对象存储服务(OBS)

产品介绍

文档版本 01

发布日期 2024-06-28

华为技术有限公司

商标声明


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

注意

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

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

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： https://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

安全声明

漏洞处理流程

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

目 录

1 什么是对象存储服务

对象存储服务简介

对象存储服务（Object Storage Service，OBS）是一个基于对象的海量存储服务，为客户提供海量、安全、高可靠、低成本的数据存储能力。

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

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

产品架构

OBS的基本组成是**桶**和**对象**。

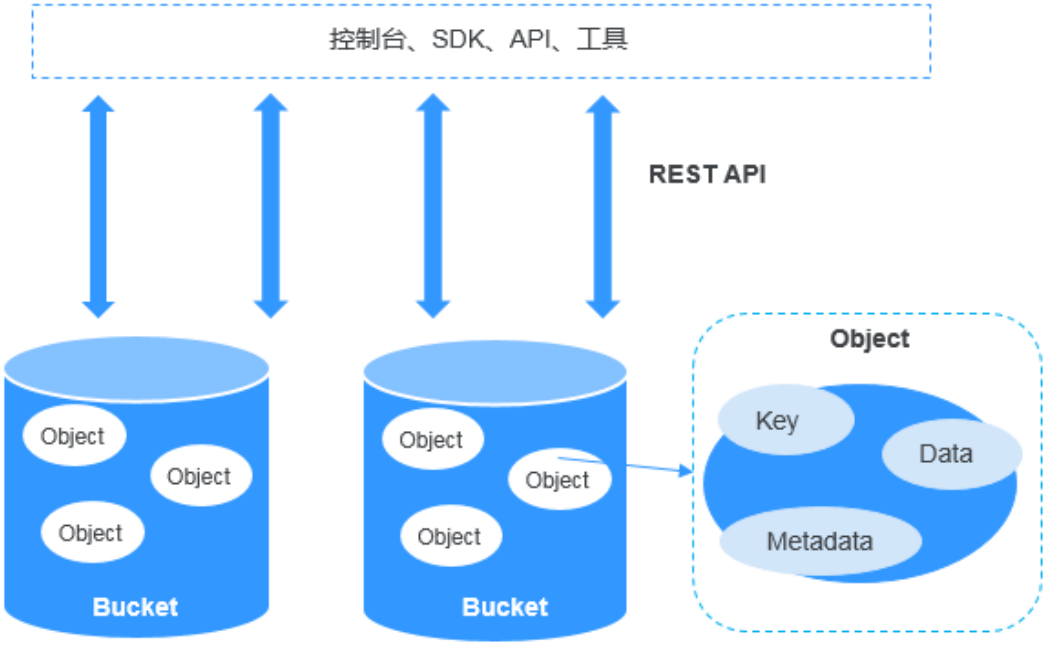
桶是OBS中存储对象的容器，每个桶都有自己的存储类别、访问权限、所属区域等属性，用户在互联网上通过桶的**访问域名**来定位桶。

对象是OBS中数据存储的基本单位，一个对象实际是一个文件的数据与其相关属性信息的集合体，包括Key、Metadata、Data三部分：

- Key：键值，即对象的名称，为经过UTF-8编码的长度大于0且不超过1024的字符序列。一个桶里的每个对象必须拥有唯一的对象键值。
- Metadata：元数据，即对象的描述信息，包括系统元数据和用户元数据，这些元数据以键值对（Key-Value）的形式被上传到OBS中。
  - 系统元数据由OBS自动产生，在处理对象数据时使用，包括Date，Content-length，Last-modify，ETag等。
  - 用户元数据由用户在上传对象时指定，是用户自定义的对象描述信息。
- Data：数据，即文件的数据内容。

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

图 1-1 产品架构



存储类别

OBS提供了四种存储类别：标准存储、低频访问存储、归档存储、深度归档存储（受限公测中），从而满足客户业务对存储性能、成本的不同诉求。不同规格的存储类别转换请参见**OBS存储类别转换**，不同规格的存储类别计费参见**存储费用**。

