列表中，单击待操作的桶，进入“概览”页面。

步骤2 在左侧导航栏，单击“权限”，进入权限管理页面。

步骤3 在“桶策略”页面，“标准桶策略”下通过单击选中卡片配置标准桶策略。

- 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。

说明

为了确保您的数据安全，不推荐配置为公共读或公共读写。

步骤4 在弹出的对话框中单击“是”。

----结束

2.9.5.2 配置高级桶策略

如果期望给予特定用户特定的权限或其他需求，则可以在高级设置下配置。当标准桶策略和高级桶策略有冲突时，以高级桶策略>标准桶策略的优先级顺序决定授权结果。

操作步骤

步骤1 在OBS管理控制台桶列表中，单击待操作的桶，进入“概览”页面。

步骤2 在左侧导航栏，单击“权限”，进入权限管理页面。

步骤3 在“桶策略”页面“高级桶策略”下，根据需求配置高级桶策略。

步骤4 单击“创建桶策略”。根据需求选择合适的策略模式。

- 只读模式：被授权用户将拥有桶内指定对象的读权限，后续操作请参见**步骤5**。
- 读写模式：被授权用户将拥有桶内指定对象的读写权限，后续操作请参见**步骤5**。
- 自定义模式：自定义配置被授权用户可以拥有的桶或对象的操作权限，具体参数配置请参照**步骤6**。

说明

一次只能配置一种策略模式的桶策略。

步骤5 （只读模式或读写模式）依次输入被授权用户和资源，然后单击“确定”，完成桶策略配置。

表 2-22 只读/读写模式下桶策略参数说明

字段	值	描述
被授权用户	• 包含、排除 • 当前账号、其他账号	桶策略作用于的用户。 • 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。
被授权用户	• 包含、排除 • 当前租户、其他租户	桶策略作用于的用户。 • 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。
资源	• 包含、排除 • 输入格式： 对象：*对象名称* 对象集：*“对象名称前缀”*+“*”、“*”+“对象名后缀”或“*”	桶策略作用于的资源。在只读模式和读写模式下，作用的资源只能是对象。 • 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。

步骤6 （自定义模式）根据实际需求配置自定义参数，然后单击“确定”，完成桶策略配置。

各字段的含义如**表2-23**所示。

表 2-23 自定义模式下桶策略参数说明

字段	值	描述
效果	Allow、Deny	桶策略的效果。 • 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。
被授权用户	• 包含、排除 • 当前账号、其他账号	桶策略作用于的用户。 • 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。
被授权用户	• 包含、排除 • 当前租户、其他租户	桶策略作用于的用户。 • 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。

字段	值	描述
资源	• 包含、排除 • 资源输入格式： 对象：*对象名称* 对象集：*“对象名称前缀”*+“*”、“*”+“对象名后缀”或“*” 空：表示资源为整个桶	桶策略作用于的资源。 • 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。 资源的类型与动作相关： • 资源为对象或对象集时，“动作”只能配置对象相关的动作。 • 资源为桶时，“动作”只能配置桶相关的动作。
动作	• 包含、排除 • 详细的动作信息，请参见**动作**。	桶策略描述的操作。 • 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。
条件	• 条件运算符：请参见**表2-18**。 • 键：请参见**通用键**、**与桶动作有关的键**和**与对象动作相关的键**。 • 值：输入的值与键相关。	桶策略生效的条件。

----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OBS管理控制台桶列表中，单击待操作的桶，进入“概览”页面。

步骤2 在左侧导航栏，单击“对象”。

步骤3 在待操作的对象的后面，单击“更多>配置对象策略”，系统弹出“配置对象策略”对话框。

步骤4 根据需求选择合适的策略模式。

- 只读模式：被授权用户将拥有该对象的读权限，后续操作请参见**步骤5**。
- 读写模式：被授权用户将拥有该对象的读写权限，后续操作请参见**步骤5**。
- 自定义模式：自定义配置被授权用户可以拥有的对象的操作权限，具体参数配置请参见**步骤6**。

说明

一次只能配置一种策略模式的对象策略。

步骤5 （只读模式或读写模式）依次输入被授权用户和资源，然后单击“确定”，完成对象策略配置。

表 2-24 只读/读写模式下对象策略参数说明

字段	值	描述
被授权用户	• 包含、排除 • 当前账号、其他账号	对象策略作用于的用户。 • 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。
被授权用户	• 包含、排除 • 当前租户、其他租户	对象策略作用于的用户。 • 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。
资源	包含、排除	对象策略作用于的资源。 • 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。

步骤6 （自定义模式）根据实际需求配置各参数，然后单击“确定”，完成对象策略配置。

表 2-25 自定义模式下对象策略参数说明

字段	值	描述
效果	Allow、Deny	对象策略的效果。 • 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。
被授权用户	• 包含、排除 • 当前账号、其他账号	对象策略作用于的用户。 • 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。

字段	值	描述
被授权用户	• 包含、排除 • 当前租户、其他租户	对象策略作用于的用户。 • 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。
资源	• 包含、排除	对象策略作用于的资源。 • 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。
动作	• 包含、排除 • 详细的动作信息，请参见**对象相关动作含义**。	对象策略描述的操作。 • 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。
条件	• 条件运算符：请参见**表1 各条件运算符含义**。 • 键：请参见**通用键**和**与对象动作相关的键**。 • 值：输入的值与键相关。	对象策略生效的条件。

步骤7 单击“确定”。

对象策略配置成功后，可在“高级桶策略”下查看到该策略。

----结束

2.9.7 配置桶 ACL

前提条件

配置桶ACL的账号需要是桶 的拥有者，或者具备该桶的ACL写权限。

操作步骤

步骤1 在OBS管理控制台桶列表中，单击待操作的桶，进入“概览”页面。

步骤2 在左侧导航栏，单击“权限”，进入权限管理页面。

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、注册用户组、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”，可对特定账号添加ACL权限。

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

步骤5 单击“保存”。

----结束

2.9.8 配置对象 ACL

前提条件

配置对象ACL的账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账号，而不是对象所属的桶的拥有者。例如，如果账号B被授予访问账号A的桶的权限，账号B上传一个文件到桶中，则账号B是对象的拥有者，而不是账号A。默认情况下，账号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OBS管理控制台桶列表中，单击待操作的桶，进入“概览”页面。

步骤2 在左侧导航栏，单击“对象”。

步骤3 单击待操作的对象。

步骤4 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、注册用户组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5 单击“增加”，可对特定账号添加ACL权限。

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

步骤6 单击“保存”。

----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

在主账号下创建一个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（主账号）或者拥有设置桶策略权限的账号及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OBS管理控制台桶列表中，单击待操作的桶，进入“概览”页面。

步骤2 在左侧导航栏，单击“权限”，进入权限管理页面。

步骤3 单击“桶策略>高级桶策略”。

步骤4 单击“创建桶策略”，系统弹出“创建桶策略”对话框。

步骤5 配置如下参数，授予IAM用户访问桶（列举对象）的权限。

表 2-26 授予访问桶的权限的参数配置

参数	取值
策略模式	自定义模式
效果	Allow
被授权用户	• 包含 • 当前账号，并选择需要授权的IAM用户
资源	• 包含 • 资源名称不配置
动作	• 包含 • ListBucket

步骤6 单击“确定”。

步骤7 单击“创建桶策略”，系统弹出“创建桶策略”对话框。

步骤8 配置如下参数，授予IAM用户上传对象的权限。

说明

授予用户对象操作权限前，需先授予其访问桶的权限。

表 2-27 授予上传对象的权限的参数配置

参数	取值
策略模式	自定义模式
效果	Allow
被授权用户	• 包含 • 当前账号，并选择需要授权的IAM用户
资源	• 包含 • 资源名称：*
动作	• 包含 • PutObject **说明** 本例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9 单击“确定”。

----结束

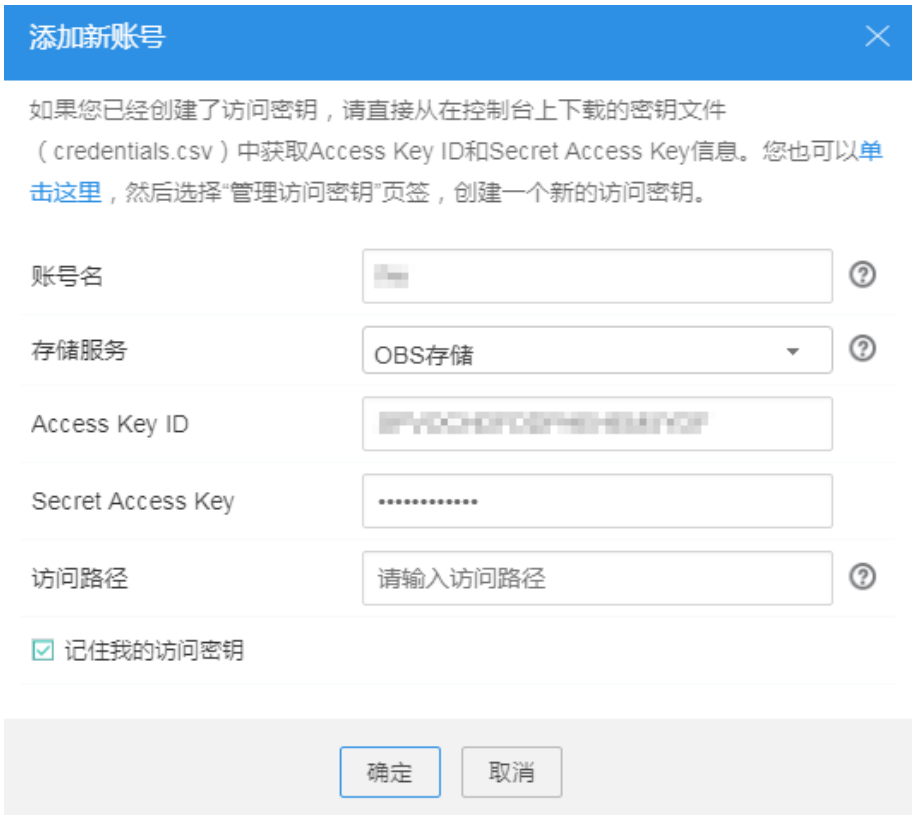
验证

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。

图 2-9 添加新账号-OBS 存储



步骤3 当主账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 主账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。单击页面右上角的，进入“任务管理”界面，“状态”为“失败”，失败原因为“拒绝访问”。

