对象存储服务

用户指南（安卡拉区域）

文档版本 01

发布日期 2024-04-15

华为云计算技术有限公司

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云计算技术有限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，华为云计算技术有限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。

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

目 录

1 产品介绍

1.1 什么是对象存储服务

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

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

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

1.2 产品优势

OBS 与自建存储服务器对比

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

表 1-1 OBS 与自建存储服务器对比

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

对比项	OBS	自建存储服务器
安全性	支持HTTPS/SSL安全协议。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。
可靠性	通过五级可靠性架构，保障数据持久性最高达99.9999999999%（多可用区），业务连续性最高达99.95%（多可用区），远高于传统架构。	一般的企业自建存储服务器不会投入巨额的成本来同时保证介质、服务器、机柜、数据中心、区域级别的可靠性，一旦出现故障或灾难，很容易导致数据出现不可逆的丢失，给企业造成严重损失。
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、防盗链、VPC网络隔离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

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

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

1.4 权限管理

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

通过IAM，您可以在账号中给员工创建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。

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。

根据授权精细程度分为角色和策略。

- 角色：IAM最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。该机制以服务为粒度，提供有限的服务相关角色用于授权。由于各服务之间存在业务依赖关系，因此给用户授予角色时，可能需要一并授予依赖的其他角色，才能正确完成业务。角色并不能满足用户对精细化授权的要求，无法完全达到企业对权限最小化的安全管控要求。
- 策略：IAM最新提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。基于策略的授权是一种更加灵活的授权方式，能够满足企业对权限最小化的安全管控要求。例如：针对OBS服务，管理员能够控制IAM用户仅能对某一个桶资源进行指定的管理操作。多数细粒度策略以API接口为粒度进行权限拆分。

说明

由于缓存的存在，对用户、用户组授予OBS相关的角色和策略后，大概需要等待10~15分钟权限才能生效。

表1-2为OBS的所有系统权限。

表 1-2 OBS 系统权限

系统角色/策略名称	描述	类别	依赖关系
Tenant Administrator	拥有该权限的用户拥有除IAM外，其他所有服务的所有执行权限。	系统角色	无

系统角色/策略名称	描述	类别	依赖关系
Tenant Guest	拥有该权限的用户拥有除IAM外，其他所有服务的只读权限。	系统角色	无
OBS Administrator	拥有该权限的用户为OBS管理员，可以对账号下的所有OBS资源执行任意操作。	系统策略	无
OBS ReadOnlyAccess	拥有该权限的用户可以执行列举桶、获取桶基本信息、获取桶元数据、列举对象（不包含多版本）的操作。	系统策略	无
OBS OperateAccess	拥有该权限的用户可以执行OBS ReadOnlyAccess的所有操作，在此基础上还可以执行上传对象、下载对象、删除对象、获取对象ACL等对象基本操作。	系统策略	无

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 1-3 OBS 操作与资源权限关系

操作名称	Tenant Administrator	Tenant Guest	OBS Administrator	OBS ReadOnly Access	OBS OperateAccess
列举桶	可以	可以	可以	可以	可以
创建桶	可以	不可以	可以	不可以	不可以
删除桶	可以	不可以	可以	不可以	不可以
获取桶基本信息	可以	可以	可以	可以	可以
管理桶访问权限	可以	不可以	可以	不可以	不可以
管理桶策略	可以	不可以	可以	不可以	不可以
列举对象	可以	可以	可以	可以	可以
列举多版本对象	可以	可以	可以	不可以	不可以
上传文件	可以	不可以	可以	不可以	可以
新建文件夹	可以	不可以	可以	不可以	可以
删除文件	可以	不可以	可以	不可以	可以
删除文件夹	可以	不可以	可以	不可以	可以
下载文件	可以	可以	可以	不可以	可以

操作名称	Tenant Administrator	Tenant Guest	OBS Administrator	OBS ReadOnly Access	OBS OperateAccess
删除多版本文件	可以	不可以	可以	不可以	可以
下载多版本文件	可以	可以	可以	不可以	可以
取消删除文件	可以	不可以	可以	不可以	可以
删除碎片	可以	不可以	可以	不可以	可以
管理对象访问权限	可以	不可以	可以	不可以	不可以
设置对象元数据	可以	不可以	可以	不可以	不可以
获取对象元数据	可以	可以	可以	不可以	可以
管理多版本控制	可以	不可以	可以	不可以	不可以
管理日志记录	可以	不可以	可以	不可以	不可以
管理事件通知	可以	不可以	可以	不可以	不可以
管理生命周期规则	可以	不可以	可以	不可以	不可以
管理静态网站托管	可以	不可以	可以	不可以	不可以
管理CORS规则	可以	不可以	可以	不可以	不可以
管理防盗链	可以	不可以	可以	不可以	不可以
域名管理	可以	不可以	可以	不可以	不可以
管理跨区域复制	可以	不可以	可以	不可以	不可以
追加写对象	可以	不可以	可以	不可以	可以
设置对象ACL	可以	不可以	可以	不可以	不可以
设置指定版本对象ACL	可以	不可以	可以	不可以	不可以

操作名称	Tenant Administrator	Tenant Guest	OBS Administrator	OBS ReadOnly Access	OBS OperateAccess
获取对象ACL	可以	可以	可以	不可以	可以
获取指定版本对象ACL	可以	可以	可以	不可以	可以
多段上传	可以	不可以	可以	不可以	可以
列举已上传段	可以	可以	可以	不可以	可以
取消多段上传任务	可以	不可以	可以	不可以	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 1-4 对象存储服务 OBS 使用限制

限制项	说明
小文件容量利用率	OBS定义的小文件是小于200KB的对象，小文件存放OBS底层会占用比文件真实大小更大的物理存储空间，对外表现为空间利用率低。OBS单节点可以支撑的对象数有限，因此海量小文件场景OBS的空间利用率随着文件越小，利用率越低。如果明确是海量小文件场景，建议单独规划存储容量和存储节点，提前做好扩容准备。
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。

1.6 使用方式

您可以通过以下工具连接到OBS资源，对资源进行管理操作。

表 1-5 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和MAC系统上的对象存储服务客户端，可以非常方便地让您在个人电脑上进行对象存储的操作。
API	OBS提供REST形式的访问接口，使用户能够非常容易地从Web应用中访问OBS。用户可以通过本文档提供的简单的REST接口，在任何时间、任何地点、任何互联网设备上进行上传和下载数据。

1.7 与其他服务的关系

表 1-6 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** **创建委托**
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**

OBS可以作为其他云服务的存储资源池，例如镜像服务（Image Management Service，IMS）等。

1.8 基本概念

1.8.1 对象

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

对象包括了Key，Metadata，Data三部分：

- Key：键值，即对象的名称，为经过UTF-8编码的长度大于0且不超过1024的字符序列。一个桶里的每个对象必须拥有唯一的对象键值。

- Metadata：元数据，即对象的描述信息，包括系统元数据和用户元数据，这些元数据以键值对（Key-Value）的形式被上传到OBS中。
  - 系统元数据由OBS自动产生，在处理对象数据时使用，包括Date，Content-length，Last-modify，ETag等。
  - 用户元数据由用户在上传对象时指定，是用户自定义的对象描述信息。
- Data：数据，即文件的数据内容。

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

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

1.8.2 桶

桶（Bucket）是OBS中存储对象的容器。对象存储提供了基于桶和对象的扁平化存储方式，桶中的所有对象都处于同一逻辑层级，去除了文件系统中的多层级树形目录结构。

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

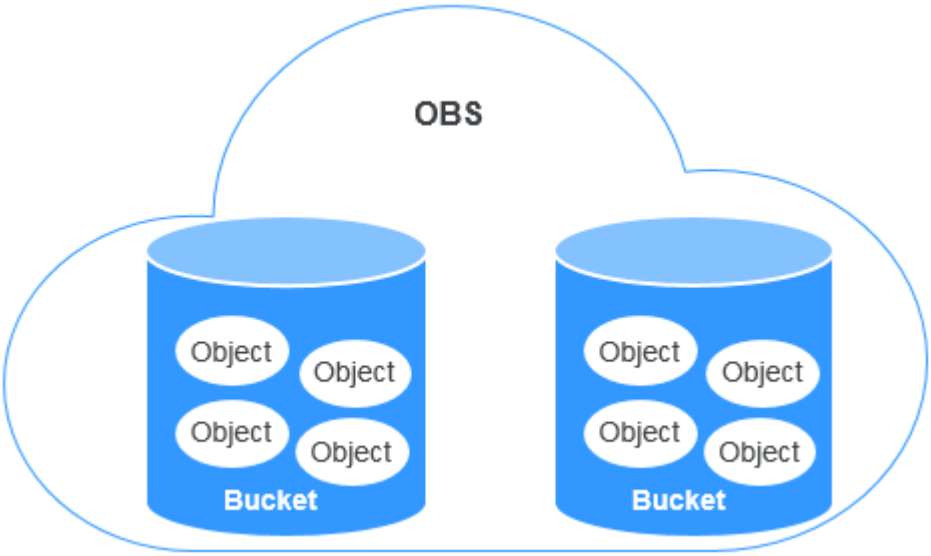
在OBS中，桶名必须是全局唯一的且不能修改，即用户创建的桶不能与自己已创建的其他桶名称相同，也不能与同账号、其他账号及账号下的所有IAM子用户创建的桶名称相同。桶所属的区域在创建后也不能修改。每个桶在创建时都会生成默认的桶ACL（Access Control List，访问控制列表），桶ACL的每项包含了对被授权用户授予什么样的权限，如读取权限、写入权限等。用户只有对桶有相应的权限，才可以对桶进行操作，如创建、删除、显示、设置桶ACL等。

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1-1**所示：

图 1-1 桶和对象



1.8.3 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》。

1.8.4 访问密钥（AK/SK）

OBS支持通过访问密钥认证方式进行认证鉴权，即使用AK/SK加密的方法来验证某个请求发送者身份。

访问密钥（AK/SK，Access Key ID/Secret Access Key）包含访问密钥ID（AK）和秘密访问密钥（SK）两部分。通过AK识别访问用户的身份，通过SK对请求数据进行签名验证，用于确保请求的机密性、完整性和请求者身份的正确性。

当您使用OBS提供的API进行二次开发并通过AK/SK认证方式完成认证鉴权时，需要按照OBS定义的签名算法来计算签名并添加到请求中。

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

永久AK/SK

用户可以在“我的凭证”页面创建永久AK/SK。

- Access Key Id（AK）：访问密钥ID。与秘密访问密钥关联的唯一标识符，通过访问密钥ID（AK）识别访问用户的身份。
- Secret Access Key（SK）：秘密访问密钥。与访问密钥ID结合使用，对请求数据进行签名验证，可标识发送方，并防止请求被修改，确保请求的机密性、完整性和请求者身份的正确性。

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。与临时秘密访问密钥关联的唯一标识符，通过临时访问密钥ID（AK）识别访问用户的身份。
- 临时Secret Access Key：临时秘密访问密钥。与临时访问密钥ID结合使用，对请求数据进行签名验证，可标识发送方，并防止请求被修改，确保请求的机密性、完整性和请求者身份的正确性。
- securitytoken：与临时访问密钥ID和临时秘密访问密钥结合使用，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 1-7 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。
API	在计算签名时添加AK和SK到请求中。

1.8.5 终端节点（Endpoint）和访问域名

终端节点（Endpoint）：OBS为每个区域提供一个终端节点，终端节点可以理解为OBS在不同区域的区域域名，用于处理各自区域的访问请求。请向企业管理员获取区域和终端节点信息。

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 1-8 OBS 终端节点信息

区域名称	区域	终端节点（Endpoint）	协议类型
土耳其-安卡拉-PUR	tr-central-201	obs.tr-central-201.hc.vodafone.com.tr	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1-9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 1-9 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 1-8**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管理控制台或OBS Browser+上查看对象属性获取。	HTTPS HTTP
静态网站访问域名	**BucketName.obs-website.Endpoint**	桶配置为静态网站托管时，桶的静态网站访问域名。	HTTPS HTTP
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

1.8.6 区域和可用区

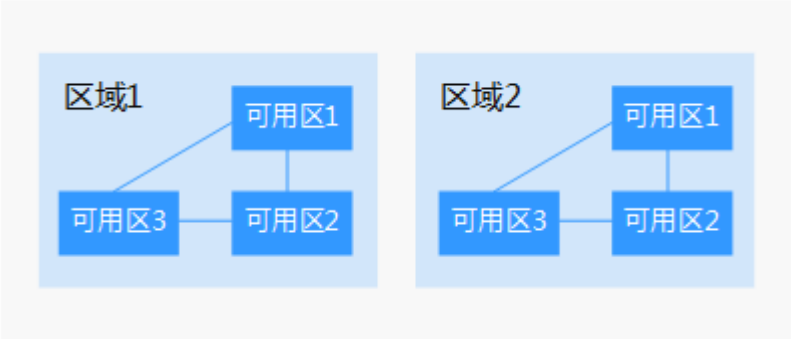
什么是区域、可用区?

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

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

图1-2阐明了区域和可用区之间的关系。

图 1-2 区域和可用区



如何选择区域?

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

如何选择可用区?

是否将资源放在同一可用区内，主要取决于您对容灾能力和网络时延的要求。

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

区域和终端节点

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

2 使用前配置

2.1 配置本地 hosts

在使用OBS的基本功能之前，需要根据本章的要求完成DNS或本地hosts配置。

说明

无论使用OBS桶还是并行文件系统，都需要按照本节介绍完成本地hosts配置。

场景介绍

终端用户访问OBS主要有以下场景，具体见表2-1。

表 2-1 访问 OBS 的场景

访问OBS的方式	使用前需要执行的配置操作	操作角色
通过云外本地网络（IDC）访问（无DNS服务器）	配置本地hosts	终端用户

配置说明

本章下述的所有配置均为举例，都遵循以下部署场景的前提，实际配置请以实际信息为准。

场景假设：

云服务对外提供的全局域名为**huaweicloud.com**，OBS分别部署在两个区域（regionID分别为**region1**和**region2**），其中：

- region1为默认区域，其默认集群lz01的IP地址为192.168.0.1
- region2为非默认区域，其默认集群lz01的IP地址为192.168.0.2

场景：配置本地 hosts

针对通过本地网络访问OBS（无DNS服务器）的场景，终端用户需要在本地hosts文件中增加如下配置信息：

注：每新创建一个桶，都需要新增对应桶的两条host记录，两条记录的域名分别为携带区域信息的域名和不携带区域信息的域名，详情参见示例下方的说明。

```
192.168.0.1 obs.huaweicloud.com
192.168.0.1 obs.region1.huaweicloud.com
192.168.0.2 obs.region2.huaweicloud.com
192.168.0.1 obsbrowser.obs.region1.huaweicloud.com #下载OBS Browser+前需要配置本条
192.168.0.1 bucket1.obs.region1.huaweicloud.com
192.168.0.2 bucket2.obs.region2.huaweicloud.com
192.168.0.1 bucket1.obs.huaweicloud.com
192.168.0.2 bucket2.obs.huaweicloud.com
.....
```

以下内容在需要使用静态网站托管功能时配置：

```
192.168.0.1 bucket1.obs-website.region1.huaweicloud.com
192.168.0.2 bucket2.obs-website.region2.huaweicloud.com
.....
```

说明

1. 上述全局域名名称（huaweicloud.com）、regionID（region1、region2）、桶名（bucket1、bucket2）、IP地址（192.168.0.1、192.168.0.2）仅为示例，具体以实际情况为准。
   - 第一条为OBS全局域名的配置，填写的IP地址为OBS的全局IP地址，即默认区域默认集群lz01的IP地址。获取方法：在默认区域CloudAutoDeploy-EDK“工程管理 >工程列表”页面，单击工程操作列的“导出交付件”，解压导出的压缩包后打开obs目录下的《obs_lld.xlsx》文件，获取lz01的lvs节点“OM IP /27”列的virtual_ip。
   - 除第一条以外，其他为各region域名的配置，填写的IP地址为各region默认集群的IP地址。获取方法：在各区域CloudAutoDeploy-EDK“工程管理 >工程列表”页面，单击工程操作列的“导出交付件”，解压导出的压缩包后打开obs目录下的《obs_lld.xlsx》文件，获取lz01的lvs节点“OM IP /27”列的virtual_ip。
2. Hosts文件路径
   - Windows：C:\Windows\System32\drivers\etc\hosts
   - Linux：/etc/hosts
3. 除了前三条全局和区域级的配置外，每个需要访问的OBS桶的访问域名也需要配置到Hosts文件中，例如以上示例中的bucket1、bucket2。实际配置需要替换为实际的桶名，并且其区域信息（regionID和对应的默认集群IP地址）也需要替换为桶对应的区域实际信息。每个桶需要同时配置2条记录，分别为携带区域信息的域名和不携带区域信息的域名。
4. 第四条为下载OBS Browser+前需要配置的内容，将OBS Browser+软件包所在桶的域名配置到Hosts文件中才能成功下载。上述桶域名中桶名（obsbrowser）和regionID（region1）仅为示例，实际以在控制台主界面OBS Browser+的下载链接中的信息为准。