- 标准存储访问时延低和吞吐量高，因而适用于有大量热点文件（平均一个月多次）或小文件（小于1MB），且需要频繁访问数据的业务场景，例如：大数据、移动应用、热点视频、社交图片等场景。
- 低频访问存储适用于不频繁访问（平均一年少于12次）但在需要时也要求快速访问数据的业务场景，例如：文件同步/共享、企业备份等场景。与标准存储相比，低频访问存储有相同的数据持久性、吞吐量以及访问时延，且成本较低，但是可用性略低于标准存储。
- 归档存储适用于很少访问（平均一年访问一次）数据的业务场景，例如：数据归档、长期备份等场景。归档存储安全、持久且成本极低，可以用来替代磁带库。为了保持成本低廉，数据恢复时间可能长达数分钟到数小时不等。
- 深度归档存储（受限公测）适用于长期不访问（平均几年访问一次）数据的业务场景，其成本相比归档存储更低，但相应的数据恢复时间将更长，一般为数小时。

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

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

表 1-1 存储类别对比

对比项目	标准存储	低频访问存储	归档存储	深度归档存储（受限公测）
特点	高性能、高可靠、高可用的对象存储服务	高可靠、较低成本的实时访问存储服务	归档数据的长期存储，存储单价更优惠	深度归档数据的长期存储，存储单价相比归档存储更优惠
应用场景	云应用、数据分享、内容分享、热点对象	网盘应用、企业备份、活跃归档、监控数据	档案数据、医疗影像、视频素材、带库替代	长期不访问的数据存档场景
设计持久性	99.999999999%	99.999999999%	99.999999999%	99.999999999%
设计持久性（多AZ）	99.999999999%	99.999999999%	不支持多AZ	不支持多AZ
设计可用性	99.99%	99%	99%	99%
设计可用性（多AZ）	99.995%	99.5%	不支持多AZ	不支持多AZ
最低存储时间	无	30天	90天	180天
最小计量单位[a]	64KB	64KB	64KB	64KB
数据恢复	不涉及	按实际恢复数据量收费，单位GB	分加急、标准恢复方式 按实际恢复数据量收费，单位GB	分加急和标准两种恢复方式 按实际恢复数据量收费，单位GB
图片处理	支持	支持	不支持	不支持

说明

最低存储时间是指对象的计费时间下限。对象存储时间小于最低存储时间时，将按照最低存储时间计费。例如，一个低频访问存储对象在OBS中存储了20天后删除，会按照30天计费。

如何访问对象存储服务

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

表 1-2 OBS 资源管理工具

工具	描述	使用方法
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。	**控制台指南**
OBS Browser（已下线）	OBS Browser已于2020年4月15日下线，相关功能已集成到新版客户端工具OBS Browser+中，请获取最新的**OBS Browser+工具**。给您带来不便敬请谅解。	-
OBS Browser+	OBS Browser+是一款运行在Windows系统上的对象存储服务管理工具，OBS Browser+的图形化界面可以非常方便地让用户在本地对OBS进行管理。	**OBS Browser+工具指南**
obsutil	obsutil是一款用于访问管理OBS的命令行工具，您可以使用该工具对OBS进行常用的配置管理操作。对于熟悉命令行程序的用户，obsutil是执行批量处理、自动化任务的不错选择。	**obsutil工具指南**
obsfs	obsfs是OBS提供的一款基于FUSE的文件系统工具，主要用于将并行文件系统挂载至Linux系统，让用户能够在本地像操作文件系统一样直接使用OBS海量的存储空间。	**obsfs工具指南**
SDK	SDK是对OBS服务提供的REST API进行的封装，以简化用户的开发工作。用户直接调用SDK提供的接口函数即可实现使用OBS业务能力的目的。	**SDK参考**
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。	**API参考**

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2-1向您详细展示了OBS与自建存储服务器的优劣势对比。