步骤6 主账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 为其他账号授予指定桶的操作权限

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

下面示例以授予其他账号访问桶和上传对象的权限为例。

说明

如果是给其他账号下的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用户所属账号配置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OBS管理控制台桶列表中，单击待操作的桶，进入“概览”页面。

步骤2 在左侧导航栏，单击“权限”，进入权限管理页面。

步骤3 单击“桶策略>高级桶策略”。

步骤4 单击“创建桶策略”，系统弹出“创建桶策略”对话框。

步骤5 配置如下参数，授予其他账号访问桶的权限。

表 2-28 授予访问桶的权限的参数配置

参数	取值
策略模式	自定义模式
效果	Allow
被授权用户	● 包含 ● 其他账号，并配置账号ID和用户ID **说明** 账号ID和用户ID通过“我的凭证”页面可以获取。如果是授权给账号，用户ID则不用配置；如果是授权给其他账号的IAM用户，还需配置用户ID，授权给多个IAM用户时，用户ID使用英文逗号“,”分隔。
资源	● 包含 ● 资源名称不配置
动作	● 包含 ● ListBucket

步骤6 单击“确定”。

步骤7 单击“创建桶策略”，系统弹出“创建桶策略”对话框。

步骤8 配置如下参数，授予其他账号上传对象的权限。

说明

授予用户对象操作权限前，需先授予其访问桶的权限。

表 2-29 授予上传对象的权限的参数配置

参数	取值
策略模式	自定义模式
效果	Allow
被授权用户	● 包含 ● 其他账号，并配置账号ID和用户ID **说明** 账号ID和用户ID通过“我的凭证”页面可以获取。如果是授权给账号，用户ID则不用配置；如果是授权给其他账号的IAM用户，还需配置用户ID，授权给多个IAM用户时，用户ID使用英文逗号“,”分隔。
资源	● 包含 ● 资源名称：*
动作	● 包含 ● PutObject

步骤9 单击“确定”。

----结束

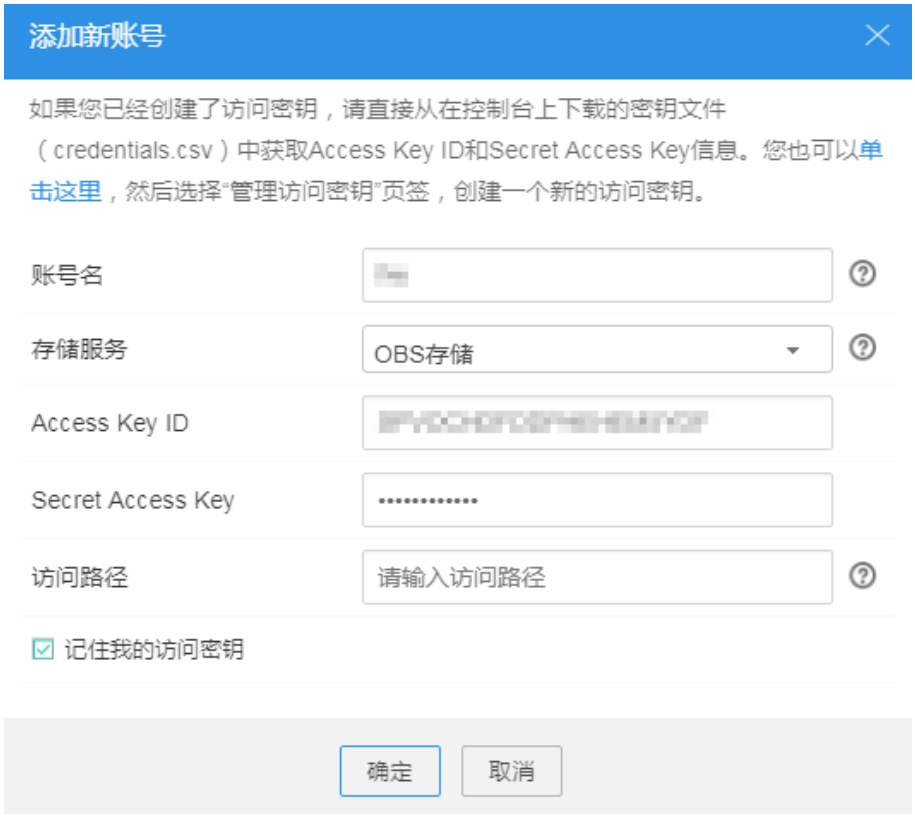
验证

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。

图 2-10 添加新账号-OBS 存储



步骤3 当主账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 主账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。单击页面右上角的，进入“任务管理”界面，“状态”为“失败”，失败原因为“拒绝访问”。

步骤6 主账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OBS管理控制台桶列表中，单击待操作的桶，进入“概览”页面。

步骤2 在左侧导航栏，单击“权限”，进入权限管理页面。

步骤3 单击“桶策略>高级桶策略”。

步骤4 单击“创建桶策略”，系统弹出“创建桶策略”对话框。

步骤5 配置如下参数：

表 2-30 授予访问桶的权限的参数配置

参数	取值
策略模式	自定义模式
效果	Deny
被授权用户	● 包含 > 其他账号 ● 账号ID输入“*”，表示对所有匿名用户的账号生效。 ● 用户ID不填。
资源	● 包含 ● 不配置前缀，表示整个桶资源。
动作	● 包含 ● *，表示所有权限。
条件	● 条件运算符：IpAddress ● 键：SourceIP ● 值：114.115.1.0/24

步骤6 单击“确定”。

----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OBS管理控制台桶列表中，单击待操作的桶，进入“概览”页面。

步骤2 在左侧导航栏，单击“权限”，进入权限管理页面。

步骤3 单击“桶策略>高级桶策略”。

步骤4 单击“创建桶策略”，系统弹出“创建桶策略”对话框。

步骤5 配置如下参数：

表 2-31 授予访问桶的权限的参数配置

参数	取值
策略模式	自定义模式
效果	Allow
被授权用户	● 包含 ● 其他账号，账号ID输入“*”，表示所有匿名用户。
资源	● 包含 ● 资源名称填写“*”，表示桶中所有资源 **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整个桶的自定义桶策略。
动作	● 包含 ● 动作名称选择“*”，表示所有权限。 **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	● 条件运算符：DateGreaterThan ● 键：CurrentTime ● 值：2019-03-26T12:00:00Z（取值为UTC格式）
条件	● 条件运算符：DateLessThan ● 键：CurrentTime ● 值：2019-03-26T15:00:00Z（取值为UTC格式）

说明

上述两个条件需要同时配置在同一条桶策略中。

步骤6 单击“确定”。

----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。

步骤5 单击“保存”保存权限设置。

----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OBS管理控制台桶列表中，单击待操作的桶，进入“概览”页面。

步骤2 在左侧导航栏，单击“权限”，进入权限管理页面。

步骤3 单击“桶策略>高级桶策略”。

步骤4 单击“创建桶策略”，系统弹出“创建桶策略”对话框。

步骤5 配置如下参数，授予匿名用户访问文件夹内对象的权限。

表 2-32 授予访问桶的权限的参数配置

参数	取值
策略模式	自定义模式
效果	Allow
被授权用户	• 包含 • 其他账号，账号ID输入“*”，表示所有匿名用户。
资源	• 包含 • 配置为选中文件夹内的所有对象，如文件夹名称为“folder-001”时，资源值为“folder-001/*”。

参数	取值
动作	• 包含 • GetObject

步骤6 单击“确定”。

----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

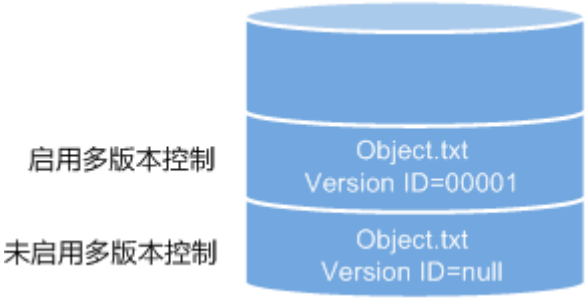
利用多版本控制，您可以在一个桶中保留多个版本的对象，使您更方便地检索和还原各个版本，在意外操作或应用程序故障时快速恢复数据。

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2-11所示。

  图 2-11 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2-12所示。

图 2-12 多版本对象示意图（新对象）

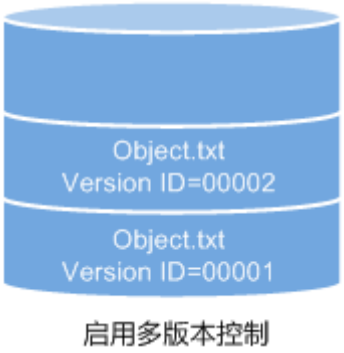
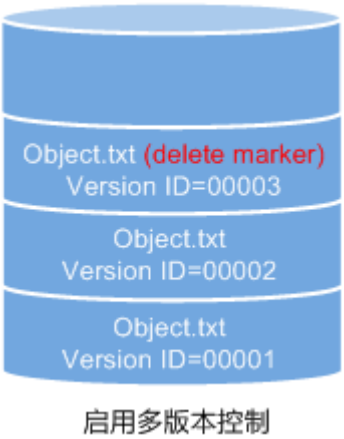


表 2-33 版本说明

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**。此时如果访问该对象，会返回404错误。

图 2-13 删除标记示意图

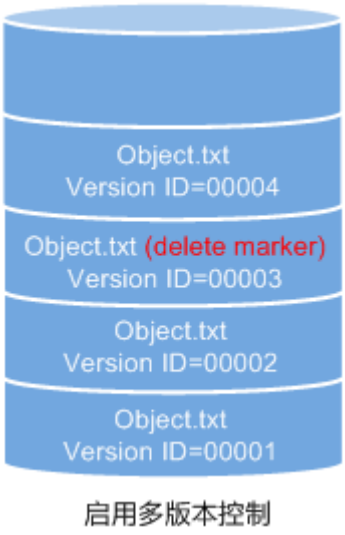


- 删除带删除标记的对象可恢复该对象。详细操作请参见**取消删除对象**的**相关操作**。
- 在“已删除对象”列表，选中对象，可指定版本号彻底删除指定版本对象。详细操作请参见**删除对象或文件夹**的**相关操作**。