3 控制台指南

3.1 控制台功能概述

目前，OBS管理控制台提供的功能如表3-1所示：

表 3-1 功能概述

功能	说明
桶基本操作	指定region（不同服务区域）创建桶、删除桶等。
对象基本操作	管理对象，包括上传（含多段上传功能）、下载、删除等。
对象元数据	根据用户需要为对象设置属性。
碎片管理	碎片管理功能可以清除由于对象上传失败而产生的碎片。
多版本控制	管理桶的多版本状态，允许桶内同一个对象存在多个版本。
日志记录	支持对桶的访问请求创建并保存访问日志记录，可用于进行请求分析。
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。
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。

功能	说明
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。
桶清单	桶清单功能可以定期生成桶内对象的相关信息，保存在CSV格式的文件中，并上传到您指定的桶中。
2AZ容灾	您可以为桶开启2AZ容灾功能，开启后可以将数据存储在2个不同可用区（AZ），以获得更高的数据可靠性。2AZ容灾策略一旦确认，后续无法更改。

3.2 使用限制

OBS管理控制台支持的浏览器版本如表3-2所示：

表 3-2 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

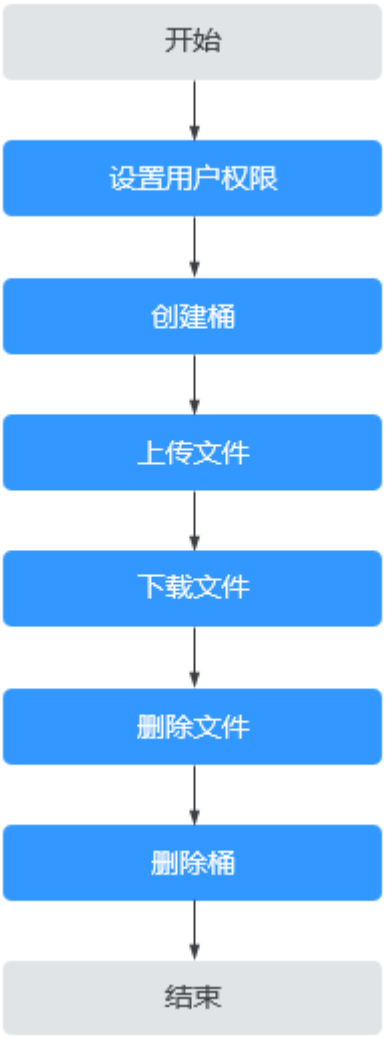
3.3 入门

3.3.1 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3-1中所示的任务。

图 3-1 快速入门



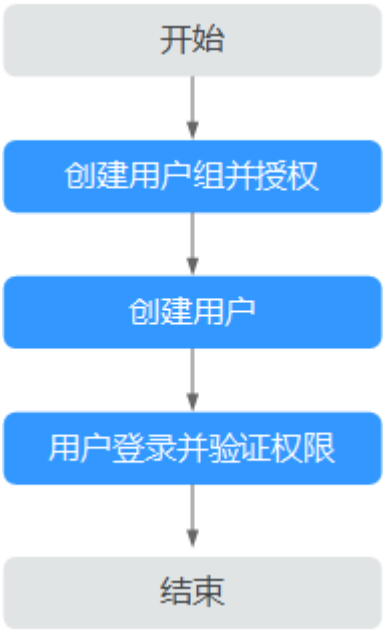
3.3.2 设置用户权限

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 3-2 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“授权”。
5. 在“选择决策”步骤中，可以根据需求在右上方进行筛选策略，选中策略名称，单击“下一步”。
6. 在“设置最小授权范围”步骤中，选择“全局服务资源”，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。

   由于缓存的存在，对用户、用户组授予OBS相关的RBAC策略和细粒度策略后，大概需要等待10~15分钟策略才能生效。

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

3.3.3 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 3-3 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。
可用区	桶所属可用区。当一个区域下有多个可用区时，可以将桶分别创建在不同可用区的集群中，通过跨集群复制实现可用区级别容灾，详情请参见**跨集群复制**。
集群	桶所属集群。OBS提供跨集群复制能力，可通过跨集群复制实现可用区级别容灾，详情请参见**跨集群复制**。
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（.）。

参数	描述
集群类型	• 公共集群：选择后，本次创建的桶将创建在所有用户共享的公共集群上。 • 专属集群：选择后，本次创建的桶将创建在您购买的专属集群上。 **说明** 仅开通专属集群的用户支持选择集群类型，其他用户默认选择公共集群。
容灾	• 关闭：数据仅存储在单个可用区（AZ），成本更低。 • 开启：数据将冗余存储在同一区域的2个可用区中，可靠性更高，但费用较高，开启后不支持关闭。
数据冗余存储策略	• 多AZ存储：数据冗余存储至多个可用区（AZ），可靠性更高。 • 单AZ存储：数据仅存储在单个可用区（AZ），成本更低。 请根据业务情况提前规划数据冗余存储策略，桶一旦创建成功，数据冗余存储策略就确定了，后续无法更改。
桶策略	桶的读写权限控制。 • 私有：除桶ACL授权外的其他用户无桶的访问权限。 • 公共读：任何用户都可以对桶内对象进行读操作。 • 公共读写：任何用户都可以对桶内对象进行读/写/删除操作。

步骤3 单击“立即创建”。

----结束

3.3.4 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+）或OBS API的多段上传接口上传。OBS Browser+软件包集成在OBS控制台上，登录OBS控制台，在控制台主界面单击OBS Browser+的下载链接进行下载。

注意：下载和使用OBS Browser+前，需要确保已**配置本地hosts**，以保证OBS Browser+下载和使用正常。

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

- 请确保已按照**配置本地hosts**的要求，完成相关配置。
- 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“对象”页面。

步骤2 进入待上传的文件夹，单击“上传对象”，系统弹出“上传对象”对话框。

说明

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

步骤3 拖拽本地文件或文件夹至“上传对象”区域框内添加待上传的文件。

也可以通过单击“上传对象”区域框内的“添加文件”，选择本地文件进行添加。

步骤4 **可选**：如果您需要配置元数据，可单击“下一步：高级配置（可选）”进行配置。

可配置的对象元数据包括：ContentDisposition、ContentLanguage、WebsiteRedirectLocation、ContentEncoding、ContentType。各元数据具体含义请参见**对象元数据**。元数据是一组名称值对，包括名称和值，值不能为空。如需配置两组以上元数据，单击“添加”即可新增。

步骤5 单击“上传”。

----结束

3.3.5 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。

前提条件

请确保已按照**配置本地hosts**的要求，完成相关配置。

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“对象”页面。

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

说明

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

----结束

3.3.6 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“对象”页面。

步骤2 选中待删除的文件，并单击右侧的“更多>删除”。

也可以选择多个文件，单击文件列表上方的“删除”删除多个文件。

步骤3 单击“确定”，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。

3.3.7 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“确定”，确认删除桶。

----结束

3.4 桶管理

3.4.1 创建桶

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

说明

一个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 3-4 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。
可用区	桶所属可用区。当一个区域下有多个可用区时，可以将桶分别创建在不同可用区的集群中，通过跨集群复制实现可用区级别容灾，详情请参见**跨集群复制**。
集群	桶所属集群。OBS提供跨集群复制能力，可通过跨集群复制实现可用区级别容灾，详情请参见**跨集群复制**。
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（.）。
集群类型	● 公共集群：选择后，本次创建的桶将创建在所有用户共享的公共集群上。 ● 专属集群：选择后，本次创建的桶将创建在您购买的专属集群上。 **说明** 仅开通专属集群的用户支持选择集群类型，其他用户默认选择公共集群。
容灾	● 关闭：数据仅存储在单个可用区（AZ），成本更低。 ● 开启：数据将冗余存储在同一区域的2个可用区中，可靠性更高，但费用较高，开启后不支持关闭。

参数	描述
数据冗余存储策略	● 多AZ存储：数据冗余存储至多个可用区（AZ），可靠性更高。 ● 单AZ存储：数据仅存储在单个可用区（AZ），成本更低。 请根据业务情况提前规划数据冗余存储策略，桶一旦创建成功，数据冗余存储策略就确定了，后续无法更改。
桶策略	桶的读写权限控制。 ● 私有：除桶ACL授权外的其他用户无桶的访问权限。 ● 公共读：任何用户都可以对桶内对象进行读操作。 ● 公共读写：任何用户都可以对桶内对象进行读/写/删除操作。

步骤3 单击“立即创建”。

----结束

3.4.2 查看桶的信息

您可以通过OBS管理控制台直接查看某个桶的详情，包括页面上方桶的部分信息、桶的基本信息、常见场景操作指引、域名信息、基础配置模块。

查看桶详情

步骤1 在OBS管理控制台桶列表中，单击待操作的桶，进入“对象”页面。

步骤2 在左侧导航栏，单击“概览”，进入“概览”页面。

步骤3 在页面上方可查看桶的部分信息，包含桶名称、所属区域、创建时间。

表 3-5 桶信息参数说明

参数	说明
桶名称	桶的名称。
区域	桶所在的区域。
创建时间	桶的创建时间。

步骤4 在页面上方可查看桶的基本信息，包含对象个数、存储用量、桶版本号、多版本控制状态和账号ID。

表 3-6 桶基本信息参数说明

参数	说明
对象个数	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。

参数	说明
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。 **说明** 当该桶支持用量统计时，存储用量数据在此处不展示。
桶版本号	桶的版本号。
多版本控制状态	多版本控制的状态。
账号ID	桶的拥有者全局唯一标识，与“我的凭证”页面的“账号ID”相同。

步骤5 在“操作指引”下查看常见场景的操作指引，单击右上角“切换场景”可选择切换权限管理、数据加速和网站托管场景的操作指引。

单击流程节点，可在下方查看对应流程节点下的细节；单击流程细节卡片，可跳转到对应流程细节的操作指导或控制台页面。

步骤6 在“域名信息”下查看桶的域名信息，包含Endpoint(终端节点)、访问域名、静态网页托管域名，可在操作列进行相关的操作。

步骤7 在“基础配置”下查看桶的基础配置信息，包含生命周期规则、静态网站托管、CORS规则等，单击卡片可执行对应操作。

----结束

导出桶列表

步骤1 进入OBS管理控制台桶列表页面。

步骤2 全部导出：单击桶列表左上方的“导出”按钮。

步骤3 选择导出：勾选需要导出的桶，单击列表左上方的“导出”按钮。

步骤4 浏览器会自动下载桶列表Excel，其中包含本账号下所有桶的如下信息：

桶名称、区域、数据冗余存储策略、存储用量、对象个数、桶版本号、创建时间。

----结束

3.4.3 搜索桶

OBS管理控制台支持按桶名称、区域搜索桶。

说明

搜索不区分大小写。

操作步骤

步骤1 在桶列表上方的搜索框中单击左键，在一级下拉框中选择“桶名称”、“区域”，然后在二级下拉框中选择你需要的选项，也可以输入关键字后再进行选择。

搜索到的桶会展示在桶列表中。

例如：您需要查找桶名称为“test”的桶，您只需在主页面上方的搜索框中单击左键，在一级下拉框中选择“桶名称”，在二级下拉框中选择“test”，或者选择“桶名称”后在搜索框中输入“test”，所有桶名称中包含“test”字符的桶都会展示到二级下拉框中，然后单击“test”。搜索到的桶会展示在桶列表中。

说明

- 桶列表支持组合过滤。
  - 当筛选条件不同时：筛选条件是交集的关系。
  - 当筛选条件相同时：筛选条件是并集的关系。
- 在桶列表上方的搜索框中直接输入关键字，桶名称、区域中包含关键字的所有桶都会展示到下拉框中，单击选择您需要的选项，符合条件的桶会在列表中展示。

步骤2 或者在桶列表上方的搜索框中直接输入关键字，单击 或Enter键。

搜索到的桶名称、区域、数据冗余存储策略中包含关键字的所有桶会展示在桶列表中。

例如：您在主页面上方的搜索框中输入“test”并单击 或Enter键，桶名称、区域、数据冗余存储策略中包含“test”关键字的所有桶都会展示到桶列表中。

----结束

相关操作

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

3.4.4 删除桶

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

前提条件

- 已彻底删除桶中对象。只有彻底删除对象后，才能删除桶。

  须知

  对象、碎片和已删除对象列表中对象都要删除。

- 只有桶的拥有者才能删除桶。

操作步骤

步骤1 在OBS管理控制台桶列表中，选择待删除的桶，并单击右侧的“删除”。

说明

用户删除桶后，需要等待30分钟才能创建同名桶和并行文件系统。

步骤2 单击“确定”，确认删除桶。

----结束

3.5 对象管理

3.5.1 新建文件夹

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

背景知识

- 由于OBS是一种对象存储服务，并没有文件系统中的文件和文件夹概念。为了使用户更方便进行管理数据，OBS提供了一种方式模拟文件夹。实际上在OBS内部是通过在对象的名称中增加“/”，将该对象在OBS管理控制台上模拟成一个文件夹的形式展现。通过API列举对象，获取到的对象名就是以“/”分隔的，最后一个“/”后的内容就是对象名。如果最后一个“/”后没有内容，则表示一个文件夹路径。文件夹的层级结构深度不会影响访问对象的性能。
- 文件夹不支持通过管理控制台进行下载，您可以使用OBS Browser+来下载文件夹。

操作步骤

步骤1 在OBS管理控制台桶列表中，单击待操作的桶，进入“对象”页面。

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

步骤3 在“文件夹名称”中输入新文件夹名称。

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

步骤4 单击“确定”。

----结束

后续操作

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

3.5.2 上传对象

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

约束与限制

- OBS管理控制台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+）或OBS API的多段上传接口上传。OBS Browser+软件包集成在OBS控制台上，登录OBS控制台，在控制台主界面单击OBS Browser+的下载链接进行下载。

  须知

  下载和使用OBS Browser+前，需要确保已**配置本地hosts**，以保证OBS Browser+下载和使用正常。

- 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

- 请确保已按照**配置本地hosts**的要求，完成相关配置。
- 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“对象”页面。

步骤2 进入待上传的文件夹，单击“上传对象”，系统弹出“上传对象”对话框。

说明

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

步骤3 拖拽本地文件或文件夹至“上传对象”区域框内添加待上传的文件。

也可以通过单击“上传对象”区域框内的“添加文件”，选择本地文件进行添加。

步骤4 **可选**：如果您需要配置元数据，可单击“下一步：高级配置（可选）”进行配置。

可配置的对象元数据包括：ContentDisposition、ContentLanguage、WebsiteRedirectLocation、ContentEncoding、ContentType。各元数据具体含义请参见**对象元数据**。元数据是一组名称值对，包括名称和值，值不能为空。如需配置两组以上元数据，单击“添加”即可新增。

步骤5 单击“上传”。

----结束

后续操作

您可以单击对象后面的“复制路径”，复制对象的路径。

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

3.5.3 下载对象

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

前提条件

请确保已按照**配置本地hosts**的要求，完成相关配置。

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“对象”页面。

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

也可以选中多个文件，单击文件列表上方的“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

3.5.4 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“对象”页面。

步骤2 在对象列表右上方的搜索框中输入需要查找的文件或文件夹的前缀。

搜索结果为根目录级别下的前缀为搜索内容的文件和文件夹。

说明

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

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

步骤3 单击  ，搜索结果在对象列表中显示。

----结束

相关操作

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

3.5.5 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**。

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“对象”页面。

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

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

----结束

3.5.6 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“对象”页面。

步骤2 选中待删除的文件或文件夹，并单击右侧的“更多 > 删除”。

也可以选中多个文件或文件夹，单击文件列表上方的“删除”进行批量删除。

步骤3 单击“确定”，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4 对于启用了多版本控制的OBS桶，想要彻底删除文件或文件夹，需要再到“已删除对象”列表进行删除。