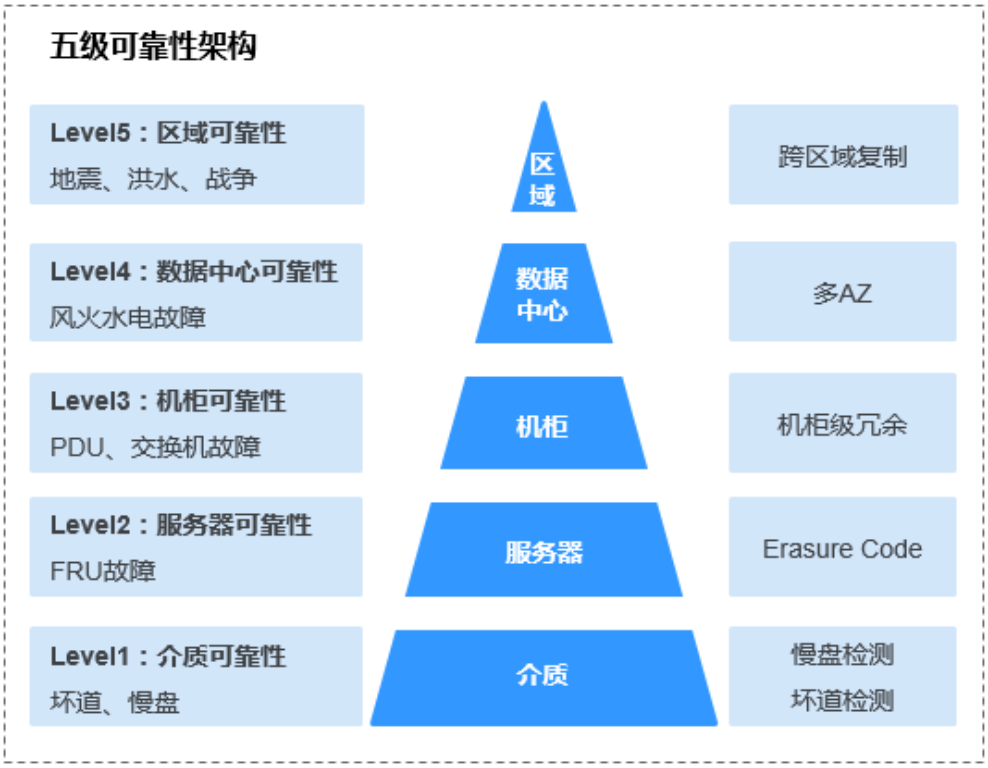
表 2-1 OBS 与自建存储服务器对比

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，在全球部署着N个数据中心，所有业务、存储节点采用分布式集群方式部署，各节点、集群都可以独立扩容，用户永远不必担心存储容量不够。	数据存储量受限于搭建存储服务器时使用的硬件设备，存储量不够时需要重新购买存储硬盘，进行人工扩容。
安全性	支持HTTPS/SSL安全协议，支持数据加密上传。同时OBS通过访问密钥（AK/SK）对访问用户的身份进行鉴权，结合IAM权限、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，保障数据持久性高达99.9999999999%，业务连续性高达99.995%，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。 按使用量付费，用多少算多少。阶梯价格，用的越多越实惠。	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