- 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。如果再次上传同名对象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2-14所示。

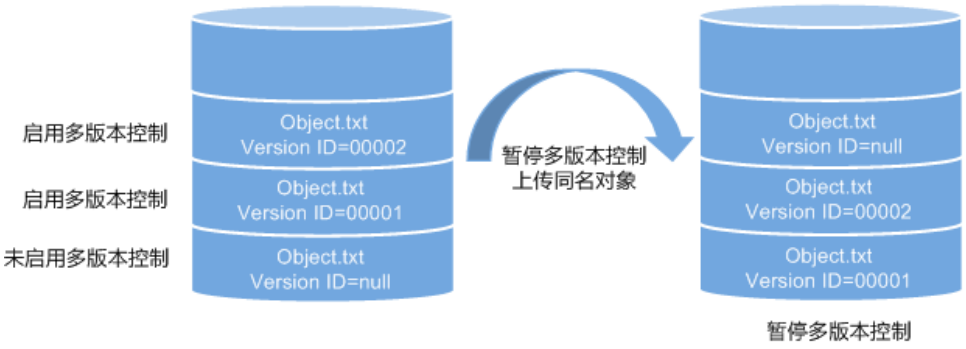
图 2-14 删除后再上传同名对象的版本示意图



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。如果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 2-15 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，如果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OBS管理控制台桶列表中，单击待操作的桶，进入“概览”页面。

步骤2 鼠标滑过“基本信息”区域“多版本控制”参数后面的“未启用”、“暂停”或“已启用”，在右侧会显示“编辑”按钮。单击“编辑”，系统弹出多版本控制对话框。

步骤3 选择“启用”。

步骤4 单击“确定”，启用目标桶中对象的多版本控制。

步骤5 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OBS管理控制台桶列表中，单击待操作的桶，进入“概览”页面。

步骤2 在左侧导航栏选中“对象”。

步骤3 在“对象”列表，单击待操作的对象，进入对象详情页面。

步骤4 在“版本”页签，显示该对象的所有版本。

步骤5 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。

   说明

   如果该版本对象为“冷存储”类别，需要先恢复，再下载。

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。如果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。如果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。

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 2-34 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

名称	示例	含义
VersionID	-	请求中带的versionId
STSLogUrn	-	联邦认证及委托授权信息
StorageClass	STANDARD_IA	当前的对象存储类别
TargetStorageClass	GLACIER	通过转换后的对象存储类别

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OBS管理控制台桶列表中，单击待操作的桶，进入“概览”页面。

步骤2 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3 选择“启用”。

步骤4 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5 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6 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

如果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 事件通知

2.12.1 SMN 通知简介

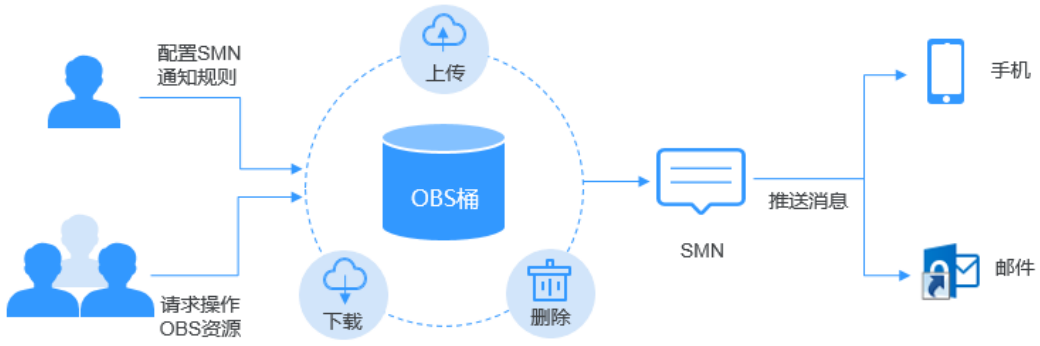
消息通知服务（SMN）是可靠，可扩展，海量的消息通知服务。它大大简化系统的耦合，能够根据用户的需求，向订阅终端主动推送消息，订阅终端可以是电子邮件、短信等。

OBS依赖SMN提供消息通知功能。您可以将OBS桶中对象的上传、删除等操作事件通过SMN发送给指定的订阅终端，以实时掌握OBS桶中发生的关键事件。例如，配置SMN通知，规定当用户往桶中上传对象时，SMN发送消息通知到指定的邮箱。

您可以将通知配置为按对象名称的前缀和后缀进行筛选。例如，您可以添加一个事件，以便仅在将带有“.jpg”后缀的图像文件添加到存储桶时收到通知。或者，您也可以添加一个事件，该配置仅在将带有前缀为“images/”的对象添加到存储桶时收到通知。

支持发送SMN通知的操作事件以及SMN通知的配置方法，请参见**配置SMN通知**。

图 2-16 SMN 通知示意图



2.12.2 配置 SMN 通知

本节介绍如何在OBS控制台配置SMN通知。

背景知识

请参见**SMN通知简介**。

操作步骤

步骤1 在OBS管理控制台桶列表中，单击待操作的桶，进入“概览”页面。

步骤2 在“基础配置”区域下，单击“事件通知”卡片，系统跳转至“事件通知”界面。

或您可以直接在左侧导航栏单击“基础配置>事件通知”，进入“事件通知”界面。

步骤3 单击“创建”，系统弹出“创建事件通知”对话框。

步骤4 配置事件通知参数，参数说明如表2-35所示。

表 2-35 事件通知参数说明

参数	说明
事件通知名称	新增事件的名称，用户自定义。如果不填写，系统将默认自动生成一个全局唯一ID作为名称。
事件	事件类型。目前，OBS支持对以下事件类型进行事件通知。 • **ObjectCreated**：表示所有创建对象的操作，包含Put、Post、Copy对象以及合并段。 – **Put**：使用Put方法创建或覆盖对象。 – **Post**：使用Post（表单上传）方法创建或覆盖对象。 – **Copy**：使用copy（拷贝）方法创建或覆盖对象。 – **CompleteMultipartUpload**：表示合并分段任务。 • **ObjectRemoved**：表示删除对象。 – **Delete**：指定对象版本号删除对象。 – **DeleteMarkerCreated**：不指定对象版本号删除对象。 多个事件类型可以作用于同一个目标对象，例如：同时选择“事件类型”复选框中的**Put**、**Copy**、**Delete**等方法作用于某目标对象，则用户往该桶中上传、复制、删除符合前后缀规则的目标对象时，均会发送事件通知给用户。**ObjectCreated**包含了**Put**、**Post**、**Copy**和**CompleteMultipartUpload**，如果选择了**ObjectCreated**，则默认选择**Put**、**Post**、**Copy**和**CompleteMultipartUpload**。同理如果选择了**ObjectRemoved**，则默认选择**Delete**和**DeleteMarkerCreated**。
前缀	指定事件作用的目标对象的前缀。 **说明** 当前缀和后缀都不配置时，事件通知规则将作用于桶中所有对象。
后缀	指定事件作用的目标对象的后缀。 **说明** • 文件夹是以“/”结尾的，“/”前的字符为文件夹名称。对文件夹的相关操作做事件通知时，如果要匹配后缀，后缀必须以“/”结尾。 • 当前缀和后缀都不配置时，事件通知规则将作用于桶中所有对象。
SMN主题	项目：选择SMN主题所在的项目。 项目用于管理和分类所有的云资源，包括SMN主题。项目不同，对应的SMN主题也不相同，请先选择项目再选择主题。

参数	说明
	主题：选择已授权给OBS发布消息的SMN主题。SMN主题需通过SMN页面创建。 **说明** • SMN主题配置成功后，请不要随意删除与OBS管理控制台事件相关联的主题，也不要取消与OBS管理控制台事件相关联主题对OBS的授权。 • 如果与OBS管理控制台事件相关联的主题被删除或取消该主题对OBS的授权，则可能出现以下现象： a. 对应主题的订阅者无法收到消息。 b. 修改当前桶的事件配置，会自动清理不可用主题对应配置。 • 详细的使用SMN服务的操作指导请参见《消息通知服务用户指南》的“创建主题”、“添加订阅者”和“主题策略”章节的内容。

步骤5 单击“确定”。

----结束

相关操作

您可以单击待操作的事件通知实例后面的“编辑”，编辑修改事件通知；单击“删除”，删除事件通知。

如果您要批量删除事件通知，选中待删除的事件通知实例，单击列表上方的“删除”，完成批量删除。

2.12.3 应用举例：配置 SMN 通知

背景知识

假设某企业日常有大量工作文件需要存档，但并不希望花费大量的人力、物力在存储资源上。因此该企业开通了OBS，用于存储日常工作文件，并希望在OBS上进行的所有允许事件通知的操作，均能通过邮件的方式及时通知到企业某员工。

配置步骤

步骤1 以企业用户登录OBS管理控制台。

步骤2 创建桶。

在页面右上角单击“创建桶”。选择“区域”，选择“存储类别”，输入“桶名称”及其他参数，并单击“立即创建”。

步骤3 创建文件夹。

单击**步骤2**中创建的桶名，进入“概览”页面。单击“对象 > 新建文件夹”，输入文件夹名称，并单击“确定”。这里以创建的文件夹名为“SMN”为例。

步骤4 在页面左上角，单击  ，搜索并选择“消息通知服务 SMN”，进入消息通知服务页面创建SMN主题。

这里假设创建的SMN主题名为“TestTopic”，消息通知方式为邮件。

使用SMN服务创建用于OBS消息通知主题的流程为：

1. 创建SMN主题。
2. 添加主题订阅。
3. 修改主题策略。必须勾选“主题访问策略”页面中的“可发布消息的服务”参数下的“OBS”。

详细的使用SMN服务的操作指导请参见**表2-35**中的主题部分。

步骤5 返回OBS管理控制台。

步骤6 配置事件通知。

1. 在桶列表中单击**步骤2**中创建的桶。
2. 在左侧导航栏单击“基础配置 > 事件通知”，进入“事件通知”界面。
3. 单击“创建”，系统弹出“创建事件通知”对话框。
4. 配置事件通知参数。