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

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

----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。

3.5.7 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“对象”页面。

步骤2 单击“已删除对象”。

步骤3 在要找回的已删除文件所在行，单击右侧的“取消删除”。

也可以选中多个文件，单击文件列表上方的“取消删除”进行批量找回。

----结束

相关操作

通过删除带“删除标记”的版本来找回文件的方法：

步骤1 在OBS管理控制台桶列表中，单击待操作的桶，进入“对象”页面。

步骤2 单击“已删除对象”。

步骤3 单击要找回的文件名称，系统显示该文件信息。

步骤4 在“版本”页签，显示该文件的所有版本。

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

----结束

3.5.8 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。

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“对象”页面。

步骤2 单击“碎片”，选中需要清理的碎片，单击右侧的“删除”。

也可选中多个碎片，单击对象列表上方的“删除”进行批量删除。

步骤3 单击“确定”，确认删除碎片。

----结束

3.6 对象元数据

3.6.1 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 3-7 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。
WebsiteRedirectLocation	为对象提供重定向功能，重定向到其他对象或者外部的URL。重定向功能通过静态网站托管实现。 例如，可根据如下步骤实现对象重定向功能。 1. 为桶“testbucket”根目录下的对象“testobject.html”设置元数据，元数据名称选择为“WebsiteRedirectLocation”，元数据值填写为“http://www.example.com” **说明** OBS仅支持为桶根目录下的对象设置重定向，不支持为桶中文件夹下的对象设置重定向。 2. 在桶“testbucket”中配置静态网站托管，将该桶中的对象“testobject.html”设置为静态网站托管的“默认首页”。 3. 当通过静态网站托管页面上的“访问地址”访问对象“testobject.html”时，会直接重定向访问http://www.example.com。
ContentEncoding	指定对象被下载时的内容编码格式，可以设置如下类型： ● 标准定义：compress、deflate、exi、identity、gzip、pack200-gzip ● 其他：br、bzip2、lzma 、peerdist、sdch、xpress、xz

名称	说明
CacheControl	指定对象被下载时的网页的缓存行为。 • 可缓冲性：public、private、no-cache、only-if-cached • 到期时间：max-age=<*seconds*>、s-maxage=<*seconds*>、max-stale[=<*seconds*>]、min-fresh=<*seconds*>、stale-while-revalidate=<*seconds*>、stale-if-error=<*seconds*> • 重新验证和重新加载：must-revalidate、proxy-revalidate、immutable • 其他：no-store、no-transform
Expires	设置缓存过期时间（GMT）。
ContentType	设置对象的文件类型。详见**对象元数据Content-Type介绍**。

说明

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

3.6.2 对象元数据 Content-Type 介绍

上传到OBS中的对象，会根据对象的文件扩展名，自动匹配Content-Tpye值。使用浏览器访问对象时，会根据Content-Tpye类型来指定应用程序来打开。您可以根据对象的文件扩展来修改Content-Type。

表 3-8 常见的 Content-Type 类型

文件扩展名	Content-Type	文件扩展名	Content-Type
.*（二进制流，不知道下载文件类型）	application/octet-stream	.tif	image/tiff
.001	application/x-001	.301	application/x-301
.323	text/h323	.906	application/x-906
.907	drawing/907	.a11	application/x-a11
.acp	audio/x-mei-aac	.ai	application/postscript
.aif	audio/aiff	.aifc	audio/aiff
.aiff	audio/aiff	.anv	application/x-anv
.asa	text/asa	.asf	video/x-ms-asf

文件扩展名	Content-Type	文件扩展名	Content-Type
.asp	text/asp	.asx	video/x-ms-asf
.au	audio/basic	.avi	video/avi
.awf	application/vnd.adobe.workflow	.biz	text/xml
.bmp	application/x-bmp	.bot	application/x-bot
.c4t	application/x-c4t	.c90	application/x-c90
.cal	application/x-cals	.cat	application/vnd.ms-pki.seccat
.cdf	application/x-netcdf	.cdr	application/x-cdr
.cel	application/x-cel	.cer	application/x-x509-ca-cert
.cg4	application/x-g4	.cgm	application/x-cgm
.cit	application/x-cit	.class	java/*
.cml	text/xml	.cmp	application/x-cmp
.cmx	application/x-cmx	.cot	application/x-cot
.crl	application/pkix-crl	.crt	application/x-x509-ca-cert
.csi	application/x-csi	.css	text/css
.cut	application/x-cut	.dbf	application/x-dbf
.dbm	application/x-dbm	.dbx	application/x-dbx
.dcd	text/xml	.dcx	application/x-dcx
.der	application/x-x509-ca-cert	.dgn	application/x-dgn
.dib	application/x-dib	.dll	application/x-msdownload
.doc	application/msword	.dot	application/msword
.drw	application/x-drw	.dtd	text/xml
.dwf	Model/vnd.dwf	.dwf	application/x-dwf
.dwg	application/x-dwg	.dxb	application/x-dxb
.dxf	application/x-dxf	.edn	application/vnd.adobe.edn

文件扩展名	Content-Type	文件扩展名	Content-Type
.emf	application/x-emf	.eml	message/rfc822
.ent	text/xml	.epi	application/x-epi
.eps	application/x-ps	.eps	application/postscript
.etd	application/x-ebx	.exe	application/x-msdownload
.fax	image/fax	.fdf	application/vnd.fdf
.fif	application/fractals	.fo	text/xml
.frm	application/x-frm	.g4	application/x-g4
.gbr	application/x-gbr	.	application/x-
.gif	image/gif	.gl2	application/x-gl2
.gp4	application/x-gp4	.hgl	application/x-hgl
.hmr	application/x-hmr	.hpg	application/x-hpgl
.hpl	application/x-hpl	.hqx	application/mac-binhex40
.hrf	application/x-hrf	.hta	application/hta
.htc	text/x-component	.htm	text/html
.html	text/html	.htt	text/webviewhtml
.htx	text/html	.icb	application/x-icb
.ico	image/x-icon	.ico	application/x-ico
.iff	application/x-iff	.ig4	application/x-g4
.igs	application/x-igs	.iii	application/x-iphone
.img	application/x-img	.ins	application/x-internet-signup
.isp	application/x-internet-signup	.IVF	video/x-ivf
.java	java/*	.jfif	image/jpeg
.jpe	image/jpeg	.jpe	application/x-jpe
.jpeg	image/jpeg	.jpg	image/jpeg
.jpg	application/x-jpg	.js	application/x-javascript

文件扩展名	Content-Type	文件扩展名	Content-Type
.jsp	text/html	.la1	audio/x-liquid-file
.lar	application/x-laplayer-reg	.latex	application/x-latex
.lavs	audio/x-liquid-secure	.lbm	application/x-lbm
.lmsff	audio/x-la-lms	.ls	application/x-javascript
.ltr	application/x-ltr	.m1v	video/x-mpeg
.m2v	video/x-mpeg	.m3u	audio/mpegurl
.m4e	video/mpeg4	.mac	application/x-mac
.man	application/x-troff-man	.math	text/xml
.mdb	application/msaccess	.mdb	application/x-mdb
.mfp	application/x-shockwave-flash	.mht	message/rfc822
.mhtml	message/rfc822	.mi	application/x-mi
.mid	audio/mid	.midi	audio/mid
.mil	application/x-mil	.mml	text/xml
.mnd	audio/x-musicnet-download	.mns	audio/x-musicnet-stream
.mocha	application/x-javascript	.movie	video/x-sgi-movie
.mp1	audio/mp1	.mp2	audio/mp2
.mp2v	video/mpeg	.mp3	audio/mp3
.mp4	video/mp4	.mpa	video/x-mpg
.mpd	application/vnd.ms-project	.mpe	video/x-mpeg
.mpeg	video/mpg	.mpg	video/mpg
.mpga	audio/rn-mpeg	.mpp	application/vnd.ms-project
.mps	video/x-mpeg	.mpt	application/vnd.ms-project
.mpv	video/mpg	.mpv2	video/mpeg

文件扩展名	Content-Type	文件扩展名	Content-Type
.mpw	application/vnd.ms-project	.mpx	application/vnd.ms-project
.mtx	text/xml	.mxp	application/x-mmxp
.net	image/pnetvue	.nrf	application/x-nrf
.nws	message/rfc822	.odc	text/x-ms-odc
.out	application/x-out	.p10	application/pkcs10
.p12	application/x-pkcs12	.p7b	application/x-pkcs7-certificates
.p7c	application/pkcs7-mime	.p7m	application/pkcs7-mime
.p7r	application/x-pkcs7-certreqresp	.p7s	application/pkcs7-signature
.pc5	application/x-pc5	.pci	application/x-pci
.pcl	application/x-pcl	.pcx	application/x-pcx
.pdf	application/pdf	.pdf	application/pdf
.pdx	application/vnd.adobe.pdx	.pfx	application/x-pkcs12
.pgl	application/x-pgl	.pic	application/x-pic
.pko	application/vnd.ms-pki.pko	.pl	application/x-perl
.plg	text/html	.pls	audio/scpls
.plt	application/x-plt	.png	image/png
.png	application/x-png	.pot	application/vnd.ms-powerpoint
.ppa	application/vnd.ms-powerpoint	.ppm	application/x-ppm
.pps	application/vnd.ms-powerpoint	.ppt	application/vnd.ms-powerpoint
.ppt	application/x-ppt	.pr	application/x-pr
.prf	application/pics-rules	.prn	application/x-prn

文件扩展名	Content-Type	文件扩展名	Content-Type
.prt	application/x-prt	.ps	application/x-ps
.ps	application/postscript	.ptn	application/x-ptn
.pwz	application/vnd.ms-powerpoint	.r3t	text/vnd.rn-realtext3d
.ra	audio/vnd.rn-realaudio	.ram	audio/x-pn-realaudio
.ras	application/x-ras	.rat	application/rat-file
.rdf	text/xml	.rec	application/vnd.rn-recording
.red	application/x-red	.rgb	application/x-rgb
.rjs	application/vnd.rn-realsystem-rjs	.rjt	application/vnd.rn-realsystem-rjt
.rlc	application/x-rlc	.rle	application/x-rle
.rm	application/vnd.rn-realmedia	.rmf	application/vnd.adobe.rmf
.rmi	audio/mid	.rmj	application/vnd.rn-realsystem-rmj
.rmm	audio/x-pn-realaudio	.rmp	application/vnd.rn-rn_music_package
.rms	application/vnd.rn-realmedia-secure	.rmvb	application/vnd.rn-realmedia-vbr
.rmx	application/vnd.rn-realsystem-rmx	.rnx	application/vnd.rn-realplayer
.rp	image/vnd.rn-realpix	.rpm	audio/x-pn-realaudio-plugin
.rsml	application/vnd.rn-rsml	.rt	text/vnd.rn-realtext
.rtf	application/msword	.rtf	application/x-rtf
.rv	video/vnd.rn-realvideo	.sam	application/x-sam

文件扩展名	Content-Type	文件扩展名	Content-Type
.sat	application/x-sat	.sdp	application/sdp
.sdw	application/x-sdw	.sit	application/x-stuffit
.slb	application/x-slb	.sld	application/x-sld
.slk	drawing/x-slk	.smi	application/smil
.smil	application/smil	.smk	application/x-smk
.snd	audio/basic	.sol	text/plain
.sor	text/plain	.spc	application/x-pkcs7-certificates
.spl	application/futuresplash	.spp	text/xml
.ssm	application/streamingmedia	.sst	application/vnd.ms-pki.certstore
.stl	application/vnd.ms-pki.stl	.stm	text/html
.sty	application/x-sty	.svg	text/xml
.swf	application/x-shockwave-flash	.tdf	application/x-tdf
.tg4	application/x-tg4	.tga	application/x-tga
.tif	image/tiff	.tif	application/x-tif
.tiff	image/tiff	.tld	text/xml
.top	drawing/x-top	.torrent	application/x-bittorrent
.tsd	text/xml	.txt	text/plain
.uin	application/x-icq	.uls	text/iuls
.vcf	text/x-vcard	.vda	application/x-vda
.vdx	application/vnd.visio	.vml	text/xml
.vpg	application/x-vpeg005	.vsd	application/vnd.visio
.vsd	application/x-vsd	.vss	application/vnd.visio
.vst	application/vnd.visio	.vst	application/x-vst

文件扩展名	Content-Type	文件扩展名	Content-Type
.vsw	application/vnd.visio	.vsx	application/vnd.visio
.vtx	application/vnd.visio	.vxml	text/xml
.wav	audio/wav	.wax	audio/x-ms-wax
.wb1	application/x-wb1	.wb2	application/x-wb2
.wb3	application/x-wb3	.wbmp	image/vnd.wap.wbmp
.wiz	application/msword	.wk3	application/x-wk3
.wk4	application/x-wk4	.wkq	application/x-wkq
.wks	application/x-wks	.wm	video/x-ms-wm
.wma	audio/x-ms-wma	.wmd	application/x-ms-wmd
.wmf	application/x-wmf	.wml	text/vnd.wap.wml
.wmv	video/x-ms-wmv	.wmx	video/x-ms-wmx
.wmz	application/x-ms-wmz	.wp6	application/x-wp6
.wpd	application/x-wpd	.wpg	application/x-wpg
.wpl	application/vnd.ms-wpl	.wq1	application/x-wq1
.wr1	application/x-wr1	.wri	application/x-wri
.wrk	application/x-wrk	.ws	application/x-ws
.ws2	application/x-ws	.wsc	text/scriptlet
.wsdl	text/xml	.wvx	video/x-ms-wvx
.xdp	application/vnd.adobe.xdp	.xdr	text/xml
.xfd	application/vnd.adobe.xfd	.xfdf	application/vnd.adobe.xfdf
.xhtml	text/html	.xls	application/vnd.ms-excel
.xls	application/x-xls	.xlw	application/x-xlw
.xml	text/xml	.xpl	audio/scpls
.xq	text/xml	.xql	text/xml

文件扩展名	Content-Type	文件扩展名	Content-Type
.xquery	text/xml	.xsd	text/xml
.xsl	text/xml	.xslt	text/xml
.xwd	application/x-xwd	.x_b	application/x-x_b
.sis	application/vnd.symbian.install	.sisx	application/vnd.symbian.install
.x_t	application/x-x_t	.ipa	application/vnd.iphone
.apk	application/vnd.android.package-archive	.xap	application/x-silverlight-app

3.6.3 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“对象”页面。

步骤2 单击待操作的对象，然后再单击“元数据”。

步骤3 单击“增加”。根据需要填写元数据信息。

步骤4 单击“确定”。

----结束

3.7 桶清单

3.7.1 桶清单简介

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

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

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

约束与限制

- 一个桶最多支持10条桶清单。
- 桶清单配置的源桶和目标桶必须归属同一个账号。

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

3.7.2 配置桶清单

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“对象”页面。

步骤2 在左侧导航栏，单击“桶清单”进入“桶清单”页面。

步骤3 单击“创建”，系统弹出“创建桶清单”对话框。

步骤4 设置“清单配置”相关参数。

表 3-9 清单配置参数说明

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

步骤5 单击“下一步”，进入“报表配置”页面。

步骤6 设置“报表格式”相关参数。

表 3-10 报表格式参数说明

参数	描述
清单格式	支持生成CSV格式的桶清单文件。
对象版本	报表中对象的版本，可以设置为“仅限当前版本”和“包含所有版本”。
清单额外字段	桶清单文件中包含的对象信息：文件大小、上次修改时间、ETag、分段上传、复制状态。
发送通知	当有新的清单生成时发送消息通知，消息将发送到SMN主题中指定的邮箱或手机等终端。 开启发送通知，会同步在清单存储桶中创建SMN事件通知规则，所创建规则的详细信息可以在清单存储桶的事件通知页面查看。关闭发送通知或修改通知的SMN主题，也会同步删除或修改已创建的SMN事件通知规则。