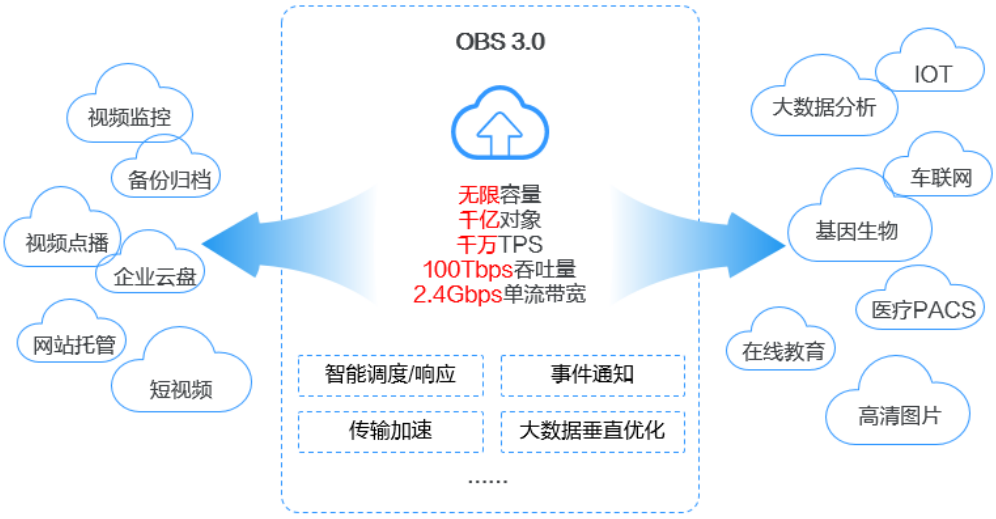
- **数据稳定，业务可靠**：OBS支撑手机云相册，数亿用户访问，稳定可靠。通过跨区域复制、AZ之间数据容灾、AZ内设备和数据冗余、存储介质的慢盘/坏道检测等技术方案，保障数据持久性高达99.9999999999%，业务连续性高达99.995%，远高于传统架构。

  图 2-1 五级可靠性架构保证数据稳定，业务可靠

- **多重防护，授权管理**：OBS通过可信云认证，让数据安全放心。支持多版本控制、服务端加密、防盗链、VPC网络隔离、访问日志审计以及细粒度的权限控制，保障数据安全可信。
- **千亿对象，千万并发**：OBS通过智能调度和响应，优化数据访问路径，并结合传输加速、大数据垂直优化等，为各场景下用户的千亿对象提供千万级并发、超高带宽、稳定低时延的数据访问体验。

图 2-2 千亿对象，千万并发的数据访问体验



- **简单易用，便于管理**：OBS支持标准REST API、多版本SDK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。OBS支持在线升级、在线扩容，升级扩容由华为云实施，客户无感知。
- **数据分层，按需使用**：提供按量计费和包年包月两种支付方式，支持标准、低频访问、归档数据、深度归档数据（受限公测）独立计量计费，降低存储成本。

3 应用场景

大数据分析

场景描述

OBS提供的大数据解决方案主要面向海量数据存储分析、历史数据明细查询、海量行为日志分析和公共事务分析统计等场景，向用户提供低成本、高性能、不断业务、无须扩容的解决方案。

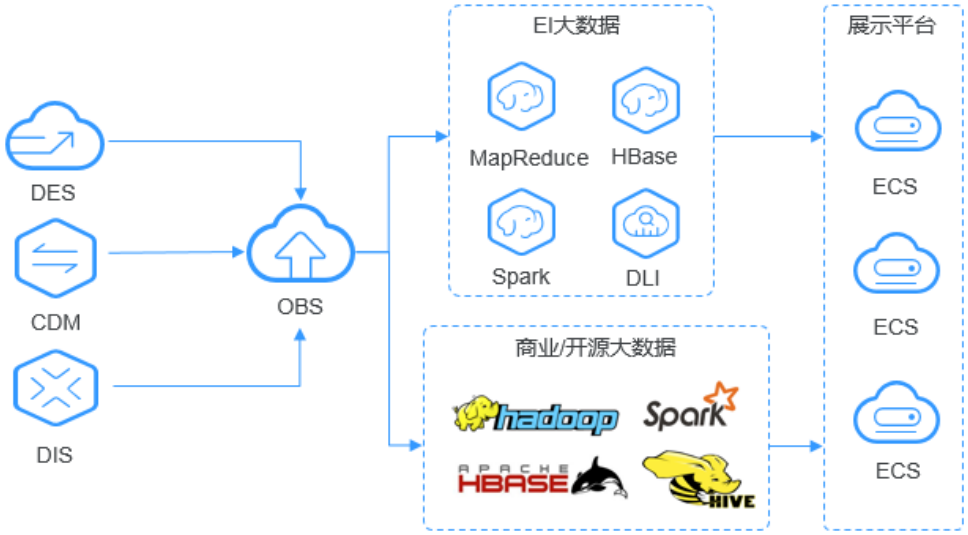
- 海量数据存储分析的典型场景：PB级的数据存储，批量数据分析，毫秒级的数据详单查询等
- 历史数据明细查询的典型场景：流水审计，设备历史能耗分析，轨迹回放，车辆驾驶行为分析，精细化监控等
- 海量行为日志分析的典型场景：学习习惯分析，运营日志分析，系统操作日志分析查询等
- 公共事务分析统计的典型场景：犯罪追踪，关联案件查询，交通拥堵分析，景点热度统计等