   企业用户往桶“testbucket”中的文件夹“SMN”中进行的所有允许事件通知的操作，均能通过邮件的方式及时通知到企业某员工。

   表 2-36 事件通知参数配置

参数	值
事件通知名称	test
事件	ObjectCreated，ObjectRemoved
前缀	SMN/ **说明** - 文件夹是以“/”结尾的，“/”前的字符为文件夹名称。对文件夹的相关操作做事件通知时，如果要匹配后缀，后缀必须以“/”结尾。 - 当前缀和后缀都不配置时，事件通知规则将作用于桶中所有对象。
通知类型	SMN主题： *选择对应区域* TestTopic

----结束

验证配置是否成功

步骤1 以企业用户登录OBS管理控制台。

步骤2 上传一个名为“test.txt”的文件到**步骤3**创建的文件夹中。

文件上传成功后，企业某员工应接收到邮件通知。邮件中的关键内容为“ObjectCreated:Post”表示对象上传成功。

步骤3 删除**步骤2**中上传的“test.txt”文件。

删除文件成功后。企业某员工应接收到邮件通知。邮件中的关键内容为“ObjectRemoved:Delete”表示对象删除成功。

----结束

2.13 跨区域复制

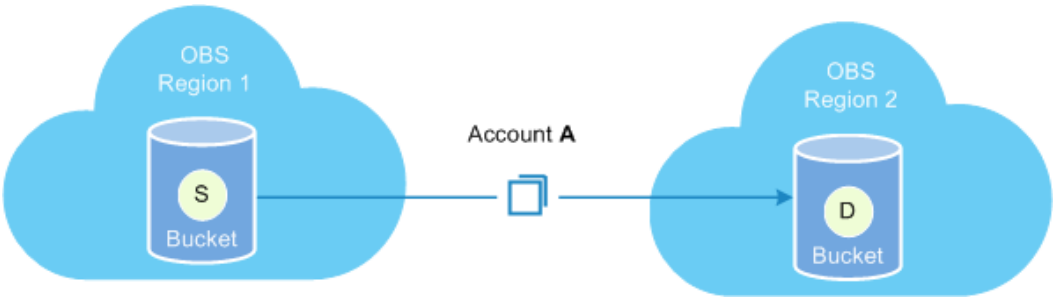
2.13.1 跨区域复制简介

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账号，暂不支持跨账号复制。

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。默认情况下复制对象的存储类别，与源对象保持一致。您也可以为复制对象指定一个存储类别。

图 2-17 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（冷存储对象除外）。
- 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。
- 桶中的历史对象（需要开启“同步历史对象”功能）。

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，默认不会被复制到目标桶，除非开启了“同步历史对象”功能。
- 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。
- 源桶冷存储类别的对象不支持跨区域复制到目标桶。
- 如果目标桶所属区域不支持存储类别，则复制后对象的存储类别均为标准存储类别。
- 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。
- 未打开同步删除对象时，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。

  打开同步删除对象时，源桶的对象删除操作将会复制到目标桶，即对象在源桶删除后目标桶也会同步删除。
- 在启用跨区域复制过程中，如果您修改目标桶的多版本控制状态，会导致对象复制失败；如果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，如果您删掉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OBS管理控制台桶列表中，单击待操作的桶，进入“概览”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。

步骤4 根据业务规划配置跨区域复制规则，参数的详细说明表2-37所示。

表 2-37 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。
	同步删除对象	选择是否将源桶的对象删除操作复制到目标桶，即对象在源桶删除后目标桶也会同步删除。

参数		说明
	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。 • 如果勾选该项，对话框下方的“IAM委托”仅会展示源端和目标端均有“KMS Administrator”权限的委托； • 如果不勾选该项，对话框下方的“IAM委托”仅会展示源端或目标端没有“KMS Administrator”权限的委托。 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。
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	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“创建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 FullAccess”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。

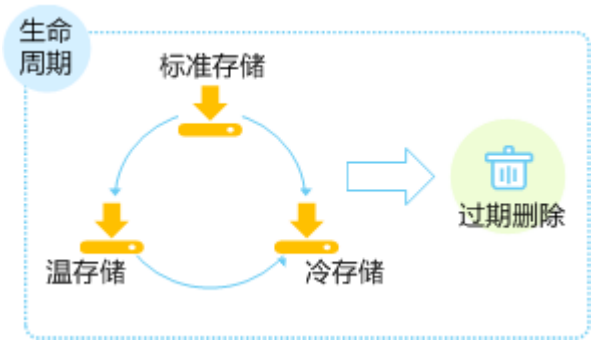
----结束

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或者定时转换对象的存储类别。

图 2-18 生命周期管理示意图



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。
- 某些文档在一段时间内经常访问，但是超过一定时间后便可能不再访问了。这些文档需要在一定时间后转化为温存储，冷存储或者删除。

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。

您可以根据您的业务需要，识别桶中哪些对象将不再频繁访问，然后配置生命周期规则将这些对象转换为温存储或者冷存储，以减少OBS的存储费用。此处的“转换”表示在不复制原对象的情况下修改对象的存储类别。您可以在对象页面手动修改对象的存储类别，详情请参见**上传对象**的相关操作，也可以通过配置生命周期规则转换对象的存储类别。

生命周期管理规则通常包含以下关键要素：

- 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。
- 时间：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转换为温存储、冷存储或者过期并自动被OBS删除。
  - 转换为温存储：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转换为温存储。
  - 转换为冷存储：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转换为冷存储。
  - 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。

转换为温存储的时间最少设置为30天，如果同时设置转换为温存储和转换为冷存储，则转换为冷存储的时间要比转换为温存储的时间至少长30天，例如转换为温存储设置为33天，则转换为冷存储至少需要设置为63天。如果单独设置转换为冷存储，则没有时间限制。过期时间必须大于前两个转换时间的最大值。

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。

- 标准对象可以转换为温或冷对象。
- 温对象可以转换为冷对象。

- 指定对象过期删除。

冷对象不能通过设置生命周期规则来转换存储类别。

操作步骤

步骤1 在OBS管理控制台桶列表中，单击待操作的桶，进入“概览”页面。

步骤2 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3 单击“创建”。

步骤4 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。
- “策略”：可以按前缀配置，也可以配置到整个桶。
  - 按前缀配置：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。
  - 配置到整个桶：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。
- 如果已存在配置到整个桶的生命周期规则，则不允许再新增按前缀配置的规则。

当前版本或历史版本：

说明

- “当前版本”与“历史版本”是针对“多版本控制”而言的。如果开启了“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。
- 转换为温存储天数：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温存储。至少设置为30天。
- 转换为冷存储天数：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冷存储。如果同时设置转换为温存储和转换为冷存储，则转换为冷存储的时间要比转换为温存储的时间至少长30天。如果单独设置转换为冷存储，则没有时间限制。
- 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。过期时间必须大于前两个转换时间的最大值。

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

如果您在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。

如果您在某天设置前缀为“log”的对象，转换为温存储的时间设置为30天，转换为冷存储的时间设置为60天，过期删除的时间设置为100天，OBS将会在“log/clientlog.log”、“log/serverlog.log”、“log/test1.log”和“log/test2.log”这四个对象上传满30天后转换为温存储，满60天后转换为冷存储，满100天后自动删除。

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，存储类别的转换以及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5 单击“确定”，完成生命周期规则配置。

----结束

后续操作

如果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 配置自定义域名

2.15.1 配置自定义域名简介

应用场景

用户将文件上传到OBS桶后，默认可以通过OBS桶的访问域名访问桶中的文件。如果用户希望通过指定的域名访问，可以为桶配置自定义域名。

例如用户拥有一个域名www.example.com，OBS桶中存放了一个图片文件image.png，配置自定义域名后，用户便可以使用http://www.example.com/image.png来访问图片文件。配置流程如下：

1. 在OBS上创建一个桶，并上传image.png文件到该桶中。
2. 通过OBS控制台，将www.example.com这个自定义的域名配置在已创建的桶上。
3. 在域名服务器上，添加CNAME规则，将www.example.com映射成桶域名。
4. http://www.example.com/image.png请求到达OBS后，OBS会找到www.example.com和桶域名的映射，转换变成访问桶的image.png文件。即对http://www.example.com/image.png的访问，经过OBS处理后，实际上访问的是http://*桶域名*/image.png。

约束与限制

1. 桶版本号为3.0及以上的桶支持自定义配置域名功能。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。
2. OBS自定义域名配置暂时不支持HTTPS访问自定义域名，只支持HTTP访问自定义域名。
3. 一个自定义域名只能配置到一个桶域名上。
4. 配置的自定义域名后缀目前支持的范围为2~6个英文大小写字母。

2.15.2 配置自定义域名

操作步骤

步骤1 在OBS管理控制台桶列表中，单击待操作的桶，进入“概览”页面。

步骤2 在左侧导航栏选择“域名管理”，进入“域名管理”界面。

步骤3 单击“绑定用户域名”，在用户域名中输入需要绑定的自定义域名。

域名后缀目前支持的范围为2~6个英文大小写字母。

步骤4 单击“确定”。

步骤5 在域名解析服务器上配置CNAME记录，将用户自定义域名（例如example.com）映射成桶域名。

不同DNS服务商的CNAME配置方式不同，具体请咨询DNS服务商。

----结束

2.16 静态网站托管

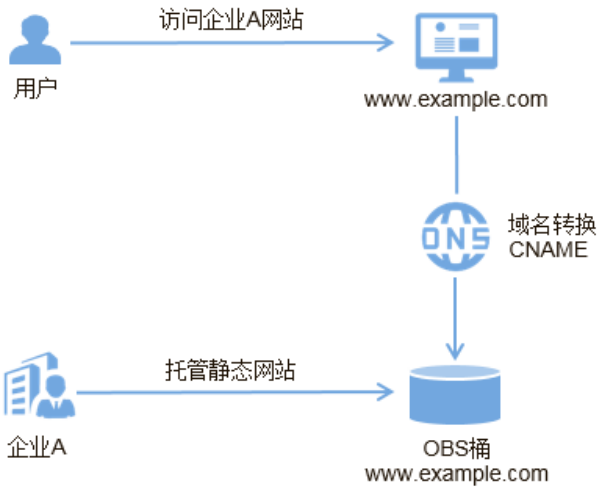
2.16.1 静态网站托管简介

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 2-19 静态网站示意图



2.16.2 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。

2.16.3 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。

如果静态网站文件为“冷存储”类别，则需要先恢复，具体操作步骤请参见**恢复冷存储文件**。

操作步骤

步骤1 在OBS管理控制台桶列表中，单击待操作的桶，进入“概览”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。