步骤7 单击“下一步”，确认桶策略。

OBS将在桶清单存储桶上创建桶策略，以允许其将清单文件存入该桶。

步骤8 单击“确定”。

----结束

相关操作

桶清单列表页支持导出桶清单操作。

步骤1 在OBS管理控制台桶列表中，单击待操作的桶，进入“对象”页面。

步骤2 在左侧导航栏，单击“桶清单”，进入桶清单列表页面。

步骤3 单击右上角的  。

步骤4 浏览器会自动下载桶清单Excel表，包含“清单名称、清单状态、筛选条件、清单存储桶、清单文件前缀、生成频率和上次生成时间”信息。

----结束

3.8 权限控制

3.8.1 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。

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。

3.8.2 权限控制方式介绍

3.8.2.1 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

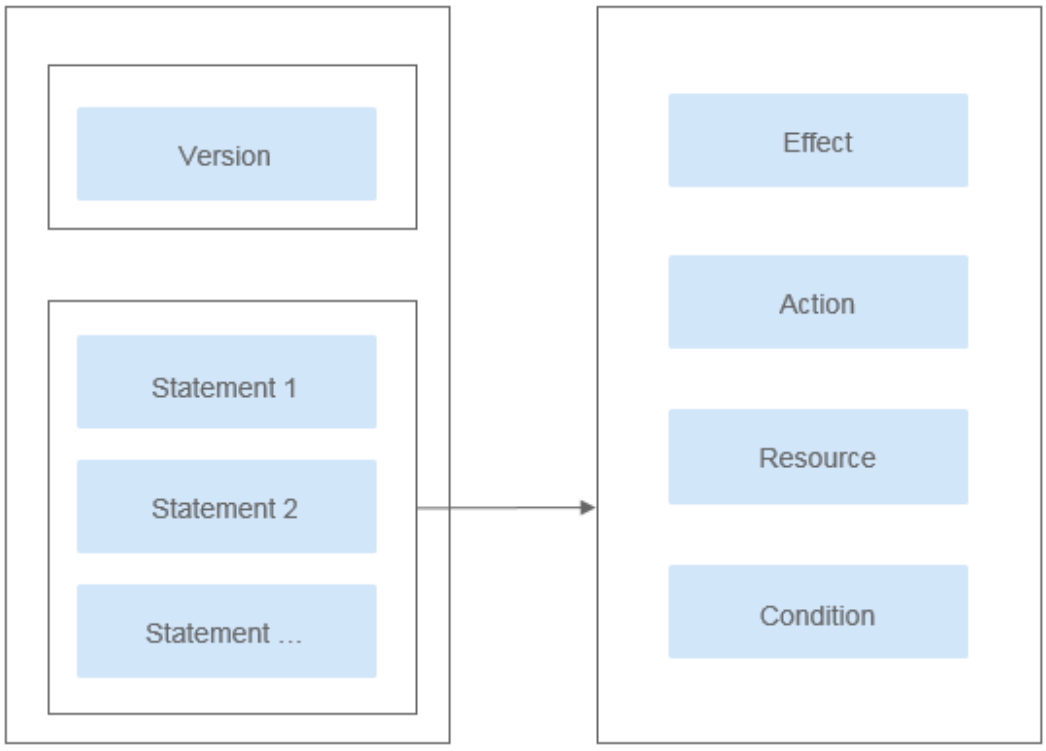
IAM策略主要面向对同账号下IAM用户授权的场景：

- 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 3-3 策略结构



```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "obs:bucket:ListAllMybuckets",
                "obs:bucket:HeadBucket",
                "obs:bucket:ListBucket",
                "obs:bucket:GetBucketLocation"
            ]
        }
    ]
}
```

表 3-11 策略语法参数

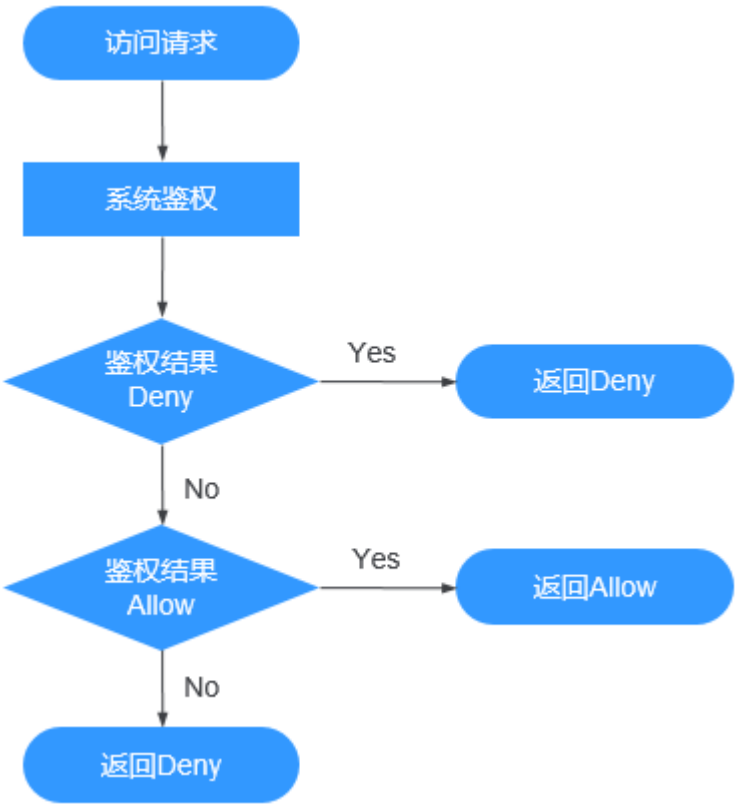
参数	说明
Version	标识策略的版本号： ● 1.0：RBAC策略。RBAC策略是将服务作为一个整体进行授权，授权后，用户可以拥有这个服务的所有权限。 ● 1.1：细粒度策略。相比RBAC策略，细粒度策略基于服务的API接口进行权限拆分，授权更加精细，可以精确到具体操作和具体资源。例如：您可以限制子用户只能访问某一个OBS桶中某一个目录下的对象。

参数	说明
Statement	策略授权语句，描述策略的详细信息，包含Effect（作用）、Action（授权项）、Resource（资源）和Condition（条件）。其中Condition为可选。 ● 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，自定义策略中可以同时包含允许和拒绝的授权语句，当策略中既有允许又有拒绝的授权语句时，遵循Deny优先的原则。 ● Action（授权项） 对资源的具体操作权限，格式为：**服务名:资源类型:操作**，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。OBS只有两种资源类型：bucket和object。 详细的Action描述请参见《对象存储服务接口参考》的“IAM权限策略和授权项 > 桶相关授权项”和“IAM权限策略和授权项 > 对象相关授权项”章节。 ● Resource（资源） 策略所作用的资源，格式为：**服务名:region:domainId:资源类型:资源路径**，支持通配符号*，通配符号表示所有。在JSON视图中，不带Resource表示对所有资源生效。 Resource支持以下字符：-_0-9a-zA-Z*./\，如果Resource中包含不支持的字符，请采用通配符号*。 OBS是全局级服务，**region**填“*”；domainId表示资源拥有者的账号ID，建议填写“*”简单地表示所填资源的账号ID。 示例： – "obs:*:*:bucket:*": 表示所有的OBS桶。 – "obs:*:*:object:my-bucket/my-object/*": 表示桶my-bucket中“my-object”目录下的所有对象。 ● Condition（条件） 使策略生效的特定条件，可选。格式为：**条件运算符: {条件名:[条件值1, 条件值2]}** 条件包含全局条件名和云服务条件名，OBS支持的条件名与桶策略中的Condition一致，在IAM配置时，需要加上“obs:”。详细的Condition介绍如**授权条件**所示。 Condition的条件值仅支持以下字符：-,./ a-zA-Z0-9_@#$ %&，如果条件值中包含不支持的字符，请考虑使用模糊匹配的条件运算符，如：StringLike，StringStartWith等。 示例： – "StringEndWithIfExists":{"g:UserName":["specialCharacter"]}：表示当用户输入的用户名以"specialCharacter"结尾时该条statement生效。 – "StringLike":{"obs:prefix":["private/"]}：表示在列举桶内对象时，需要指定prefix为private/或者包含private/这一子字符串。

IAM 策略鉴权

IAM策略遵循Deny优先的原则。在用户访问资源时，权限检查逻辑如下：

图 3-4 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。

3.8.2.2 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。

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。

桶策略模板：

OBS控制台预置了八种常用典型场景的桶策略模板，用户可以使用模板创建桶策略，快速完成桶策略配置。

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

表 3-12 桶策略模板

被授权用户	授权资源	模板名称	模板动作	高级设置
所有账号	整个桶（包括桶内对象）	公共读	**允许所有账号（所有互联网用户）对整个桶及桶内所有对象执行以下动作：** HeadBucket（判断桶是否存在、获取桶元数据） GetBucketLocation（获取桶位置） GetObject（获取对象内容、获取对象元数据） GetObjectVersion（获取指定版本对象内容、获取指定版本对象元数据）	不支持排除以上授权操作

被授权用户	授权资源	模板名称	模板动作	高级设置
		公共读写	**允许所有账号（所有互联网用户）对整个桶及桶内所有对象执行以下动作：** ListBucket（列举桶内对象、获取桶元数据） ListBucketVersions（列举桶内多版本对象） HeadBucket（判断桶是否存在、获取桶元数据） GetBucketLocation（获取桶位置） PutObject（PUT上传，POST上传，上传段，初始化上传段任务，合并段） GetObject（获取对象内容、获取对象元数据） ModifyObjectMetaData（修改对象元数据） ListBucketMultipartUploads（列举多段上传任务） ListMultipartUploadParts（列举已上传段） AbortMultipartUpload（取消多段上传任务） GetObjectVersion（获取指定版本对象内容、获取指定版本对象元数据） PutObjectAcl（设置对象ACL） GetObjectVersionAcl（获取指定版本对象ACL） GetObjectAcl（获取对象ACL）	不支持排除以上授权操作
当前账号/其他账号/委托账号	整个桶（包括桶内对象）	桶只读	**允许指定账号对整个桶及桶内所有对象执行以下动作：** Get*（所有获取操作） List*（所有列举操作） HeadBucket（判断桶是否存在、获取桶元数据）	不支持排除以上授权操作
		桶读写	**允许指定账号对整个桶及桶内所有对象执行除以下动作以外的所有动作：** DeleteBucket（删除桶） PutBucketPolicy（设置桶策略） PutBucketAcl（设置桶ACL）	排除以上授权操作

被授权用户	授权资源	模板名称	模板动作	高级设置
所有账号/当前账号/其他账号/委托账号	当前桶+指定对象	目录只读	**允许所有账号（所有互联网用户）或指定账号对当前桶和桶内指定资源执行以下动作：** GetObject（获取对象内容、获取对象元数据） GetObjectVersion（获取指定版本对象内容、获取指定版本对象元数据） GetObjectVersionAcl（获取指定版本对象ACL） GetObjectAcl（获取对象ACL） ListBucket（列举桶内对象、获取桶元数据） ListBucketVersions（列举桶内多版本对象） HeadBucket（判断桶是否存在、获取桶元数据） GetBucketLocation（获取桶位置） **说明** 被授权用户选择“所有账号”时，模板动作中不包含ListBucket、ListBucketVersions。	不支持排除以上授权操作

被授权用户	授权资源	模板名称	模板动作	高级设置
		目录读写	**允许所有账号（所有互联网用户）或指定账号对当前桶和桶内指定资源执行以下动作：** PutObject（PUT上传，POST上传，上传段，初始化上传段任务，合并段） GetObject（获取对象内容、获取对象元数据） GetObjectVersion（获取指定版本对象内容、获取指定版本对象元数据） ModifyObjectMetaData（修改对象元数据） ListBucketMultipartUploads（列举多段上传任务） ListMultipartUploadParts（列举已上传段） AbortMultipartUpload（取消多段上传任务） GetObjectVersionAcl（获取指定版本对象ACL） GetObjectAcl（获取对象ACL） PutObjectAcl（设置对象ACL） ListBucket（列举桶内对象、获取桶元数据） ListBucketVersions（列举桶内多版本对象） HeadBucket（判断桶是否存在、获取桶元数据） GetBucketLocation（获取桶位置）	不支持排除以上授权操作

被授权用户	授权资源	模板名称	模板动作	高级设置
所有账号/当前账号/其他账号/委托账号	指定对象	对象只读	**允许所有账号（所有互联网用户）或指定账号对桶内指定资源执行以下动作：** GetObject（获取对象内容、获取对象元数据） GetObjectVersion（获取指定版本对象内容、获取指定版本对象元数据） GetObjectVersionAcl（获取指定版本对象ACL） GetObjectAcl（获取对象ACL）	不支持排除以上授权操作
		对象读写	**允许所有账号（所有互联网用户）或指定账号对桶内指定资源执行以下动作：** PutObject（PUT上传，POST上传，上传段，初始化上传段任务，合并段） GetObject（获取对象内容、获取对象元数据） GetObjectVersion（获取指定版本对象内容、获取指定版本对象元数据） ModifyObjectMetaData（修改对象元数据） ListMultipartUploadParts（列举已上传段） AbortMultipartUpload（取消多段上传任务） GetObjectVersionAcl GetObjectAcl（获取对象ACL） PutObjectAcl（设置对象ACL）	不支持排除以上授权操作

自定义桶策略：

您也可以根据实际业务场景的定制化需求，不使用预置桶策略模板，自定义创建桶策略。自定义桶策略由效力、被授权用户、授权资源、授权操作和授权条件5个桶策略基本元素共同决定。详细请参见**桶策略参数说明**。

对象策略

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

对象策略模板：

OBS控制台预置了两种常用典型场景的对象策略模板，用户可以使用模板创建对象策略，快速完成对象策略配置。

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

表 3-13 对象策略模板

被授权用户	授权资源	模板名称	模板动作	高级设置
所有账号/当前账号/其他账号/委托账号	指定对象	对象只读	**允许所有账号（所有互联网用户）或指定账号对桶内指定资源执行以下动作：** GetObject（获取对象内容、获取对象元数据） GetObjectVersion（获取指定版本对象内容、获取指定版本对象元数据） GetObjectVersionAcl（获取指定版本对象ACL） GetObjectAcl（获取对象ACL）	不支持排除以上授权操作
		对象读写	**允许所有账号（所有互联网用户）或指定账号对桶内指定资源执行以下动作：** PutObject（PUT上传，POST上传，上传段，初始化上传段任务，合并段） GetObject（获取对象内容、获取对象元数据） GetObjectVersion（获取指定版本对象内容、获取指定版本对象元数据） ModifyObjectMetaData（修改对象元数据） ListMultipartUploadParts（列举已上传段） AbortMultipartUpload（取消多段上传任务） GetObjectVersionAcl（获取指定版本对象ACL） GetObjectAcl（获取对象ACL） PutObjectAcl（设置对象ACL）	不支持排除以上授权操作

自定义对象策略：

您也可以根据实际业务场景的定制化需求，不使用预置对象策略模板，自定义创建对象策略。自定义对象策略由效力、被授权用户、授权资源、授权操作和授权条件5个桶

策略基本元素共同决定，与桶策略类似，详细请参见**桶策略参数说明**。其中授权资源为已选择的对象，系统自动配置。

3.8.2.3 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3-14**所示。

表 3-14 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	如果匿名用户被授予了访问桶/对象的权限，则表示所有人都可以访问对应的桶/对象，并且不需要经过任何身份认证。
日志投递用户组 **说明** 仅桶ACL支持。	日志投递用户组用于投递OBS桶及对象的访问日志。由于OBS本身不能在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3-15所示：

表 3-15 桶 ACL 访问权限

权限	选项	描述
桶访问权限	读取权限 READ	此权限可以获取桶内对象列表、桶内多段任务、桶的元数据、桶的多版本设置和桶内多版本对象列表。
	写入权限 WRITE	此权限可以上传、覆盖和删除该桶内任何对象。
对象权限	对象读权限READ	此权限可以获取该桶内对象的内容和对象的元数据。
ACL访问权限	读取权限 READ_ACP	此权限可以获取对应的桶及桶内对象的权限控制列表。 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3-16所示：

表 3-16 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3-17所示。

表 3-17 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。
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。

3.8.2.4 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3-18**所示。

表 3-18 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
对象权限	对象读权限	• GetObject
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3-19**所示。