用户通过DES等迁移服务将海量数据迁移至OBS，再基于提供的MapReduce等大数据服务或开源的Hadoop、Spark等运算框架，对存储在OBS上的海量数据进行大数据分析，最终将分析的结果呈现在ECS中的各类程序或应用上。

建议搭配服务

MapReduce服务 MRS，弹性云服务器 ECS，数据快递服务 DES

图 3-1 大数据分析



静态网站托管

场景描述

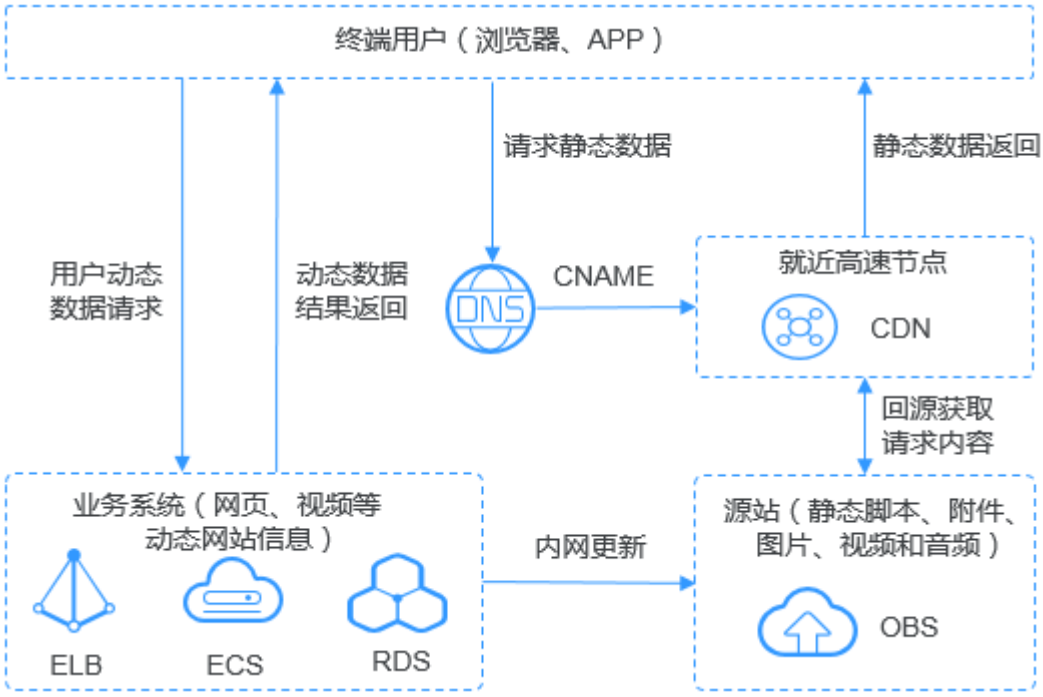
OBS提供低成本、高可用、可根据流量需求自动扩展的网站托管解决方案，结合内容分发网络CDN和弹性云服务器ECS快速构建动静态分离的网站/应用系统。

终端用户浏览器和APP上的动态数据直接与搭建在华为云上的业务系统进行交互，动态数据请求发往业务系统处理后直接返回给用户。静态数据保存在OBS中，业务系统通过内网对静态数据进行处理，终端用户通过就近的高速节点，直接向OBS请求和读取静态数据。