参考**为匿名用户设置对象的访问权限**为匿名用户授予静态网站文件的读取权限。

如果桶中只有静态网站文件，可直接配置桶为“公共读”权限，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. 在“标准桶策略”下配置桶的“公共读”权限。
3. 单击“公共读”卡片。并在弹出的确认信息对话框中单击“是”。

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 打开“状态”开关。

步骤6 “托管模式”选择“配置到当前桶”。

步骤7 在“默认首页”、“默认404错误页面”中设置默认首页页面和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8 **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**表2-38**所示。

表 2-38 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	描述重定向请求时使用的对象名前缀，请求中的对象名会将KeyPrefixEquals的内容替换为ReplaceKeyPrefixWith的内容。 例如：想把所有对docs（目录下的对象）的请求重定向到documents（目录下的对象），可以将Condition中的KeyPrefixEquals设置为docs，Redirect中的ReplaceKeyPrefixWith设置为documents。那么对于对象名称为"docs/a.html"，重定向的结果为"documents/a.html"。
	ReplaceKeyWith	描述重定向请求时使用的对象名，请求中的整个对象名会被替换为ReplaceKeyWith的内容。 例如：想把所有对"docs"目录下的所有对象的请求重定向到"documents/error.html"，可以将Condition中的KeyPrefixEquals设置为docs，Redirect中的ReplaceKeyWith设置为"documents/error.html"。那么对于对象名称为"docs/a.html"和"docs/b.html"，重定向的结果都为"documents/error.html"。
	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9 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

2.16.4 配置重定向请求

如果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。

如果静态网站文件为“冷存储”类别，则需要先恢复，具体操作步骤请参见**恢复冷存储文件**。

操作步骤

步骤1 在OBS管理控制台桶列表中，单击待操作的桶，进入“概览”页面。

步骤2 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3 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4 打开“状态”开关。

步骤5 “托管模式”选择“重定向请求”，输入桶访问域名或URL。

步骤6 单击“确定”。

步骤7 在桶列表中选择重定向的桶。

步骤8 **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。

参考**为匿名用户设置对象的访问权限**为匿名用户授予静态网站文件的读取权限。

如果桶中只有静态网站文件，可直接配置桶为“公共读”权限，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. 在“标准桶策略”下配置桶的“公共读”权限。
3. 单击“公共读”卡片。并在弹出的确认信息对话框中单击“是”。

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

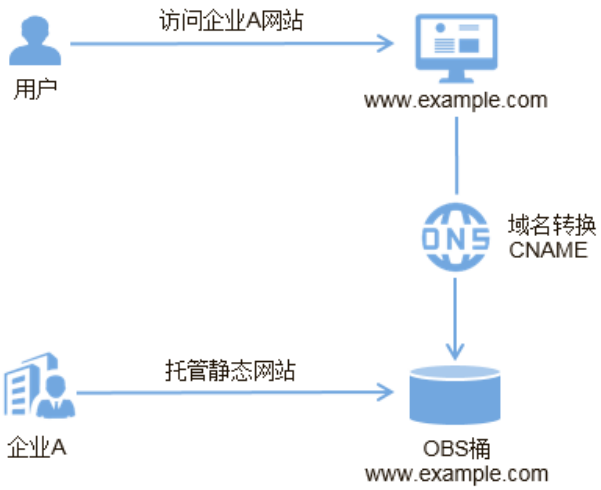
2.16.5 使用自定义域名托管静态网站

OBS支持通过自定义域名访问托管在OBS上的静态网站。本节将以一个具体场景作为示例，帮助您了解如何使用自定义域名配置静态网站托管。在此之前，您可能需要了解一些关于OBS静态网站托管的基本概念及操作，详情请参阅**配置静态网站托管**。

场景介绍

企业A有大量静态网站文件需要存档，但并不希望花费大量的人力、物力在存储资源上。因此该企业开通了OBS对象存储，用于托管静态网站，并希望使用自定义域名让该企业下的用户访问这些静态资源，如**图2-20**所示。

图 2-20 使用自定义域名访问静态网站示意图



操作流程

您需要先在OBS管理控制台上创建一个桶，用于存放静态网站资源，并启用该桶的静态网站托管，然后通过云解析服务（DNS，Domain Name Service）创建和配置域名托管。具体操作流程如下：

1. **注册域名**
2. **创建桶**
3. **上传静态网站文件**
4. **在OBS上配置静态网站托管**
5. **绑定自定义域名**
6. **创建和配置域名托管**
7. **验证**

数据规划

执行配置操作前，需要提前规划如**表2-39**所示的数据。

表 2-39 数据规划

规划项	说明	示例
自定义域名	用户自己的域名地址。	www.example.com
静态网站首页	访问静态网站时返回的索引页面，即首页。	index.html
404错误页面	当访问错误的静态网站路径时，返回的404错误页面。	error.html

- index.html的内容为：

```
<html>
 <head>
    <title>Hello OBS!</title>
    <meta charset="utf-8">
 </head>
 <body>
    <p>欢迎使用OBS静态网站托管功能</p>
    <p>这是首页</p>
 </body>
</html>
```

- error.html的内容为：

```
<html>
 <head>
    <title>Hello OBS!</title>
    <meta charset="utf-8">
 </head>
 <body>
    <p>欢迎使用OBS静态网站托管功能</p>
    <p>这是404错误页面</p>
 </body>
</html>
```

操作步骤

步骤1 注册域名。

如果您拥有一个已注册的域名，可跳过本步骤。

如果您还没有，请选择一个合适的注册商注册一个属于自己企业的域名。在本场景下，以数据规划中的示例域名www.example.com进行注册，在实际操作中，您需要将此域名替换为您自己规划的域名。

步骤2 创建桶。

桶名没有特殊要求，您只需要按照界面提示的命名规则创建一个桶用于存储静态网站文件。此处以创建一个桶名称为example的桶为例，其具体操作步骤如下：

1. 打开OBS管理控制台。
2. 在页面上方单击“创建桶”。
3. 在弹出的对话框中配置以下参数。
   - **“区域”**：根据就近原则选择离业务较近的区域。
   - **“桶名称”**：输入“example”。
   - **“存储类别”**：推荐选择“标准存储”。

说明

您也可以根据网站的访问频率以及对响应速度的要求，选择“温存储”或“冷存储”。存储类别具体介绍请参见**存储类别简介**。

- **“桶策略”**：选择“公共读”使桶内对象能够被任何用户访问。
- **“默认加密”**：选择“关闭”。

4. 单击“立即创建”，完成桶创建。

步骤3 上传静态网站文件。

整理好待上传的静态网站文件，执行以下步骤，将所有的静态网站文件都上传至桶example中。

1. 单击桶example的桶名称，进入桶“对象”页面。
2. 单击“上传对象”。
3. 拖拽本地准备好的静态网站文件至“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。

   说明

   - 不可加密上传静态网站文件。
   - 网站首页文件（index.html）和404错误页面（error.html），需要存放在桶的根目录下。
   - 存储类别建议选择“标准存储”。如果静态网站文件的存储类别为“冷存储”，则需要先恢复才能被访问，具体操作步骤请参见**恢复冷存储文件**。
4. 单击“上传”完成文件上传。

步骤4 配置静态网站托管。

上传完静态网站文件后，您需要执行以下步骤，将当前桶设置为静态网站托管模式。

说明

您也可以将整个静态网站直接重定向至另一个桶或域名，配置操作请参见**配置重定向请求**。

1. 单击桶example的桶名称，进入桶对象页面。
2. 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”页面。
3. 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。
4. 打开“状态”开关。
5. “托管模式”选择“配置到当前桶”。

   说明

   您也可以根据业务需求配置重定向规则，实现网站内容重定向，具体操作请参见**配置静态网站托管**。
6. **“默认首页”**配置为数据规划中的index.html，**“默认404错误页面”**配置为数据规划中的error.html。
7. 单击“确定”。

步骤5 绑定自定义域名。

通过OBS绑定自定义域名的操作步骤如下：

1. 单击桶example的桶名称进入“对象”页面，在左侧导航栏选择“域名管理”。
2. 单击“绑定用户域名”，在“用户域名”输入“www.example.com”。
3. 单击“确定”，完成自定义域名绑定。

步骤6 创建和配置域名托管。

为了方便对您的自定义域名和静态网站统一管理，实现业务全面云化，您可以直接在云解析服务（DNS，Domain Name Service）上托管您的自定义域名。托管完成后，后续域名解析的管理都可以在云解析服务上进行，包括：管理记录集、管理反向解析、设置域名泛解析等等。

您也可以直接在域名注册商域名解析中添加一条别名记录，指向对象存储桶的静态网站域名。

使用云解析服务创建和配置域名托管的操作步骤如下：

1. 创建公网域名。

   在云解析服务中创建公网域名，使用**步骤1**中注册的根域名“example.com”作为创建的公网域名的“名称”。详细的创建方法请参见《云解析服务用户指南》中“配置网站解析”章节中的“添加域名”部分内容。

2. 添加别名记录。

   在云解析服务中为托管域名子域名“www.example.com”添加记录集，配置该子域名别名指向OBS的静态网站托管域名。在添加别名记录时参数配置如下：

   - **“主机记录”**：输入“www”。
   - **“类型”**：选择“CNAME-规范名称记录”。
   - **“线路类型”**：选择“全网默认”。
   - **“TTL（秒）”**：保持默认。
   - **“值”**：需指向的域名，即OBS桶example的静态网站托管域名。