表 3-19 对象 ACL 和桶策略的映射关系

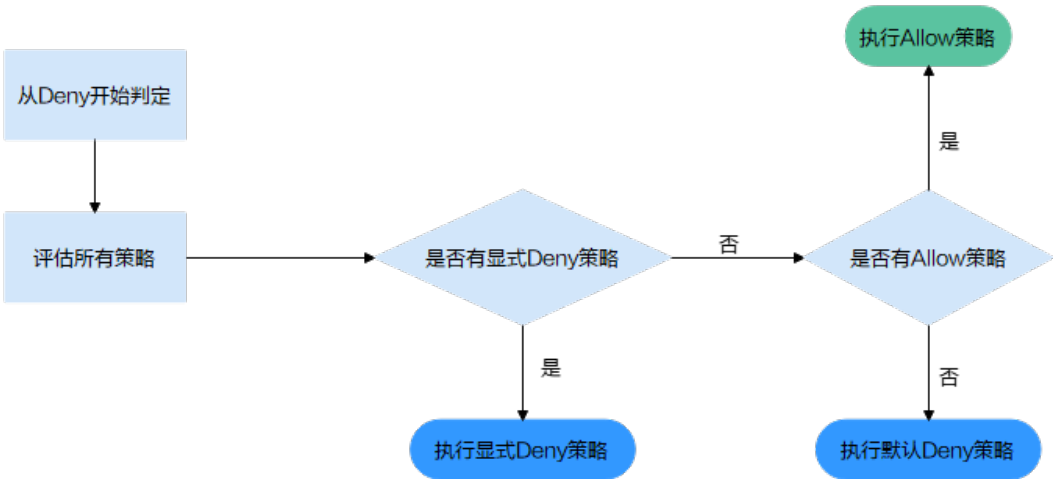
对象ACL权限	选项	对应桶策略高级设置中的动作
对象访问权限	读取权限	• GetObject • GetObjectVersion
ACL访问权限	读取权限	• GetObjectAcl • GetObjectVersionAcl
	写入权限	• PutObjectAcl • PutObjectVersionAcl

3.8.2.5 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 3-5 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3-6所示。

图 3-6 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

3.8.3 桶策略参数说明

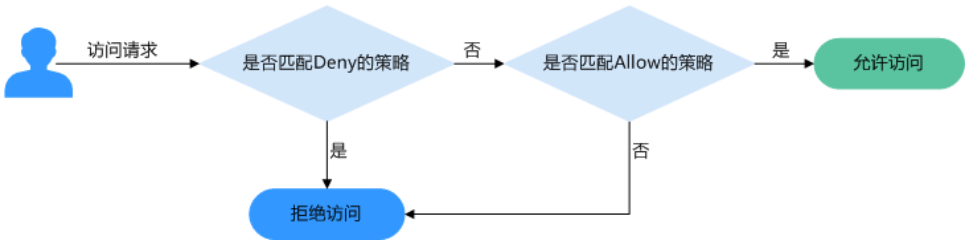
3.8.3.1 效力

桶策略的效力，具体表现为允许或拒绝请求。

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

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

图 3-7 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力设置为拒绝（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。

3.8.3.2 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排除策略来指定：

（可选项）排除以上被授权用户：桶策略对除指定用户外的其他用户生效。

说明

- 不勾选：表示桶策略对指定的用户生效。
- 勾选：表示桶策略对除指定用户外的其他用户生效。

3.8.3.3 授权资源

在指定授权资源时，授权资源可以是整个桶（包含桶内对象）、当前桶、指定对象。

授权资源可以通过排除策略来指定：

（可选项）排除以上授权资源：桶策略对除指定资源外的其他资源生效。

说明

- 不勾选：表示桶策略对指定的OBS资源生效。
- 勾选：表示桶策略对除设置外的其他OBS资源生效。

指定授权资源为整个桶（包含桶内对象）

指定资源为整个桶（包含桶内对象）时，桶策略动作需配置为桶和对象相关的动作，配置方法为“资源范围”选择“整个桶（包含桶内对象）”。

指定授权资源为桶

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

指定授权资源为对象

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，配置方法为“资源范围”选择“指定对象”，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

3.8.3.4 授权操作

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。

桶策略授权授权操作可以通过排除策略来指定：

（可选项）排除以上授权操作：桶策略对除指定动作外的其他动作生效。

说明

- 不勾选：表示桶策略对指定的动作生效。
- 勾选：表示桶策略对除指定动作外的其他动作生效。
- 对于桶策略模板，“桶读写”模板默认勾选，其他模板默认不勾选。桶策略模板中的动作排除策略不支持修改。

与桶相关的动作

表 3-20 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。

类型	值	描述
	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。
	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 3-21 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。

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

3.8.3.5 授权条件

除了指定效力、被授权用户、授权资源、授权操作外，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3-22**所示的预定义条件运算符。

表 3-22 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。
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 3-23 通用键

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

表 3-24 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。	

Action	可选键	描述	说明
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 3-25 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。

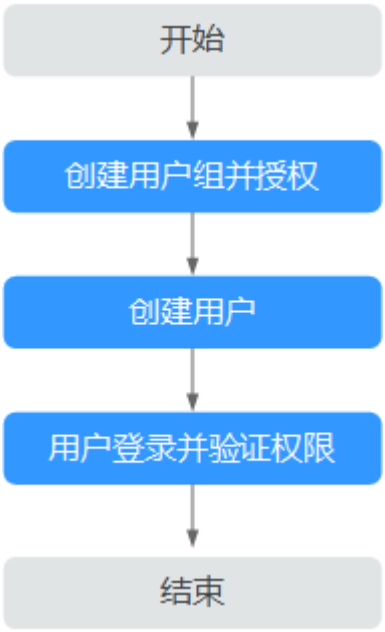
Action	可选键	描述
DeleteObjectVersion	VersionId	String类型，删除VersionId为xxx版本的对象。

3.8.4 配置 IAM 策略

3.8.4.1 创建 IAM 用户并授权使用 OBS

示例流程

图 3-8 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“授权”。
5. 在“选择决策”步骤中，可以根据需求在右上方进行筛选策略，选中策略名称，单击“下一步”。
6. 在“设置最小授权范围”步骤中，选择“全局服务资源”，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。

由于缓存的存在，对用户、用户组授予OBS相关的RBAC策略和细粒度策略后，大概需要等待10~15分钟策略才能生效。

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

3.8.4.2 配置细粒度策略

如果系统预置的OBS权限，不满足您的授权要求，可以创建自定义策略。

操作步骤

步骤1 登录统一身份认证服务管理控制台。

步骤2 在左侧导航栏单击“策略”，进入“策略”界面。

步骤3 单击“创建自定义策略”。

步骤4 在“创建自定义策略”中，填写如下参数：

表 3-26 自定义策略参数

参数	说明
策略名称	只能包含如下字符：大小写字母、中文、数字、空格和特殊字符（-_,）。
作用范围	根据服务的属性填写。OBS为全局服务。
策略描述	可选，对策略的描述。
策略信息	可选择模板后，自定义编辑策略授权的内容。 详见**策略结构&语法**。

说明

一个自定义策略中可以包含多个授权项，且除了可以包含本服务的授权项外，还可以包含其他服务的授权项，可以包含的其他服务必须跟本服务同属性，即都是项目级服务或都是全局级服务。

步骤5 单击“确定”完成细粒度策略配置。

步骤6 将细粒度策略授权给用户组，配置用户加入用户组，以获取细粒度策略授权的权限，请参考**创建IAM用户并授权使用OBS**完成。

----结束

3.8.5 配置桶策略

3.8.5.1 使用模板创建桶策略

OBS控制台预置了八种常用典型场景的桶策略模板，用户可以使用模板创建桶策略，快速完成桶策略配置。

操作步骤

步骤1 在OBS管理控制台桶列表中，单击待操作的桶，进入“对象”页面。

步骤2 在左侧导航栏，单击“访问权限控制 > 桶策略”。

步骤3 单击“创建”。

步骤4 选择桶策略模板。详细参数说明请参见**桶策略和对象策略**。

表 3-27 桶策略模板

被授权用户	授权资源	模板名称	模板动作	高级设置
所有账号	整个桶（包括桶内对象）	公共读	**允许所有账号（所有互联网用户）对整个桶及桶内所有对象执行以下动作：** GetBucketLocation（获取桶位置） GetObject（获取对象内容、获取对象元数据） GetObjectVersion（获取指定版本对象内容、获取指定版本对象元数据）	不支持排除以上授权操作

被授权用户	授权资源	模板名称	模板动作	高级设置
		公共读写	**允许所有账号（所有互联网用户）对整个桶及桶内所有对象执行以下动作：** ListBucket（列举桶内对象、获取桶元数据） ListBucketVersions（列举桶内多版本对象） GetBucketLocation（获取桶位置） PutObject（PUT上传，POST上传，上传段，初始化上传段任务，合并段） GetObject（获取对象内容、获取对象元数据） ModifyObjectMetaData（修改对象元数据） ListBucketMultipartUploads（列举多段上传任务） ListMultipartUploadParts（列举已上传段） AbortMultipartUpload（取消多段上传任务） GetObjectVersion（获取指定版本对象内容、获取指定版本对象元数据） PutObjectAcl（设置对象ACL） GetObjectVersionAcl（获取指定版本对象ACL） GetObjectAcl（获取对象ACL）	不支持排除以上授权操作
当前账号/其他账号/委托账号	整个桶（包括桶内对象）	桶只读	**允许指定账号对整个桶及桶内所有对象执行以下动作：** Get*（所有获取操作） List*（所有列举操作）	不支持排除以上授权操作
		桶读写	**允许指定账号对整个桶及桶内所有对象执行除以下动作以外的所有动作：** DeleteBucket（删除桶） PutBucketPolicy（设置桶策略） PutBucketAcl（设置桶ACL）	排除以上授权操作

被授权用户	授权资源	模板名称	模板动作	高级设置
所有账号/当前账号/其他账号/委托账号	当前桶+指定对象	目录只读	**允许所有账号（所有互联网用户）或指定账号对当前桶和桶内指定资源执行以下动作：** GetObject（获取对象内容、获取对象元数据） GetObjectVersion（获取指定版本对象内容、获取指定版本对象元数据） GetObjectVersionAcl（获取指定版本对象ACL） GetObjectAcl（获取对象ACL） ListBucket（列举桶内对象、获取桶元数据） ListBucketVersions（列举桶内多版本对象） GetBucketLocation（获取桶位置） **说明** 被授权用户选择“所有账号”时，模板动作中不包含ListBucket、ListBucketVersions。	不支持排除以上授权操作

被授权用户	授权资源	模板名称	模板动作	高级设置
		目录读写	**允许所有账号（所有互联网用户）或指定账号对当前桶和桶内指定资源执行以下动作：** PutObject（PUT上传，POST上传，上传段，初始化上传段任务，合并段） GetObject（获取对象内容、获取对象元数据） GetObjectVersion（获取指定版本对象内容、获取指定版本对象元数据） ModifyObjectMetaData（修改对象元数据） ListBucketMultipartUploads（列举多段上传任务） ListMultipartUploadParts（列举已上传段） AbortMultipartUpload（取消多段上传任务） GetObjectVersionAcl（获取指定版本对象ACL） GetObjectAcl（获取对象ACL） PutObjectAcl（设置对象ACL） ListBucket（列举桶内对象、获取桶元数据） ListBucketVersions（列举桶内多版本对象） GetBucketLocation（获取桶位置）	不支持排除以上授权操作
所有账号/当前账号/其他账号/委托账号	指定对象	对象只读	**允许所有账号（所有互联网用户）或指定账号对桶内指定资源执行以下动作：** GetObject（获取对象内容、获取对象元数据） GetObjectVersion（获取指定版本对象内容、获取指定版本对象元数据） GetObjectVersionAcl（获取指定版本对象ACL） GetObjectAcl（获取对象ACL）	不支持排除以上授权操作

被授权用户	授权资源	模板名称	模板动作	高级设置
		对象读写	**允许所有账号（所有互联网用户）或指定账号对桶内指定资源执行以下动作：** PutObject（PUT上传，POST上传，上传段，初始化上传段任务，合并段） GetObject（获取对象内容、获取对象元数据） GetObjectVersion（获取指定版本对象内容、获取指定版本对象元数据） ModifyObjectMetaData（修改对象元数据） ListMultipartUploadParts（列举已上传段） AbortMultipartUpload（取消多段上传任务） GetObjectVersionAcl GetObjectAcl（获取对象ACL） PutObjectAcl（设置对象ACL）	不支持排除以上授权操作

步骤5 完善桶策略配置信息。

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

步骤6 单击界面右下角的“创建”，完成桶策略创建。

----结束

3.8.5.2 自定义创建桶策略（可视化视图）

您可以根据实际业务场景的定制化需求，不使用预置桶策略模板，自定义创建桶策略。自定义桶策略由效力、被授权用户、资源、动作和条件5个桶策略基本元素共同决定。

操作步骤

步骤1 在OBS管理控制台桶列表中，单击待操作的桶，进入“对象”页面。

步骤2 在左侧导航栏，单击“访问权限控制 > 桶策略”。

步骤3 单击“创建”。

步骤4 配置桶策略。

表 3-28 自定义桶策略参数配置说明

参数		说明
策略配置方式		支持可视化视图和JSON视图。此处以可视化视图为例，JSON视图的说明请参见**自定义创建桶策略（JSON视图）**。
策略名称		输入自定义桶策略的名称。
策略内容	效力	• 允许：指定本条桶策略描述的权限为接受请求。 • 拒绝：指定本条桶策略描述的权限为拒绝请求。
	被授权用户	• 所有账号：表示桶策略授权给互联网上的所有人。 • 当前账号：可以选择当前账号下的一个或多个IAM子用户。 • 其他账号：可以设置一个或多个其他账号。 **说明** 账号ID和IAM子用户ID可在“我的凭证”页面获取。 输入格式：domainId/userId，可授权给多个账号，每行一个。 domainId/*表示授权给账号下的所有用户。 • 委托账号：勾选“其他账号”后才可添加委托账号，可以设置一个或多个委托账号。 **说明** 输入格式：domainId/agencyname，domainId为委托方账号ID，可授权给多个委托，每行一个。
	授权资源	• 整个桶（包括桶内对象）：表示整个桶及桶内所有对象，可以在动作中配置桶和对象相关动作。 • 当前桶：表示当前桶，可以在动作中配置桶相关动作。 • 指定对象：表示桶内指定对象，可以在动作中配置对象相关动作。 **说明** 1. 指定对象支持输入多个资源路径。 2. 资源路径输入格式：文件夹/对象名，例如“testdir/a.txt”。如果你想要指定文件夹及文件夹下所有对象，可以输入“testdir/*”。 3. 您可以指定资源路径为具体对象、对象集或目录，*表示桶内所有对象。 如果指定某个对象：请输入对象名称。 如果指定某个对象集：请输入“对象名称前缀”+“*”、“*”+“对象名后缀”或“*”。例如，”testdir/*”为指定testdir文件夹下的对象，“testprefix*”为指定前缀为testprefix的对象。

参数		说明
	授权操作	• 动作范围：自定义配置 • 选择动作：详细的动作信息请参见**授权操作**。 **说明** 1. 如果“授权资源”仅选择“整个桶（包括桶内对象）”，可选择配置“通用动作”、“桶动作”和“对象动作”。 2. 如果“授权资源”仅选择“当前桶”，可选择配置“通用动作”和“桶动作”。 3. 如果“授权资源”仅选择“指定对象”，可选择配置“通用动作”和“对象动作”。 4. 如果“授权资源”同时选择“当前桶”和“指定对象”，可选择配置“通用动作”、“桶动作”和“对象动作”。
	授权条件（可选）	• 键：请参见**授权条件**。 • 条件运算符：请参见**授权条件**。 • 值：输入的值与键相关。
	高级设置-排除策略（可选）	• 排除以上被授权用户：桶策略对除指定用户外的其他用户生效。 **说明** 1. 不勾选：表示桶策略对指定的用户生效。 2. 勾选：表示桶策略对除指定用户外的其他用户生效。 • 排除以上授权资源：桶策略对除指定资源外的其他资源生效。 **说明** 1. 不勾选：表示桶策略对指定的OBS资源生效。 2. 勾选：表示桶策略对除设置外的其他OBS资源生效。 • 排除以上授权操作：桶策略对除指定动作外的其他动作生效。 **说明** 1. 不勾选：表示桶策略对指定的动作生效。 2. 勾选：表示桶策略对除指定动作外的其他动作生效。 3. 对于桶策略模板，“桶读写”模板默认勾选，其他模板默认不勾选。桶策略模板中的动作排除策略不支持修改。