建议搭配服务

内容分发网络 CDN，弹性云服务器 ECS

图 3-2 静态网站托管



在线视频点播

场景描述

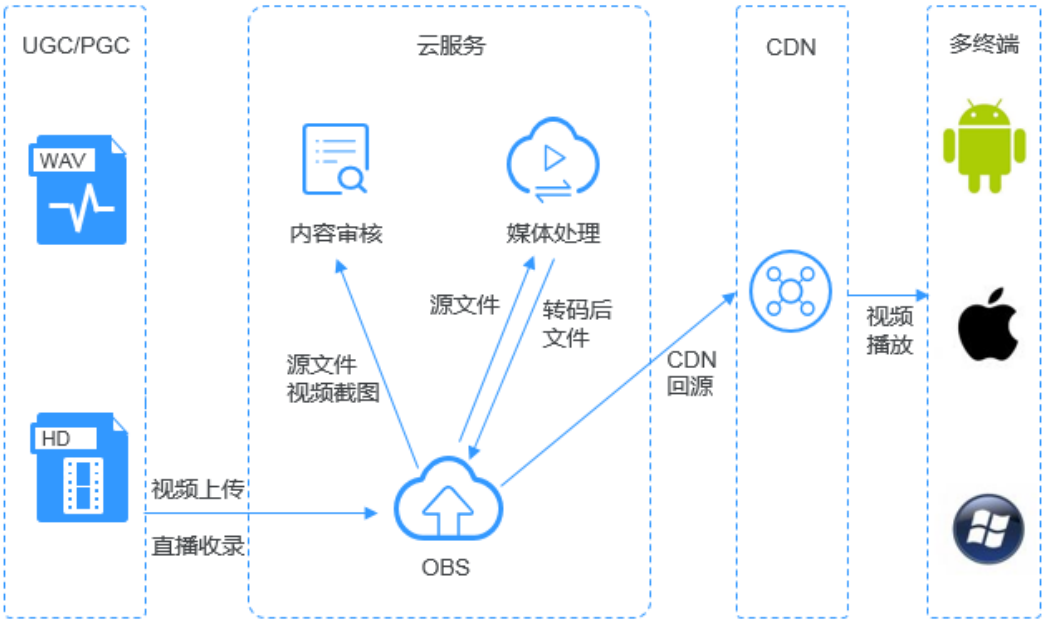
OBS提供高并发、高可靠、低时延、低成本的海量存储系统，结合媒体处理MPC、内容审核Moderation和内容分发网络CDN可快速搭建极速、安全、高可用的视频在线点播平台。

OBS作为视频点播的源站，一般的互联网用户或专业的创作主体将各类视频文件上传至OBS后，通过Moderation对视频内容进行审核，并通过MPC对视频源文件进行转码，最终通过CDN回源加速之后便可以在各类终端上进行点播。