   详细的创建方法请参见《云解析服务用户指南》中“增加CNAME类型记录集”章节。

3. 在域名注册商处修改域名解析服务器地址。

   在域名注册商处，将该根域名对应的NS记录中域名解析服务器地址修改为云解析服务（DNS）服务器的地址，具体地址为云解析服务中该公网域名记录集中NS记录的值字段内容信息。

   详细的更改域名解析服务器地址的方法请参见《云解析服务用户指南》中“配置网站解析”章节中的“更改域名的DNS服务器”部分内容。

   说明

   更改后的域名解析服务器地址将于48小时内生效，具体生效时间请以域名注册商处的说明为准。

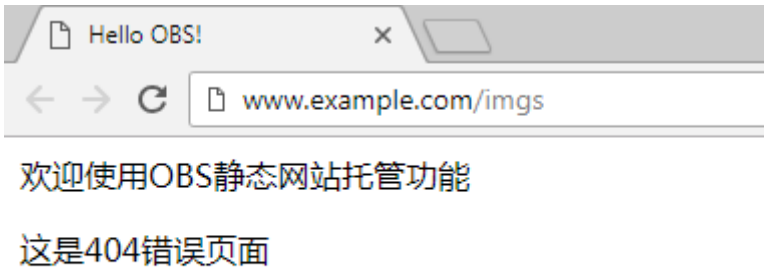
步骤7 验证。

- 在浏览器中输入访问地址：www.example.com，验证能否访问到配置的默认首页，如**图2-21**所示。

图 2-21 默认首页

- 在浏览器中输入一个桶中不存在的静态文件访问地址，例如：www.example.com/imgs，验证能否访问到配置的404错误页面，如图2-22所示。

图 2-22 404 错误页面



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

网站更新操作

后续如果需要对网站某个静态文件（如：图片、音乐、html文件、css文件等）进行更新，用户可以重新上传该静态文件。

默认情况下，在OBS同一路径下新上传的文件会覆盖OBS上已存在的同名文件。为避免文件覆盖的情况，用户可以选择启用OBS的多版本控制功能。利用多版本控制，用户便可以保留静态文件的多个版本，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。关于多版本控制的更多介绍以及操作指导，请参见多版本控制简介。

2.17 跨域资源共享

2.17.1 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。

2.17.2 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OBS管理控制台桶列表中，单击待操作的桶，进入“概览”页面。

步骤2 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“基础配置>CORS规则”，进入“CORS规则”界面。

步骤3 单击“创建”，系统弹出“创建CORS规则”对话框。

说明

一个桶最多可设置100条CORS规则。

步骤4 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 2-40 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

参数	说明
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5 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

2.18 防盗链

2.18.1 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，如果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。

2.18.2 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OBS管理控制台桶列表中，单击待操作的桶，进入“概览”页面。

步骤2 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3 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4 单击 保存设置。

----结束

2.19 监控

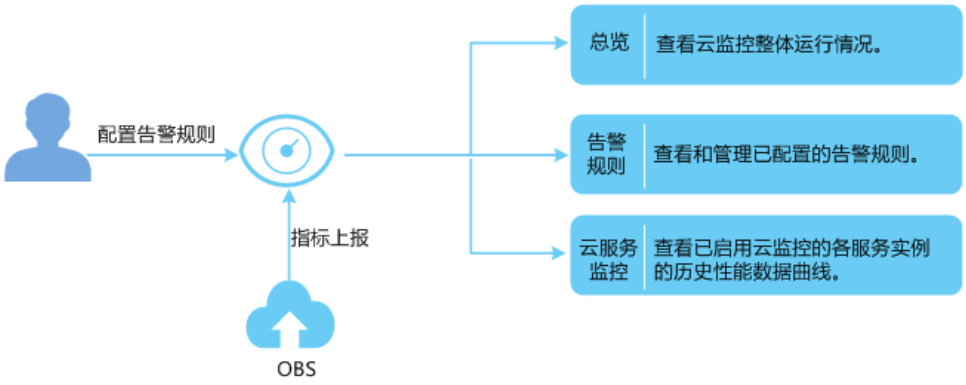
2.19.1 监控对象存储服务

操作场景

用户在使用OBS的过程中会不断发送PUT、GET类的请求，产生上传、下载流量，也可能会遇到服务端返回的错误响应。用户可使用云监控服务（Cloud Eye）监控自己的OBS桶，执行自动实时监控、告警和通知操作，帮助您实时掌握桶中所产生的请求、流量和错误响应等信息。

云监控服务不需要开通，会在用户创建资源（如OBS桶）后自动启动。关于云监控服务的更多介绍，请参见《云监控用户指南》。

图 2-23 云监控示意图



设置告警规则

在自动实时监控的基础上，用户可以在云监控服务中设置告警规则，规定在某些特殊情况出现时向用户发送告警通知。

设置OBS监控信息告警规则的方法，请参见《云监控用户指南》的“创建告警规则和通知”章节。

查看监控指标

云监控服务对**OBS的监控指标**进行实时监控，用户可以在云监控服务控制台查看各项指标的详细监控数据。

查看OBS监控指标详情的方法，请参见《云监控用户指南》的“查看云服务监控指标”章节。

2.19.2 对象存储服务监控指标说明

功能说明

本节定义了对象存储服务OBS上报云监控服务Cloud Eye的监控指标的命名空间，监控指标列表和维度，用户可以通过云监控服务提供的管理控制台或API接口来检索对象存储服务产生的监控指标和告警信息。

命名空间

SYS.OBS

监控指标

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
download_bytes	下载流量	该指标用于统计所有桶的所有下载请求响应的字节数，包括HTTP body体。 单位：字节	≥ 0 bytes	桶	5分钟
upload_bytes	上传流量	该指标用于统计所有桶的所有上传请求消息体的字节数，包括HTTP body体。 单位：字节	≥ 0 bytes	桶	5分钟
get_request_count	GET类请求次数	该指标用于统计所有桶及桶中对象的GET/HEAD/OPTIONS请求次数。 单位：次	≥ 0 counts	桶	5分钟
put_request_count	PUT类请求次数	该指标用于统计所有桶及桶中对象的PUT/POST/DELETE请求次数。 单位：次	≥ 0 counts	桶	5分钟
first_byte_latency	GET类请求首字节平均时延	该指标用于统计GET/HEAD/OPTIONS操作，在一个统计周期内从系统收到完整请求到开始返回响应的耗时平均值。 单位：毫秒	≥ 0 ms	桶	5分钟
request_count_4xx	4xx错误次数	该指标用于统计服务端响应错误状态码为4xx的请求数。 单位：次	≥ 0 counts	桶	5分钟
request_count_5xx	5xx错误次数	该指标用于统计服务端响应错误状态码为5xx的请求数。 单位：次	≥ 0 counts	桶	5分钟

维度

表 2-41 维度列表

Key	Value
bucket_name	桶维度，取值为桶名。

2.20 相关操作参考

2.20.1 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“对象存储服务 OBS”。

步骤6 选择“持续时间”。

步骤7 在“权限选择”项，单击“全局服务>对象存储服务”行的“修改”，系统弹出“修改策略”对话框。

步骤8 选择“基本>Tenant Administrator”，单击“确定”。

步骤9 （可选）如跨域复制规则勾选了“复制使用KMS加密的对象”，源桶和目标桶所在区域需配置KMS Administrator权限集。

1. 单击源桶/目标桶所在区域行的“修改”，系统弹出“修改策略”对话框。
2. 搜索KMS，并选择KMS Administrator权限集。
3. 单击“确定”。

步骤10 单击“确定”，完成委托创建。

----结束

2.21 异常处理

2.21.1 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。

2.21.2 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?

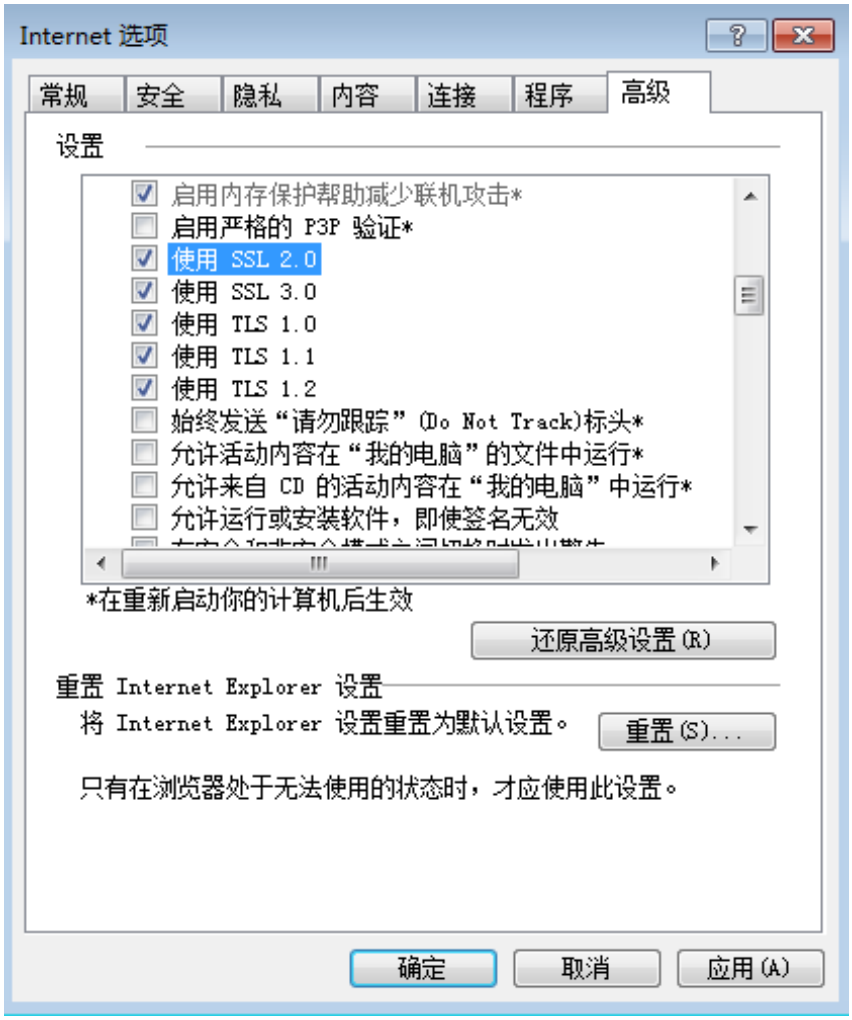
回答

检查浏览器的“Internet选项”中是否勾选SSL和TLS选项，如果没有，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2-24**所示。