步骤5 单击界面右下角的“创建”，完成桶策略创建。

----结束

3.8.5.3 自定义创建桶策略（JSON 视图）

熟悉JSON以及OBS桶策略语法结构的用户，可以直接使用JSON视图编辑桶策略。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。

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“对象”页面。

步骤2 在左侧导航栏，单击“访问权限控制 > 桶策略”。

步骤3 单击“创建”，选择“JSON视图”页签。

步骤4 编辑桶策略。桶策略JSON格式如下：

```
{
  "Statement":[
    {
      "Action":[
        "CreateBucket",
        "DeleteBucket"
      ],
      "Effect":"Allow",
      "Principal":{
        "ID":[
          "domain/account ID",
          "domain/account ID:user/User ID"
        ]
      },
      "Condition":{
        "NumericNotEquals":{
          "Referer":"sdf"
        },
        "StringNotLike":{
          "Delimiter":"ouio"
        }
      },
      "Resource":"000-02/key01"
    }
  ]
}
```

表 3-29 参数说明

参数	描述
Action	桶策略授权操作，详见**授权操作**。
Effect	桶策略效力，详见**效力**。
Principal	桶策略被授权用户，ID可以通过控制台在“我的凭证”页面获取。Principal格式： ● “domain/账号ID”（表示被授权用户为xxx账号）。 ● “domain/账号ID:user/用户ID”（表示被授权用户为xxx账号下的xxx用户）。
Condition	桶策略授权条件，详见**授权条件**。
Resource	桶策略作用的资源，详见**授权资源**。

步骤5 单击“创建”。

----结束

3.8.6 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“对象”页面。

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

支持使用模板创建和自定义创建两种方式，您可以根据需要进行选择。

- 使用模板创建：系统预置了两种常用典型场景的对象策略模板，您可以使用模板快速完成对象策略配置。
- 自定义创建：您也可以根据实际业务场景的定制化需求，不使用预置对象策略模板，自定义创建对象策略。自定义对象策略由效力、被授权用户、资源、动作和条件5个桶策略基本元素共同决定，与桶策略类似，详细请参见**桶策略参数说明**。其中资源为已选择的对象，系统自动配置。自定义创建的方法，可参见**自定义创建桶策略（可视化视图）**，与自定义桶策略相比有如下两点区别：
  a. 资源不需要指定，系统默认指定为已选择对象。
  b. 配置的动作仅支持对象相关动作。

----结束

3.8.7 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“对象”页面。

步骤2 在左侧导航栏，单击“访问权限控制 > 桶ACLs”。

步骤3 在“桶ACLs”中，支持切换公共权限（私有/公共读/公共读写），快速配置匿名用户的桶ACL访问权限。

说明

1. 公共读/公共读写权限切换私有权限，切换后除桶或对象的所有者外，其余用户无访问权限。
2. 私有权限切换公共读权限，可以使任何用户在不用身份认证的情况下直接读取桶内的对象，请谨慎操作。
3. 私有权限切换公共读写权限，可以使任何用户在不用身份认证的情况下直接读/写/删桶内的对象，请谨慎操作。

步骤4 单击用户类型操作列的“编辑”可按照需求通过勾选相应权限对拥有者、匿名用户以及日志投递用户组赋予目标桶的ACL权限。

步骤5 单击页面中部的“导出”，可导出桶ACLs权限信息，包含用户类型、账号、桶访问权限和ACL访问权限。

步骤6 单击页面中部的“增加”，可对特定账号添加ACL权限。

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

单击“确定”。

说明

勾选“桶访问权限>读取权限”，才支持勾选“对象权限>对象读权限”。

----结束

3.8.8 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“对象”页面。

步骤2 单击待操作的对象。

步骤3 在“对象ACL”中，支持切换公共权限（私有/公共读），快速配置匿名用户的对象ACL访问权限。

说明

1. 公共读权限切换私有权限，切换后除桶或对象的所有者外，其余用户无访问权限。
2. 私有权限切换公共读权限，任何用户在不经过身份认证的情况下可直接读对象的内容、对象的元数据，请谨慎操作。

步骤4 单击“编辑”可按照需求通过勾选相应权限对拥有者、匿名用户以及其他账号赋予目标对象的ACL权限。

步骤5 单击“导出”，可导出对象ACLs权限信息，包含用户类型、账号、对象访问权限和ACL访问权限。

步骤6 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”，并为其设定相应的ACL权限。“账号ID”可通过“我的凭证”页面查看。

单击“确定”。

----结束

3.8.9 应用示例

3.8.9.1 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“对象”页面。

步骤2 在左侧导航栏，单击“访问权限控制 > 桶策略”。

步骤3 单击“创建”。

步骤4 配置如下参数，授予IAM用户访问桶（列举对象）和上传对象的权限。

表 3-30 授予访问桶和上传对象的权限参数配置

参数		说明
策略配置方式		可视化视图
策略名称		自定义
策略内容	效力	允许
	被授权用户	• 被授权用户：当前账号 • 子账号：选择需要授权的IAM用户
	授权资源	• 方式一： – 资源范围：整个桶（包括桶内对象） • 方式二： – 资源范围：当前桶、指定对象 – 指定对象 - 资源路径：*（*表示桶内所有对象）
	授权操作	• 动作范围：自定义配置 • 选择动作： – ListBucket（列举桶内对象，获取桶元数据） – PutObject（上传对象） **说明** 本例对象动作仅授予上传对象权限。可以根据业务需要选择多个动作，同时授予其他操作权限。“*”代表所有操作。 支持的动作及含义请参见**授权操作**。

步骤5 单击右下角的“创建”，完成桶策略创建。

----结束

3.8.9.2 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“对象”页面。

步骤2 在左侧导航栏，单击“访问权限控制 > 桶策略”。

步骤3 单击“创建”。

步骤4 配置如下参数，授予其他账号访问桶（列举对象）和上传对象的权限。

表 3-31 授予访问桶和上传对象的权限参数配置

参数		说明
策略配置方式		可视化视图
策略名称		自定义
策略内容	效力	允许
	被授权用户	• 被授权用户：其他账号 **说明** 1. 账号ID和IAM用户ID可在“我的凭证”页面获取。 2. 输入格式：domainId/userId，可授权给多个账号，每行一个。 3. 不同授权场景的设置说明： 授权给所有账号及IAM用户：账号ID和IAM用户ID填写通配符（*）。 仅授权给某个账号：填写被授权账号的账号ID和IAM用户ID。 授权给某个账号及账号下所有IAM用户：账号ID填写被授权账号的账号ID，用户ID填写通配符（*）。 授权给IAM用户：填写被授权IAM用户的账号ID和IAM用户ID。

参数		说明
	授权资源	• 方式一： – 资源范围：整个桶（包括桶内对象） • 方式二： – 资源范围：当前桶、指定对象 – 指定对象 - 资源路径：*（*表示桶内所有对象）
	授权操作	• 动作范围：自定义配置 • 选择动作：ListBucket（列举桶内对象，获取桶元数据）和PutObject（上传对象） **说明** 本例对象动作仅授予上传对象权限。可以根据业务需要选择多个动作，同时授予其他操作权限。“*”代表所有操作。 支持的动作及含义请参见**授权操作**。

步骤5 单击右下角的“创建”，完成桶策略创建。

----结束

3.8.9.3 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“对象”页面。

步骤2 在左侧导航栏，单击“访问权限控制 > 桶策略”。

步骤3 单击“创建”。

步骤4 配置如下参数。

表 3-32 限制特定地址对桶的访问权限

参数		说明
策略配置方式		可视化视图
策略名称		自定义
策略内容	效力	拒绝
	被授权用户	• 被授权用户：所有账号

参数		说明
	授权资源	● 方式一： – 资源范围：整个桶（包括桶内对象） ● 方式二： – 资源范围：当前桶、指定对象 – 指定对象 - 资源路径：*（*表示桶内所有对象）
	授权操作	● 动作范围：自定义配置 ● 选择动作：*（表示所有动作）
	授权条件	● 键：SourceIP ● 条件运算符：IpAddress ● 值：114.115.1.0/24

步骤5 单击右下角的“创建”，完成桶策略创建。

----结束

验证

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

3.8.9.4 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“对象”页面。

步骤2 在左侧导航栏，单击“访问权限控制 > 桶策略”。

步骤3 单击“创建”。

步骤4 配置如下参数。

表 3-33 限制桶中对象的访问起始时间和结束时间

参数		说明
策略配置方式		可视化视图
策略名称		自定义
策略内容	效力	允许
	被授权用户	● 被授权用户：所有账号

参数		说明
	授权资源	● 资源范围：指定对象 ● 资源路径：* **说明** 1. *表示桶内所有对象。 2. 本示例仅配置桶内资源的权限，如果还需要配置桶的权限（如列举桶内对象），则需要再额外创建一条配置到当前桶的自定义桶策略。
	授权操作	● 动作范围：自定义配置 ● 选择动作：*（表示所有与对象相关的动作） **说明** 配置所有权限可能有资源被删除的风险，如果想规避此风险，建议配置动作名称为“Get*”，表示所有读权限。
	授权条件	● 条件1： – 键：CurrentTime – 条件运算符：DateGreaterThan – 值：2019-03-26T12:00:00Z（取值为UTC格式） ● 条件2： – 键：CurrentTime – 条件运算符：DateLessThan – 值：2019-03-26T15:00:00Z（取值为UTC格式）

步骤5 单击右下角的“创建”，完成桶策略创建。

----结束

验证

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

3.8.9.5 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 选择“对象ACL>公共权限>公共读”，勾选“我已知晓上述配置可能产生的影响”，再单击“确认修改”。

步骤5 在匿名用户的操作列单击“编辑”，为匿名用户设置对象的读取权限。

步骤6 单击“确定”。

----结束

验证

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

步骤2 匿名用户将对应的URL复制到浏览器，则可以访问到对象。

----结束

3.8.9.6 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“对象”页面。

步骤2 在左侧导航栏，单击“访问权限控制 > 桶策略”。

步骤3 单击“创建”。

步骤4 配置如下参数。

表 3-34 为匿名用户设置文件夹的访问权限

参数		说明
策略配置方式		可视化视图
策略名称		自定义
策略内容	效力	允许
	被授权用户	• 被授权用户：所有账户
	授权资源	• 资源范围：指定对象 • 资源路径：输入指定对象前缀。配置为需要访问的文件夹内的所有对象，如文件夹名称为“folder-001”时，资源路径为“folder-001/*”。

参数		说明
	授权操作	• 动作范围：自定义配置 • 选择动作：GetObject（获取对象内容，获取对象元数据）

步骤5 单击右下角的“创建”，完成桶策略创建。

----结束

验证

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

步骤2 任何用户将对应的URL复制到浏览器，则可以访问到对象。

----结束

3.9 多版本控制

3.9.1 多版本控制简介

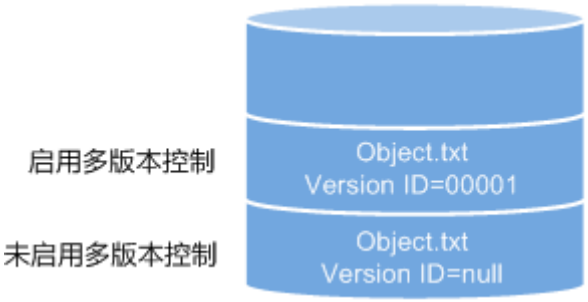
利用多版本控制，您可以在一个桶中保留多个版本的对象，使您更方便地检索和还原各个版本，在意外操作或应用程序故障时快速恢复数据。

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3-9所示。

  图 3-9 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3-10所示。

图 3-10 多版本对象示意图（新对象）

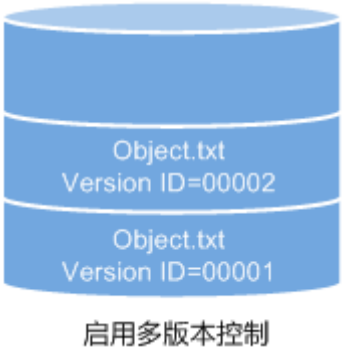
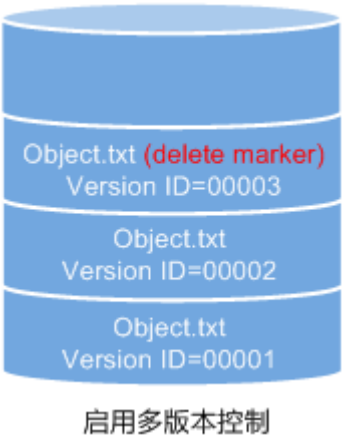


表 3-35 版本说明

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 3-11 删除标记示意图

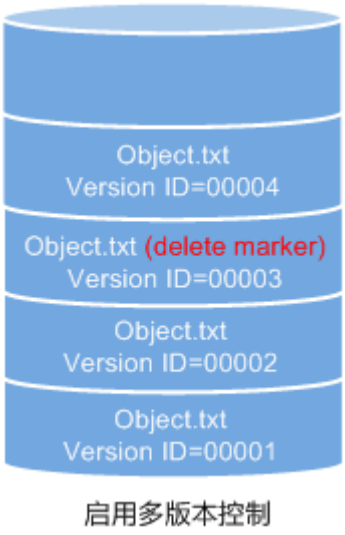


- 删除带删除标记的对象可恢复该对象。详细操作请参见**取消删除对象**的**相关操作**。
- 在“已删除对象”列表，选中对象，可指定版本号彻底删除指定版本对象。详细操作请参见**删除对象或文件夹**的**相关操作**。

- 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3-12所示。

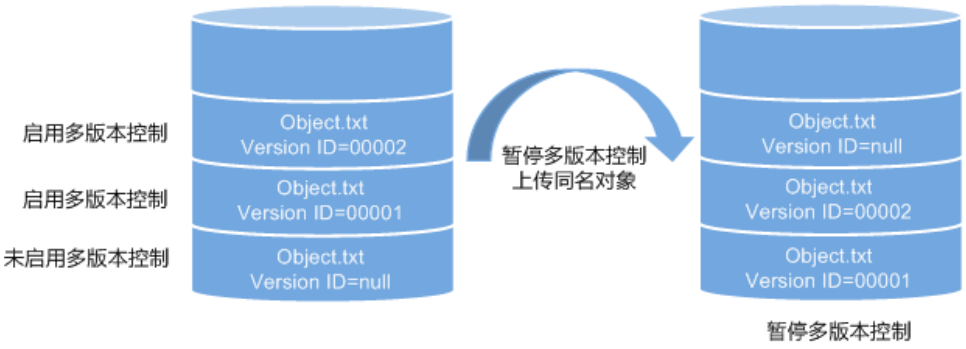
图 3-12 删除后再上传同名对象的版本示意图



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 3-13 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。

3.9.2 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“对象”页面。

步骤2 在左侧导航栏，单击“概览”，进入“概览”页面。

步骤3 单击“基础配置”区域下的“多版本控制”卡片，系统弹出多版本控制对话框。

步骤4 选择“启用”。

步骤5 单击“确定”，启用目标桶中对象的多版本控制。

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

----结束

相关操作

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

步骤1 在OBS管理控制台桶列表中，单击待操作的桶，进入“对象”页面。

步骤2 在“对象”列表，单击待操作的对象，进入对象详情页面。

步骤3 在“版本”页签，显示该对象的所有版本。

步骤4 对多版本对象可做以下操作。

1. 在待操作版本对象右侧，单击“下载”，可下载该版本对象。
2. 在待操作版本对象右侧，单击“删除”，将永久删除该版本对象，不可恢复。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

3.10 日志记录

3.10.1 访问日志记录简介

出于分析目的，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。

由于日志文件是OBS产生，并且由OBS上传到存放日志的桶中，因此OBS需要获得委托授权，用于上传生成的日志文件。所以在配置桶日志记录前，需要先到统一身份认证服务生成一个对OBS服务的委托，并在配置日志记录时添加该委托。默认情况下，在

为委托配置权限时只需设置日志存储桶的上传对象（PutObject）权限，示例如下（其中mybucketlogs为日志存储桶的桶名）。

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

由于日志存储在OBS中也会占用用户租用的OBS存储空间，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 3-36 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

名称	示例	含义
ErrorCode	-	错误码
BytesSent	211	HTTP响应的字节大小
ObjectSize	-	对象大小（bytes）
TotalTime	6	服务端处理时间（ms）
Turn-AroundTime	6	总请求时间（ms）
Referer	-	请求的referrer头域
User-Agent	HttpClient	请求的user-agent头域
VersionID	-	请求中带的versionId
STSLogUrn	-	联邦认证及委托授权信息