图 2-24 Internet 选项



步骤3 单击“确定”。

----结束

2.21.3 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。

2.21.4 配置事件通知失败

问题

通过OBS配置事件时，提示“主题暂未授权给对象存储服务。前往消息通知服务，将该主题授权给对象存储服务。”

回答

前往SMN页面，通过勾选“主题访问策略”页面中的“可发布消息的服务”参数下的“OBS”来修改主题策略从而将该主题授权给OBS。

详细的使用SMN服务的操作指导请参见《消息通知服务用户指南》的“主题策略”章节的内容。

2.21.5 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。

2.22 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2-42列出了错误响应中的常见错误码。

表 2-42 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。

错误码	描述
Obs.0006	用户拥有的桶的数量已经达到了系统的上限。 一个账号及账号下的所有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	你的账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账号。
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。 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 产品咨询

3.1.1 如何获得对象存储服务?

在云服务网站申请账号，充值后，即可使用对象存储服务。

如果是IAM子账号，需主账号通过IAM授权其OBS资源使用权限，IAM子账号才能访问OBS。

3.1.2 如何获取 OBS 的终端节点?

OBS可以通过域名进行访问，在使用API、第三方工具等方式使用OBS时，可通过域名方便定位OBS中的资源。

在使用OBS之前，请确保客户端环境已经正确配置DNS服务器地址，用于OBS域名解析。

不同服务不同区域的终端节点不同，OBS的终端节点信息如下表所示。

表 3-1 OBS 终端节点信息

区域名称	区域	终端节点（Endpoint）	协议类型
欧洲-巴黎	eu-west-0	oss.eu-west-0.prod-cloud-ocb.orange-business.com	HTTPS/HTTP

3.1.3 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。

3.1.4 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。

3.1.5 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：

- 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。如果只上传1个文件，则这个文件最大为5GB。
- OBS Browser+、obsutil、API和SDK上传的单个对象最大是48.8TB。

3.1.6 OBS 是否支持流量监控?

OBS支持流量监控功能：

通过云监控CES，能监控OBS包括流量指标在内的如下指标：

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
download_bytes	下载流量	该指标用于统计所有桶的所有下载请求响应的字节数，包括HTTP body体。 单位：字节	≥ 0 bytes	桶	5分钟
upload_bytes	上传流量	该指标用于统计所有桶的所有上传请求消息体的字节数，包括HTTP body体。 单位：字节	≥ 0 bytes	桶	5分钟
get_request_count	GET类请求次数	该指标用于统计所有桶及桶中对象的GET/HEAD/OPTIONS请求次数。 单位：次	≥ 0 counts	桶	5分钟
put_request_count	PUT类请求次数	该指标用于统计所有桶及桶中对象的PUT/POST/DELETE请求次数。 单位：次	≥ 0 counts	桶	5分钟

指标ID	指标名称	指标含义	取值范围	测量对象	监控周期（原始指标）
first_byte_latency	GET类请求首字节平均时延	该指标用于统计GET/HEAD/OPTIONS操作，在一个统计周期内从系统收到完整请求到开始返回响应的耗时平均值。 单位：毫秒	≥ 0 ms	桶	5分钟
request_count_4xx	4xx错误次数	该指标用于统计服务端响应错误状态码为4xx的请求数。 单位：次	≥ 0 counts	桶	5分钟
request_count_5xx	5xx错误次数	该指标用于统计服务端响应错误状态码为5xx的请求数。 单位：次	≥ 0 counts	桶	5分钟

3.1.7 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。

3.1.8 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。

3.1.9 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。

3.1.10 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，或者设置对象分享功能，其他用户即可访问该对象。

3.1.11 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 3-2 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
obsutil	支持
SDK	支持 使用SDK的断点续传接口时，必须开启断点续传选项后才能在进程再次进入时读取上一次上传的进度，具体设置方法请参考对应语言的SDK文档。
API	不支持

3.1.12 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 3-3 OBS 管理工具批量上传功能

工具	批量上传
管理控制台	不支持
OBS Browser+	支持上传多个文件或文件夹。单次最多支持500个文件或文件夹同时上传。
obsutil	支持上传文件夹，单次上传一个文件夹，最大为48.8TB。
SDK	不支持
API	不支持

3.1.13 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 3-4 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

工具	批量下载
obsutil	支持
SDK	不支持
API	不支持

3.1.14 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 3-5 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，如果选择文件夹，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。
obsutil	支持按前缀批量删除对象。
SDK	支持，批量删除对象一次能接收最大对象数目为1000个。
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。

3.1.15 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:

- 单个账号默认的OBS读写带宽（GET请求带宽与PUT请求带宽的总和）上限是16Gbit/s(包括公网和内网带宽一共16Gbit/s)。如果带宽达到该阈值，请求会触发流控。
- 如果用户购买的虚拟机网卡带宽低于16Gbit/s，那么节点带宽会先受虚机带宽限制，需要购买多台虚拟机并发运行才能达到16Gbit/s的带宽。
- 上传下载速率还受磁盘io及是否有其它进程抢占资源的影响。

3.1.16 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。如果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。

3.1.17 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。

3.1.18 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。

3.1.19 我的 OBS 桶性能是否会受其他用户业务的影响?

不会。OBS对不同账号的访问做了性能隔离，不同账号之间不会出现性能干扰或影响。

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：对同一账号内的子用户授权。

  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用户或其他账号授权桶及桶内对象的操作权限。

- 访问控制列表 (ACL)

  ACL是基于账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

- 如果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。
- 如果是当前桶名已存在，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。
- 检查账号是否拥有权限，如果无权限，请授予对应的操作权限。
- 检查账号是否已欠费或余额不足。如果欠费，请先续费。
- 检查本地与OBS的网络是否正常，如果存在网络故障，解决网络故障，确保网络正常。
- 如果以上都不是，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，如果存在网络故障，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。
- 检查账号是否已欠费或余额不足。如果欠费，请先续费。
- 检查账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。如果无权限，请先授权。
- 如果以上都不是，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，如果存在网络故障，解决网络故障，确保网络正常。
- 检查账号是否已欠费或余额不足。如果欠费，请先续费。
- 检查账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。如果无权限，请先授权。
- 检查当前对象是否采用了KMS加密，如果对象已加密，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。
- 检查当前对象是否为冷存储类别，如果是且该对象的状态为“未恢复”，则先恢复该对象。
- 如果以上都不是，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，如果存在网络故障，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。如果没有，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。如果没有，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。如果没有，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账号是否为桶的拥有者。
- 如果以上都不是，请联系客服进一步解决。

3.3.5 桶存储类别和对象存储类别有什么关系?

上传对象时，对象的存储类别默认继承桶的存储类别。您也可以重新指定对象的存储类别。

修改桶的存储类别，桶内已有对象的存储类别不会修改，新上传对象时的默认对象存储类别随之修改。

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 3-6 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。
obsutil	不支持
SDK	通过调用对象的getObjectUrl接口可获取上传对象的URL。 **说明** 在上传对象过程中，可以在返回值获取到URL，但不支持已上传的对象。
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。如果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。

3.3.9 使用 IE 浏览器访问带有中文字符的对象 URL 地址报错如何处理?

问题描述

使用IE浏览器访问带有中文字符的对象URL地址，报HTTP 400错误。

处理思路

IE浏览器默认不是使用UTF-8发送查询字符串，修改IE浏览器的默认配置可以解决此问题。

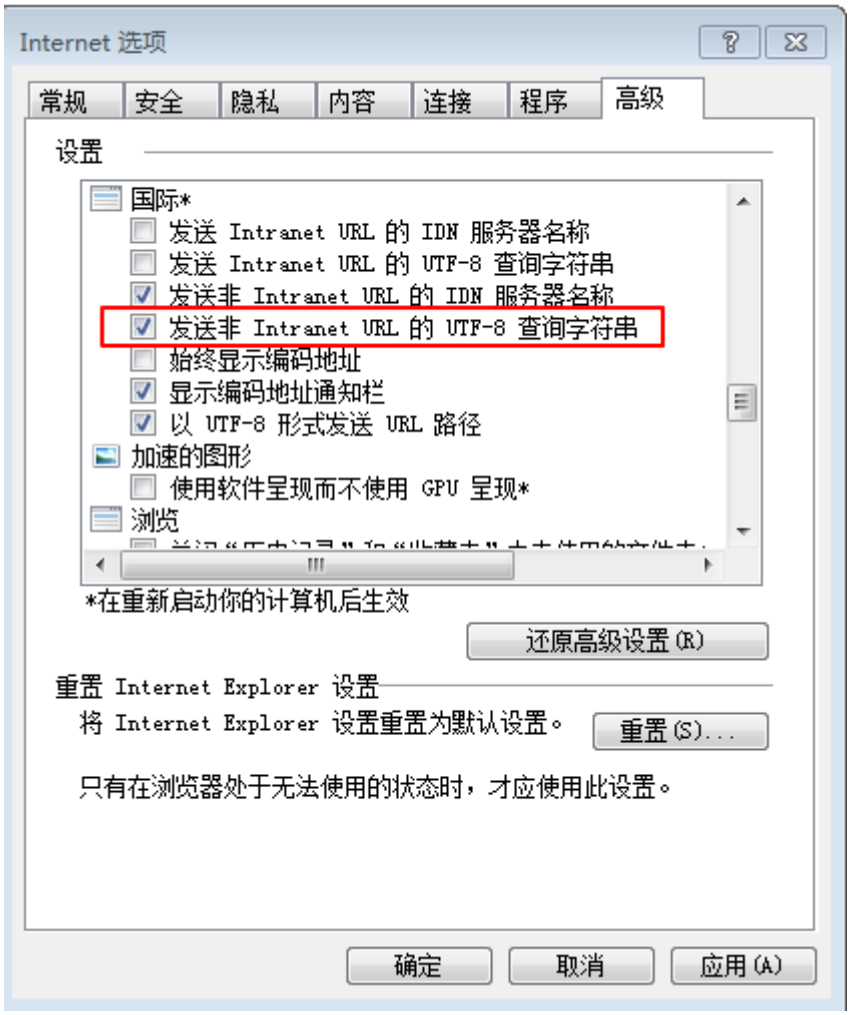
处理步骤

步骤1 打开IE浏览器（以IE 11为例）。

步骤2 单击浏览器右上角的“设置”图标，单击“Internet选项 > 高级”。

步骤3 勾选“发送非Intranet URL的UTF-8查询字符串”，如图3-1所示。

图 3-1 修改 IE 默认配置



步骤4 单击“应用”，并单击“确定”。

步骤5 重新启动IE浏览器。

此时便可以正常访问带有中文字符的对象URL地址。

----结束

3.4 工具相关

3.4.1 使用 obsutil 下载文件夹前期速度正常，下载到 90%后速度变慢

出现此种现象有两种场景。

- 场景一：文件夹中存在部分大对象和大量小对象。对于大对象，下载速度很快；对于大量小对象，下载速度主要受TPS影响。如果下载到90%后都是小对象，此时下载速度一定程度上可能会降低。
- 场景二：文件夹中的对象大小均匀。可能原因为数据已经下载完成，但是在写入磁盘时产生排队现象，造成显示下载变慢的假象，请客户排查客户端的写入速率等问题。

3.4.2 使用 obsutil 下载文件到 99%后失败

出现该问题的主要原因：

1. 网络波动导致下载失败。
2. 磁盘IO卡顿导致缓存文件到目标文件夹失败。

解决方法：

1. 重新执行下载命令。

   obsutil在下载的时候默认开启断点续传，此时只要重新执行之前的下载命令就可以将之前下载失败的对象采用续传的方式重新下载到本地。
2. 如果问题未能解决，请将obsutil升级到最新版本再进行下载。

3.4.3 obsutil cp 命令如何开启增量上传/下载/复制?

在执行**obsutil cp**命令进行上传/下载时，可以通过增加“-u”参数开启增量功能。

该参数的含义为：上传/下载/复制每个对象时都会对比源路径和目标路径，仅在目标对象不存在，或者对象大小不一致，或者目标对象的最后修改时间早于源对象的最后修改时间时进行上传/下载/复制。

3.5 API 和 SDK 等开发者相关

3.5.1 PUT 上传和 POST 上传有什么区别?

PUT上传中参数通过请求头域传递；POST上传则作为消息体中的表单域传递。

PUT上传需在URL中指定对象名；POST上传提交的URL为桶域名，无需指定对象名。两者的请求行分别为：

```
PUT /ObjectName HTTP/1.1
POST / HTTP/1.1
```

两种方式单次上传对象大小范围均为[0, 5GB]，如果需要上传超过5GB的大文件，需要通过多段上传实现。

关于PUT和POST上传更详细的API信息，请参见《对象存储接口参考》。

3.5.2 使用 OBS SDK 上传超过 5GB 的大文件失败

OBS服务端上传对象接口有规格限制，单次可上传的最大文件为5GB，如果需要上传超过5GB的大文件，需要通过OBS服务端提供的分段上传接口实现。具体步骤为：

1. 调用OBS服务端初始化上传段任务接口，生成分段上传ID（Upload ID）。
2. 调用OBS服务端上传段接口，逐个或并行上传段，每个段最大可支持5GB。
3. 上传段完成后，调用OBS服务端合并段接口，生成最终对象。

OBS SDK实现了OBS服务端分段上传需要使用的原子接口，可在各语言《SDK参考》的“分段上传”章节获取更多使用OBS SDK进行分段上传的介绍。

3.5.3 签名不匹配（SignatureDoesNotMatch）如何处理

问题现象

调用OBS API报如下错误：

状态码：403 Forbidden

错误码：SignatureDoesNotMatch

错误信息：The request signature we calculated does not match the signature you provided. Check your key and signing method.

问题原因

请求中携带的签名与系统计算得到的签名不一致。

解决方法

步骤1 检查endpoint

使用OBS SDK时需要检查此项。

需要确保填写的**endpoint**正确，当用户将endpoint错误地填写为桶访问域名，即在endpoint前多加了桶名，也会报签名不匹配错误。

步骤2 检查AK、SK

请确保AK、SK输入正确，成对匹配，且与请求所用AK、SK保持一致。

步骤3 检查HTTP-Verb

签名所用HTTP-Verb与请求所用HTTP-Verb保持一致。

步骤4 检查Date/Expires

- Header中携带签名：检查签名所用Date与请求头域所带Date是否一致。
- URL中携带签名：检查签名所用Expires与请求URL中的Expires参数是否一致。

步骤5 检查头域

检查Content-MD5、Content-Type、Canonicalized Headers，如果计算签名时有包含在内，发送请求时也必须带上对应的头域。

说明

如果直接在浏览器中使用携带签名的URL访问OBS资源，因为这种方式不能携带头域参数，故在计算签名时也不能携带此类头域。

步骤6 检查Canonicalized Resource

Canonicalized Resource表示请求访问的obs资源，请严格按照API文档中Canonicalized Resource参数的规范设置。

步骤7 检查StringToSign

StringToSign的构造规则为：

- Header中携带签名：
  ```
  HTTP-Verb + "\n" + Content-MD5 + "\n" + Content-Type + "\n" + Date + "\n" + CanonicalizedHeaders + CanonicalizedResource
  ```
- URL中携带签名：
  ```
  HTTP-Verb + "\n" + Content-MD5 + "\n" + Content-Type + "\n" + Expires + "\n" + CanonicalizedHeaders + CanonicalizedResource
  ```

说明

值为空的参数处直接换行。

步骤8 检查签名算法

签名的计算方法：

1. 构造请求字符串（StringToSign）；
2. 对第一步的结果进行UTF-8编码；
3. 使用SK对第二步的结果进行HMAC-SHA1签名计算；
4. 对第三步的结果进行Base64编码，header中携带的签名到此得到最终的签名；
5. URL中携带的签名还需要对第4步的结果进行URL编码才能得到最终的签名。

----结束

3.6 安全性

3.6.1 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。

3.6.2 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。

3.6.3 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）。

3.6.4 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。

3.6.5 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。

3.6.6 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。

3.7 碎片管理

3.7.1 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。

3.7.2 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。

3.8 多版本控制

3.8.1 我可以上传同名对象到同一个文件夹中吗?

如果开启了多版本控制，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。

如果未开启多版本控制，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。

3.8.2 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**。

3.9 事件通知

3.9.1 哪些事件可以触发事件通知?

OBS支持对以下事件类型进行事件通知：

- **ObjectCreated**：表示所有创建对象的操作，包含Put、Post、Copy对象以及合并段。
  - **Put**：使用Put方法创建或覆盖对象。
  - **Post**：使用Post（表单上传）方法创建或覆盖对象。
  - **Copy**：使用copy（拷贝）方法创建或覆盖对象。
  - **CompleteMultipartUpload**：表示合并分段任务。
- **ObjectRemoved**：表示删除对象。
  - **Delete**：指定对象版本号删除对象。
  - **DeleteMarkerCreated**：不指定对象版本号删除对象。

3.10 生命周期管理

3.10.1 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。
- 某些文档在一段时间内经常访问，但是超过一定时间后便可能不再访问了。这些文档需要在一定时间后转化为温存储，冷存储或者删除。

如果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3-7**参数创建规则：

表 3-7 过期删除参数配置

参数	取值
状态	启用

参数	取值
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。如果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。

3.11 静态网站托管

3.11.1 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。

3.11.2 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。

3.11.3 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*。

3.12 跨区域复制

3.12.1 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。

3.12.2 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（冷存储对象除外）。
- 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。
- 桶中的历史对象（需要开启“同步历史对象”功能）。

3.12.3 创建跨区域复制规则后，为什么对象没有复制到目标桶中?

- 跨区复制规则没有开启“同步历史对象”功能的时候，桶中已有的对象不会复制到目标桶中。
- 新上传的对象存储类别为冷存储。
- 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。

3.13 服务端加密

3.13.1 OBS 是否支持对象加密上传?

OBS提供了服务端加密功能，用户可以使用加密的方式上传对象，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提供的多种访问方式中，对于对象加密上传的支持情况不同，具体如表3-8所示。

表 3-8 对象加密上传在不同访问方式下的支持情况

访问方式	是否支持对象加密上传	参考文档
OBS控制台	是	使用服务端加密方式上传对象
OBS Browser+	否 不支持对象加密上传，但如果桶配置了默认加密，那向该桶中上传的对象会自动加密。	-

访问方式	是否支持对象加密上传	参考文档
obsutil	否 不支持对象加密上传，但如果桶配置了默认加密，那向该桶中上传的对象会自动加密。	-
OBS API	是	请参考《对象存储服务接口参考》的“与服务端加密相关的接口”章节

3.13.2 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)和客户提供加密密钥的服务端加密（SSE-C）两种方式，SSE-C方式是指OBS使用用户提供的密钥和密钥的MD5值进行服务端加密。

A 修订记录

发布日期	修订记录
2024-02-29	第六次正式发布。 本次更新说明如下： ● 下线“欧洲-阿姆斯特丹-OP1”区域。
2022-10-30	第五次正式发布。 本次更新说明如下： ● 修改上传对象的大小限制说明。 ● 优化产品介绍和常见问题部分内容。
2022-05-17	第四次正式发布。 本次更新说明如下： ● 优化访问密钥和终端节点相关说明。
2021-11-19	第三次正式发布。 本次更新说明如下： ● 新增“欧洲-阿姆斯特丹-OP1”区域。
2020-12-11	第二次正式发布。
2019-01-04	第一次正式发布。