3.10.2 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“对象”页面。

步骤2 在左侧导航栏，单击“概览”，进入“概览”页面。

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

步骤4 选择“启用”。

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

步骤6 设置“日志文件前缀”，指定日志文件的前缀。

启用日志记录功能后，生成的日志文件根据如下规则命名：

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

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

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

例如：

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

步骤7 选择IAM委托，给OBS授予上传日志文件到日志存储桶的权限。

默认情况下，在为委托配置权限时只需设置日志存储桶的上传对象（PutObject）权限，示例如下（其中mybucketlogs为日志存储桶的桶名）。

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

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

步骤8 单击“确定”。

日志记录设置成功后，大约15分钟后可在日志存储桶中查看到桶的操作日志。

----结束

相关操作

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。

3.11 事件通知

3.11.1 SMN 通知简介

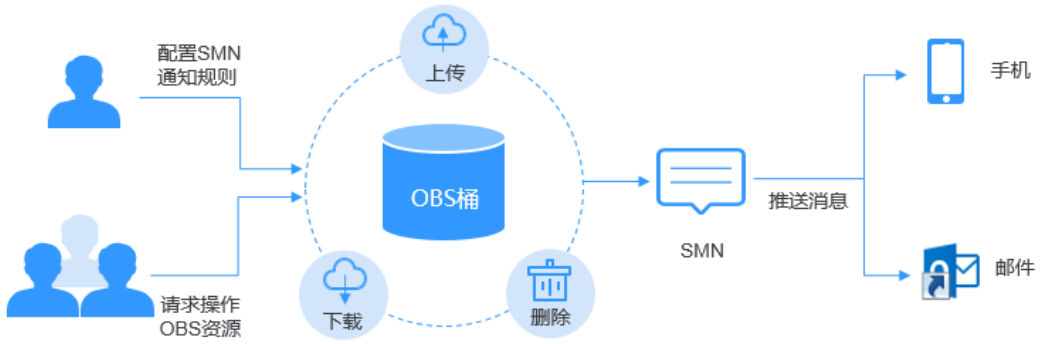
消息通知服务（SMN）是可靠，可扩展，海量的消息通知服务。它大大简化系统的耦合，能够根据用户的需求，向订阅终端主动推送消息，订阅终端可以是电子邮件、短信等。

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 3-14 SMN 通知示意图



3.11.2 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“对象”页面。

步骤2 在左侧导航栏，单击“概览”，进入“概览”页面。

步骤3 在“基础配置”区域下，单击“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4 单击“创建”，系统弹出“创建事件通知”对话框。

步骤5 配置事件通知参数，参数说明如**表3-37**所示。

表 3-37 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。

参数	说明
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。
	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6 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。

3.11.3 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”，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“对象”页面。单击“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3-37**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 3-38 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

3.12 跨区域复制

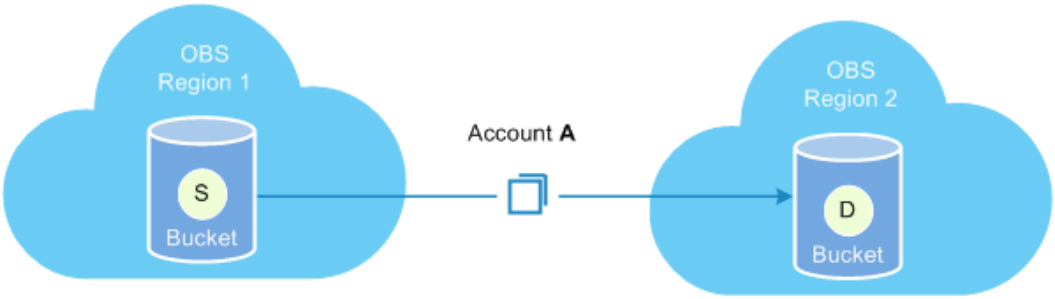
3.12.1 跨区域复制简介

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。

图 3-15 跨区域复制示意图



复制的内容

启用跨区域复制规则后，符合以下条件的对象会复制到目标桶中：

- 新上传的对象。
- 有更新的对象，比如对象内容有更新，或者某一对象跨区域复制成功后源桶对象ACL设置有更新。
- 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。
- 源桶和目标桶的多版本控制状态必须保持一致。
- 源桶中的对象只能被复制到一个目标桶中，且复制过去的对象不能再被复制到另外一个目标桶。例如有两个不同区域的桶A和桶B，桶A数据可以复制到桶B中，桶

B数据也可以复制到桶A中，但桶B中存储的桶A数据的副本不会复制，同理桶A中存储的桶B数据的副本也不会复制。

- 当且仅当源桶、目标桶多版本控制状态开启，在源桶中不指定版本删除对象时，目标桶会同步删除此对象；除此之外，删除源桶对象时，目标桶默认不会同步删除操作。
- 在启用跨区域复制过程中，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。
- 启用历史对象复制后，修改跨区域复制配置可能导致历史对象不复制，建议在历史对象复制完成前不要改变该桶的跨区域复制配置。
- 开启跨区域复制功能后，源桶将不再支持追加写对象。
- 如果已经设置过桶的跨集群或跨区域复制配置，再次设置将会覆盖已有的复制策略。
- 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。
- 配置了2AZ容灾功能的桶，不支持另外配置跨区域复制规则；已经配置跨区域复制规则的桶，也不支持2AZ容灾。
- 在主区域故障期间不支持查询桶、创建桶或者删除桶。

3.12.2 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“对象”页面。

步骤2 在左侧导航栏，单击“跨区域复制”。

步骤3 单击“创建规则”，系统将弹出“创建跨区域复制规则”对话框。

步骤4 根据业务规划配置跨区域复制规则，参数的详细说明如表3-39所示。

表 3-39 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。 跨区域复制规则配置完成后需要等待15分钟，才会开始启动历史对象复制任务。
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。
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“Tenant Administrator”权限。

步骤5 （可选）创建IAM委托，参见创建委托。

步骤6 单击“确定”，完成跨区域复制规则创建。

----结束

3.13 跨集群复制

操作场景

跨集群复制能够为用户提供跨AZ数据容灾的能力，满足用户数据复制到同一区域下不同AZ进行备份的需求。

每个OBS桶都有其所属的区域、可用区（AZ）和集群。当需要对桶进行AZ间容灾时，可以使用跨集群复制功能，将一个桶（源桶）的数据复制到另一个AZ的集群下的另一个桶（目标桶）。当其中一个AZ故障时，另一个AZ中的数据仍能够正常使用，保证业务不中断。

在配置跨集群复制规则时，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。

复制的内容

启用跨集群复制规则后，符合以下条件的对象会复制到目标桶中：

- 新上传的对象。
- 有更新的对象，比如对象内容有更新或者已复制成功的对象ACL有更新。
- 桶中的历史对象（需要开启“同步历史对象”功能）。

约束与限制

- 启用跨集群复制功能之前上传的对象，默认不会被复制到目标桶。
- 源桶和目标桶必须属于同一区域的不同可用区。
- 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。例如有两个不同可用区的桶A和桶B，桶A数据可以复制到桶B中，桶B数据也可以复制到桶A中，但桶B中存储的桶A数据的副本不会复制，同理桶A中存储的桶B数据的副本也不会复制。
- 当且仅当源桶、目标桶多版本控制状态开启，在源桶中不指定版本删除对象时，目标桶会同步删除此对象；除此之外，删除源桶对象时，目标桶默认不会同步删除操作。
- 在启用跨集群复制过程中，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。
- 如果源桶拥有者与对象拥有者不同，则对象拥有者必须通过对象ACL向源桶拥有者授予对象读取和ACL读取权限；如果目标桶拥有者与源桶拥有者不同，需要目

标桶拥有者通过桶策略向源桶拥有者授予ReplicateObject和ReplicateDelete权限。

- 同一个源桶只能创建一条复制所有对象的跨集群复制规则，或多条（最多100条）按前缀匹配的跨集群复制规则。
- 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。
- 在启用跨集群复制过程中，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桶不一致。
- 如果已经设置过桶的跨集群或跨区域复制配置，再次设置将会覆盖已有的复制策略。

操作步骤

步骤1 在左侧导航栏，单击“跨集群复制”。

步骤2 单击“创建规则”，系统将弹出“创建跨集群复制规则”对话框。

步骤3 根据业务规划配置跨集群复制规则，参数的详细说明如表3-40所示。

表 3-40 跨集群复制规则参数

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1023个字节。 • 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或被包含关系，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“ab”或“abcd”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。 跨集群复制规则配置完成后需要等待15分钟，才会开始启动历史对象复制任务。 后台管理员开启同步历史对象功能时，该选项才可见。

参数		说明
目标桶	桶	选择复制到的目标桶，目标桶需要与源桶处于不同集群。 当一个源桶配置多条跨集群复制规则时，不同规则指定的目标桶必须保持一致。如果修改其中一条规则的目标桶，将改变所有规则的目标桶。
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集群复制。 如果还未创建委托，请先参考**创建用于跨区域或跨集群复制的委托**进行创建。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，且需要具有OBS管理员权限（即OBS所有权限）。

步骤4 单击“确定”，完成跨集群复制规则创建。

----结束

3.14 生命周期管理

3.14.1 生命周期管理简介

生命周期管理是指通过配置指定的规则，实现定时删除桶中的对象。

生命周期管理可适用于以下典型场景：

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

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

生命周期管理规则通常包含以下关键要素：

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

3.14.2 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。

- 指定对象过期删除。

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“对象”页面。

步骤2 在左侧导航栏，单击“概览”，进入“概览”页面。

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

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

步骤4 单击“创建”。

步骤5 配置生命周期管理规则。

基本信息：

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

说明

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

- 如果桶开启过“多版本控制”，配置界面可见“当前版本”和“历史版本”。

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

说明

- “当前版本”与“历史版本”是针对“多版本控制”而言的。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。
- 对象过期删除天数：指定在对象最后一次更新后多少天，受规则影响的对象将过期并自动被OBS删除。

例如，您于2015年1月7日在OBS中存储了以下几个文件：

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

您于2015年1月10日在OBS中存储了以下几个文件：

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

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。

说明

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

步骤6 单击“确定”，完成生命周期规则配置。

----结束

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。

3.15 配置自定义域名

3.15.1 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。

3.15.2 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“对象”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 单击页面上方的“配置自定义域名”，如果没有绑定自定义域名也可以在页面下方的配置自定义域名卡片中单击“配置自定义域名”，在用户域名中输入需要配置的自定义域名。

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。

----结束

3.16 静态网站托管

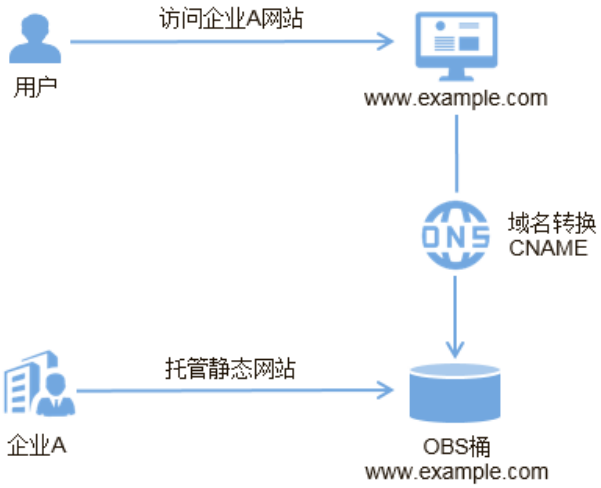
3.16.1 静态网站托管简介

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 3-16 静态网站示意图



3.16.2 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。

3.16.3 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所有用户可访问。

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“对象”页面。

步骤2 **可选**：如果还未将桶内静态网站文件配置为任何用户可访问，请执行本步骤配置所有账户的访问权限。如果已经配置，请跳过此步骤。

参考**为所有账号设置对象的访问权限**为所有账号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，则配置桶策略为“对象只读”，使桶内所有文件能被公开访问。

1. 单击“访问权限控制>桶策略”。
2. 单击“创建”。
3. 配置桶策略信息。

表 3-41 配置公共读策略参数配置说明

参数		说明
策略配置方式		支持可视化视图和JSON视图。此处以可视化视图为例，JSON视图的说明请参见**自定义创建桶策略（JSON视图）**。
策略名称		输入自定义桶策略的名称。
策略内容	效力	允许
	被授权用户	被授权用户：所有账号
	授权资源	- 资源范围：指定对象 - 资源路径：*（*表示桶内所有对象）
	授权操作	- 动作范围：模板配置 - 模板：对象只读

4. 单击“创建”，完成桶策略创建。

步骤3 在左侧导航栏，单击“概览”，进入“概览”页面。

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

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

步骤5 单击“配置静态网站托管”，系统弹出“配置静态网站托管”对话框。

步骤6 打开“状态”开关。

步骤7 “托管模式”选择“配置到当前桶”。

步骤8 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API的方式配置时，OBS不进行限制，用户必须指定对象的“Content-Type”。

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

“重定向规则”采用JSON或XML格式编写，可以包含多条重定向规则，每条重定向规则包含一个Condition和一个Redirect，参数说明如**表3-42**所示。

表 3-42 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"。

容器	键值	键值说明
	HttpRedirectCode	响应中的HTTP状态码。默认值为301，表示永久重定向到Redirect指定的位置，也可根据业务实际情况设置。

重定向规则示例

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

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

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

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

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

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

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

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

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



```
    }
  }
]
```

步骤10 单击“确定”。

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

说明

由于浏览器缓存等原因，您可能需要清除浏览器缓存后才能查看到预期效果。

----结束

3.16.4 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所有用户可访问。

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“对象”页面。

步骤2 在左侧导航栏，单击“概览”，进入“概览”页面。

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

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

步骤4 单击“配置静态网站托管”，系统弹出“配置静态网站托管”对话框。

步骤5 打开“状态”开关。

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

步骤7 单击“确定”。

步骤8 在桶列表中选择重定向的桶。

步骤9 **可选**：如果还未将桶内静态网站文件配置为任何用户可访问，请执行本步骤配置所有账户的访问权限。如果已经配置，请跳过此步骤。

参考**为所有账号设置对象的访问权限**为所有账号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，则配置桶策略为“对象只读”，使桶内所有文件能被公开访问。

1. 单击“访问权限控制>桶策略”。
2. 单击“创建”。
3. 配置桶策略信息。

表 3-43 配置公共读策略参数配置说明

参数		说明
策略配置方式		支持可视化视图和JSON视图。此处以可视化视图为例，JSON视图的说明请参见**自定义创建桶策略（JSON视图）**。
策略名称		输入自定义桶策略的名称。
策略内容	效力	允许
	被授权用户	被授权用户：所有账号
	授权资源	- 资源范围：指定对象 - 资源路径：*（*表示桶内所有对象）
	授权操作	- 动作范围：模板配置 - 模板：对象只读

4. 单击“创建”，完成桶策略创建。

步骤10 **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

3.17 跨域资源共享

3.17.1 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。

3.17.2 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“对象”页面。

步骤2 在左侧导航栏，单击“概览”，进入“概览”页面。

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

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

步骤4 单击“创建”，系统弹出“创建CORS规则”对话框。

说明

一个桶最多可设置100条CORS规则。

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

表 3-44 CORS 规则

参数	说明
允许的来源	必选参数，指定允许的跨域请求的来源，即允许来自该域名下的请求访问该桶。 允许多条匹配规则，以回车换行为间隔。每个匹配规则允许使用最多一个“*”通配符。例如： http://rds.example.com https://*.vbs.example.com
允许的方法	必选参数，指定允许的跨域请求方法，即桶和对象的几种操作类型。包括：Get、Post、Put、Delete、Head。
允许的头域	可选参数，指定允许的跨域请求的头域。只有匹配上允许的头域中的配置，才被视为是合法的CORS请求。 允许的头域可设置多个，多个头域之间换行隔开，每行最多可填写一个*符号，不支持&、:、<、空格以及中文字符。

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

步骤6 单击“确定”。

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

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

----结束

3.18 防盗链

3.18.1 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。

3.18.2 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“对象”页面。

步骤2 在左侧导航栏，单击“概览”，进入“概览”页面。

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

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

Referer规则如下：

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

说明

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

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

步骤5 单击 保存设置。

----结束

3.19 任务中心

当您执行上传对象、删除文件夹时，会在任务中心生成一条任务记录，方便您查看任务进度和状态。

说明

刷新或关闭浏览器，会取消当前任务并清除全部记录。

操作步骤

步骤1 在桶的对象列表页，单击界面右上角的“任务中心”。

步骤2 执行上传对象、删除文件夹操作，可查看对应操作的任务记录。

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

----结束

3.20 2AZ 容灾

3.20.1 2AZ 容灾简介

背景知识

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，又提供了低时延的网络连接。本文中将可用区简称为AZ。

当桶不开启2AZ容灾，数据仅存储在单个可用区（AZ），成本更低。当桶开启2AZ容灾功能后，数据存储至2个可用区（AZ），可靠性更高。

当桶开启2AZ容灾功能，具备2AZ容灾能力的桶称为融合桶。

使用场景

2AZ容灾能够为用户提供2AZ数据容灾的能力，满足用户数据同步到异地进行备份的需求。

为桶开启2AZ容灾功能时，支持将数据存储在同一区域的2个不同可用区（AZ）。当某个AZ不可用时，仍然能够从另一个AZ正常访问数据，适用于对可靠性要求较高的数据存储场景。遇到风火水电故障时，有效保障数据的可靠性。

同步到另一个AZ的对象是历史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。

同步复制的内容

启用容灾后，符合以下条件的对象会同步到另一个AZ中：

- 新上传的对象。
- 有更新的对象，比如对象内容有更新。
- 删除对象，另一个AZ内的对象同步删除。

约束与限制

- 2AZ容灾策略一旦确认，后续无法更改。请根据业务情况提前规划2AZ容灾策略。
- 2AZ容灾策略不保证时效性，配置2AZ容灾功能后，可能会出现对象不会立即同步的情况，请耐心等待。
- 桶版本号为3.0及以上的桶支持2AZ容灾功能。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。
- 配置了2AZ容灾功能的桶，不支持另外配置跨区域复制规则；已经配置跨区域复制规则的桶，也不支持2AZ容灾。

- 追加写对象不支持2AZ容灾。
- 融合桶删除后，12h后才能创建同名桶。
- 在主集群故障期间不支持查询桶、创建桶或者删除桶。

3.20.2 配置 2AZ 容灾

本章节介绍存量桶的2AZ容灾的配置方法。新创桶的2AZ容灾的配置方法详见**创建桶**。

前提条件

已存在一个单AZ存储桶，且桶未配置跨区域复制规则。

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“对象”页面。

步骤2 在左侧导航栏，单击“概览”，进入“概览”页面。

步骤3 单击“基础配置”区域下的“容灾”卡片，系统弹出容灾对话框。

步骤4 在弹出的弹窗内，单击“启用”，然后单击“确定”。

说明

开启容灾后，桶及桶中对象将存储在同一区域的2个可用区中，存储费用较高，且开启后不支持关闭，请谨慎操作。

----结束

3.21 相关操作参考

3.21.1 创建委托

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。

创建用于上传日志的委托

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

步骤2 单击“创建委托”，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 单击“下一步”。

步骤8 在“选择策略”页面，选择拥有日志存储桶上传权限的自定义策略，然后单击“下一步”。

如还未创建自定义策略，需要先在左侧导航“权限管理 > 权限”栏目创建自定义策略。

策略配置方式选择“JSON视图”，策略内容如下：

说明

下方JSON中mybucketlogs需要替换为实际日志存储桶的桶名。

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

步骤9 选择授权范围方案时，选择“全局服务资源”，单击下方的“确定”完成委托创建。

----结束

创建用于跨区域或跨集群复制的委托

步骤1 进入“统一身份认证服务”管理控制台“委托”页面。

步骤2 单击“创建委托”，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”。

步骤6 选择“持续时间”。

步骤7 在“权限选择”区域，“全局服务 > 对象存储服务”右侧，单击“修改”。

步骤8 选择具有OBS管理员权限（即OBS所有操作权限）的自定义策略，单击“确定”。

1. 如还未创建自定义策略，需要先在左侧导航“权限管理 > 权限”栏目创建自定义策略。

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

   ```
   {
      "Version": "1.1",
      "Statement": [
         {
            "Action": [
               "obs:*:*"
            ],
            "Effect": "Allow"
         }
      ]
   }
   ```

步骤9 选择权限作用范围，并在权限区域搜索并选择系统策略 “OBS Administrator”。

步骤10 单击“确定”，完成委托创建。

----结束

3.22 异常处理

3.22.1 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。

3.22.2 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”。

步骤3 单击“确定”。

----结束

3.22.3 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。

3.22.4 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。

3.22.5 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。

3.22.6 AZ1 使用在 AZ2 创建失败的桶名创桶返回 500

问题

双AZ环境AZ2下电，请求发往AZ1并指定在AZ2创桶，创桶失败。接着，使用创建失败的桶名，再次向AZ1发起创桶请求并指定在AZ1创桶，接口返500。

回答

在AZ2创桶失败后，桶信息已经存在且会保留30分钟。如果30分钟内继续在其它AZ创建同名桶，则会创建失败。建议30分钟后再使用创建失败后的桶名进行创桶，或者使用新桶名创桶。

3.22.7 上传或下载对象报错

本节介绍使用OBS console上传或下载对象报错的常见场景和解决方案。常见于上传大文件（大于8M）失败。

场景一

现象描述

上传或下载对象时，浏览器网页提示无法找到服务器的IP地址，对应错误码为ERR_NAME_NOT_RESOLVED（以Chrome浏览器为例）。

解决方案

出现该问题的原因为未配置localhost。请参考**配置本地hosts**的说明，完成localhost配置。

说明

配置本地hosts文件的格式为：OBS后台服务的ip 桶域名。例如：

```
xx.xx.xx.xx bucket-name.obsv3.example-region.com
```

其中：

OBS后台服务的ip是在安装OBS服务阶段导出的工程参数导出表中，表单 “1.1 基本参数” obsv3_address 参数的值。

桶域名请在登录console后，在桶基本信息页面查找。

配置完成之后，刷新页面，此时可能出现一个警告"您的连接不是私密连接"，请参考**场景三**。

场景二

现象描述

上传或下载对象时，浏览器网页超时，对应错误码为ERR_CONNECTION_TIMED_OUT（以Chrome浏览器为例）。

解决方案

出现该问题的原因为本地hosts文件配置错误，或当前终端与OBS的网络不通。请参考**配置本地hosts**确认配置是否正确，或检查ip正确性和网络连通性。

ip配置正确的检验标准是：

打开浏览器新窗口，输入桶域名（注意是以 https:// 开头的地址），浏览器应弹出警告：您的连接不是私密连接。

选择跳过警告。跳过之后的响应，必须是这种xml格式的才对，如果是其他类型的响应，请检查步ip是否正确。

场景三

现象描述

上传或下载对象时，浏览器网页提示隐私错误，对应错误码为NET::ERR_CERT_AUTHORITY_INVALID（以Chrome浏览器为例）。

解决方案

出现该问题的原因为OBS未购买商用证书，浏览器无法信任，所以会显示警告并阻止用户发送请求。临时的解决方法是单击网页下方的“高级”，在弹出的扩展信息中再单击“继续访问”即可。

如果要完全避免此问题，请下载并安装OBS证书。安装证书请注意选择“将所有的证书都放入下列存储（受信任的根证书颁发机构）”。

3.23 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3-45列出了错误响应中的常见错误码。

表 3-45 错误码列表

错误码	描述
Obs.0000	无效的参数。
Obs.0001	所有对这个对象的访问已经无效了。
Obs.0002	文件的绝对路径总长度不能超过1023字符，请重试。
Obs.0003	连接超时。
Obs.0004	客户端与服务器的时间相差大于15分钟。 出于安全目的，OBS会校验客户端与OBS服务器的时间差，当该时间差大于15分钟时，OBS服务器会拒绝您的请求，从而出现此报错。请根据本地UTC时间调整本地时间后再访问。
Obs.0005	服务器负载过高，请稍后重试。
Obs.0006	用户拥有的桶的数量已经达到了系统的上限。 一个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.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。

错误码	描述
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。

4 常见问题

4.1 一般性问题

4.1.1 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。

4.1.2 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。

4.1.3 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。

4.1.4 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+）或OBS API的多段上传接口上传。
- OBS Browser+和API上传的单个对象最大是48.8TB。

4.1.5 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。

4.1.6 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。

4.1.7 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。

4.1.8 OBS 中的数据可以让其他用户访问吗?

可以。

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

4.1.9 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 4-1 OBS 管理工具断点续传功能

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

4.1.10 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 4-2 OBS 管理工具批量上传功能

工具	批量上传
管理控制台	OBS管理控制台支持批量上传文件，单次最多支持100个文件同时上传，总大小不超过5GB。详见**上传文件**。
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。
API	不支持

4.1.11 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 4-3 OBS 管理工具批量下载功能

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

4.1.12 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 4-4 OBS 管理工具批量删除功能

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

说明

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

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

4.1.13 OBS 上传下载速率的影响因素有哪些?

影响OBS上传下载速率的因素有：

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

4.1.14 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。

4.1.15 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。

4.1.16 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。

4.1.17 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。

4.2 权限相关

4.2.1 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。

4.2.2 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。

4.2.3 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。

4.3 桶和对象相关

4.3.1 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。

4.3.2 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，请联系管理员进一步解决。

4.3.3 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。
- 如果以上都不是，请联系管理员进一步解决。

4.3.4 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，请联系管理员进一步解决。

4.3.5 我可以修改对象名称吗?

可以。您可以用OBS Browser+客户端重命名桶中的对象，但不支持批量操作。

4.3.6 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。

4.3.7 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 4-5 对象 URL 获取方式

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

说明

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

4.3.8 无法搜索到桶中对象

OBS管理控制台和OBS Browser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。

4.3.9 OBS 是否支持配额管理?

OBS支持桶的存储空间配额管理。

单个桶的存储空间大小默认没有限制，您可以通过桶配额管理能力，修改单个桶的存储空间大小限制。超过设置的配额限制后，上传对象会失败。

并行文件系统暂不支持配额配置功能，默认无配额限制。

⚠ 注意

配额设置生效时间为15分钟，在进行桶存量统计之后的15分钟，OBS才会校验配额是否达到上限。如果桶持续在进行对象写入，且校验时发现已达到上限，已经写入的对象依然是有效的，只会限制后续新的对象无法写入。所以某些情况下桶中实际的容量可能略大于设置的桶配额。

桶配额设置方法

您可以通过OBS控制台、API管理桶配额。

API设置桶配额的方法请参见API参考中的“设置桶配额”接口。

此处介绍如何通过OBS控制台设置桶配额。

步骤1 在左侧导航栏，单击“概览”，进入“概览”页面。

步骤2 单击“基础配置”区域的“配额限制”卡片，直接修改当前桶的配额。

配额默认无限制，最小设置阶梯为1MB。

步骤3 修改完成后单击“确定”。

----结束

4.4 安全性

4.4.1 我的数据存在 OBS 中，如何保证安全性?

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

4.4.2 OBS 会不会扫描我的数据用于其他用途?

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

4.4.3 后台工程师能否导出我存在 OBS 中的数据?

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

4.4.4 OBS 如何保证我的数据不会被盗用?

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

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

可以。在使用过程中，密钥AK和SK可以随时更换。

4.4.6 多个用户是否可以共享一对 AK 和 SK 来访问 OBS?

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

4.5 持久性和可用性

4.5.1 OBS 的持久性和可用性如何?

OBS通过存储介质的慢盘/坏道检测、AZ内设备和数据冗余、AZ之间数据容灾、跨区域复制等技术方案，提供针对介质、服务器、机柜、数据中心和区域的多级可靠性保障。其数据持久性最高达99.9999999999%（12个9，多可用区），可用性高达99.95%（多可用区），远高于传统架构。

99.9999999999%（12个9）的持久性意味着平均每年对象损失率预计为0.0000000001%。例如，您在OBS中存储了一亿个对象，则预计平均每一万年才会出现丢失一个对象的可能。

可用性也可以理解为业务连续性，99.95%的可用性意味着如果连续访问OBS一万分钟（7天左右），期间出现不可访问的时长不超过5分钟。

4.5.2 OBS 单 AZ 和多 AZ 有什么区别?

问题一：

Q：创建桶时，数据冗余存储策略选择单AZ存储和多AZ存储有什么区别?

A：选择多AZ存储，数据将冗余存储至多个AZ中，可靠性更高。选择单AZ存储，数据仅存储在单个AZ中，但相比多AZ更加便宜。

问题二：

Q：选择多AZ存储后，数据是以副本的形式分别存放在多个AZ中吗？如果某个AZ出现故障，其他AZ中的数据是否完整?

A：多AZ采用Erasure Code（EC，纠删码）算法做数据冗余，不是以副本的形式存储。选择多AZ存储的桶，数据将存储在同一区域的多个不同AZ。当某个AZ不可用时，仍然能够从其他AZ正常访问数据，适用于对可靠性要求较高的数据存储场景。目前多AZ只支持一个AZ故障。

问题三：

Q：在不删除桶的前提下能否更改数据冗余存储策略?

A：不能。桶一旦创建成功，数据冗余存储策略就确定了，后续无法更改。可以考虑将数据迁移至新创建的桶，以实现数据冗余存储策略修改。

4.5.3 OBS 的数据冗余存储方式是什么?

OBS采用Erasure Code（EC，纠删码）算法做数据冗余，不是以副本的形式存储。

在满足同等可靠性要求的前提下，EC的空间利用率优于多副本。

数据冗余存储策略为“单AZ”的桶，在AZ内的节点间使用EC算法做数据冗余；“多AZ”的桶在AZ内节点间EC冗余的基础上，会同时在多个AZ间再做数据冗余。

4.5.4 OBS 的 SLA 及约束

SLA（Service Level Agreement）：是产品对用户承诺的服务质量，是对自身服务的全年不中断（可用性）时长的一个承诺。OBS的标准存储单可用区存储每服务周期服务可用性不低于99.9%；标准存储多可用区存储每服务周期服务可用性不低于99.95%。SLA可用性的达成，强依赖硬件的更换速度，可用性为99.95%（全年业务中断容忍4.38H内）时，硬件更换需要在8小时内完成；可用性为99.9%（全年业务中断容忍8.76H内）时，硬件更换需要在30小时内完成。

SLA协议未达到服务可用性的情形不包括：

1. 因边缘接入的网络故障（如边缘节点断网、运营商线路时延抖动或故障）、硬件故障（如设备电源故障、硬盘故障、内存、背板）、机房故障（如断电、台风、洪水、地震、疫情）等原因，导致无法通过边缘网络进行业务接入的情况不作为服务不可用情况。
2. 设备部署在客户机房，依赖于客户提供的基础设施和网络。

4.6 碎片管理

4.6.1 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。

4.6.2 如何处理碎片?

您可以通过OBS管理控制台或OBS Browser将桶中碎片清理掉。

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

您可以通过OBS管理控制台或OBS Browser+将桶中碎片清理掉。

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

4.7 多版本控制

4.7.1 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。

4.7.2 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**。

4.8 事件通知

4.8.1 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。

事件通知详细的配置请参见**配置事件通知**。

4.9 生命周期管理

4.9.1 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。

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4-6**参数创建规则：

表 4-6 过期删除参数配置

参数		取值
状态		启用
规则名称		例如：rule-delete
前缀		可选。 ● 填写前缀：满足该前缀的对象将受生命周期规则管理，即批量删除指定前缀的对象。 ● 未填写前缀：桶内所有对象都将受生命周期规则管理，即清空桶。
当前版本	对象过期删除天数	1天
历史版本	对象过期删除天数	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。

4.10 静态网站托管

4.10.1 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。

4.10.2 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。

4.10.3 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*。

4.11 跨区域复制

4.11.1 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。

4.11.2 删除对象操作会同步复制到跨区复制的桶中吗?

不会，删除操作不同步。

启用跨区域复制规则后，符合以下条件的对象会复制到目标桶中：

- 新上传的对象。
- 有更新的对象，比如对象内容有更新，或者某一对象跨区域复制成功后源桶对象ACL设置有更新。
- 桶中的历史对象（需要开启“同步历史对象”功能）。

4.11.3 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。
- 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。

A 修订记录

发布日期	修订记录
2024-04-15	第一次正式发布。