建议搭配服务

内容分发网络 CDN，媒体处理 MPC，内容审核 Moderation

图 3-3 视频点播



基因测序

场景描述

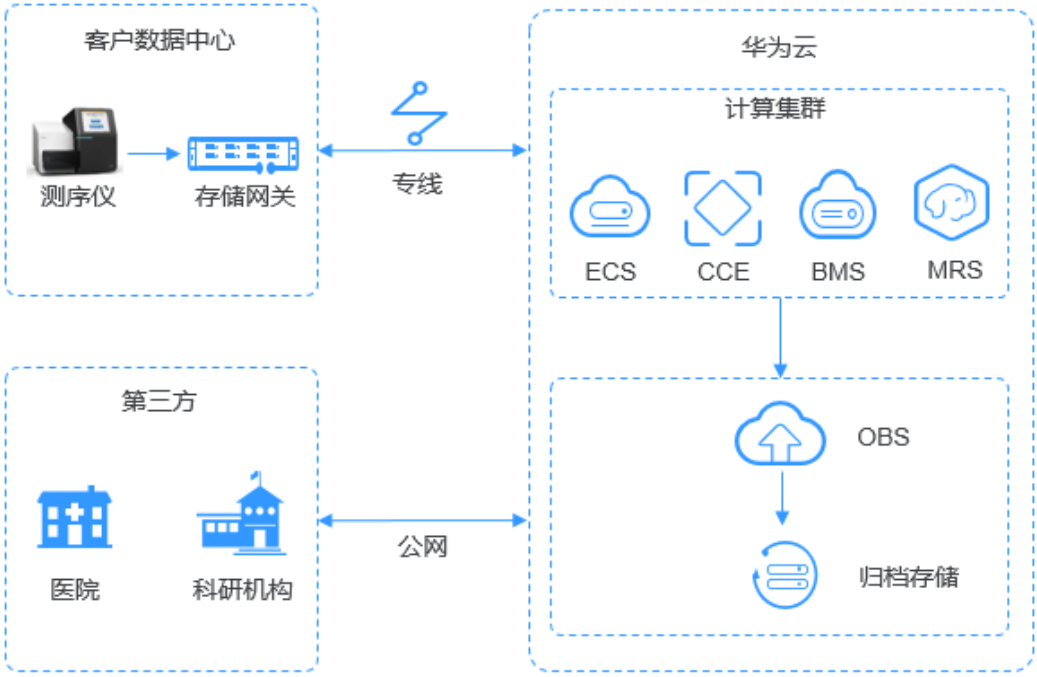
OBS提供高并发、高可靠、低时延、低成本的海量存储系统，结合计算服务可快速搭建高扩展性、低成本、高可用的基因测序平台。

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

建议搭配服务

弹性云服务器 ECS，裸金属服务器 BMS，MapReduce服务 MRS，云容器引擎 CCE，云专线 DC

图 3-4 基因测序



智能视频监控

场景描述

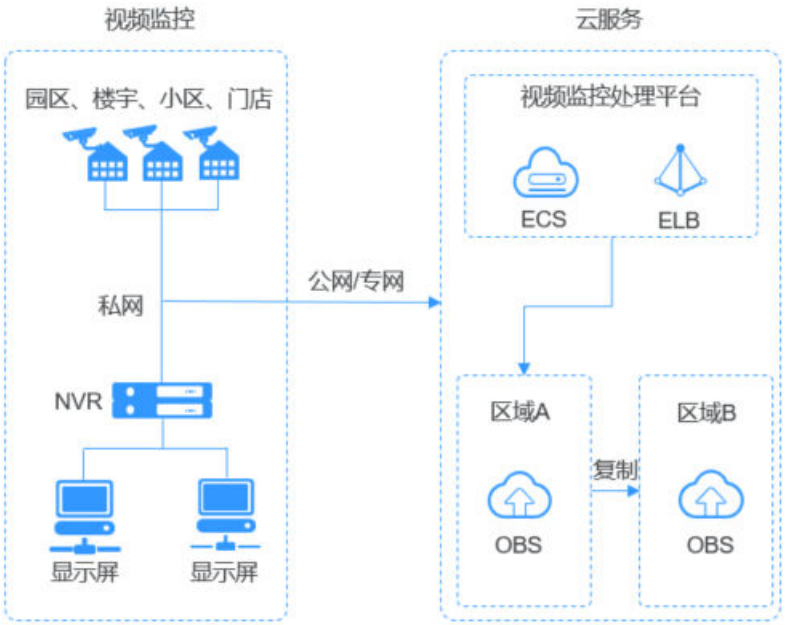
OBS为视频监控解决方案提供高性能、高可靠、低时延、低成本的海量存储空间，满足个人/企业等各类视频监控场景需求，提供设备管理、视频监控以及视频处理等多种能力的端到端解决方案。

摄像头拍摄的监控视频通过公网或**专线**传输至华为云，在弹性云服务器ECS和弹性负载均衡ELB组成的视频监控处理平台将视频流切片后存入OBS，后续再从OBS下载历史视频对象传输到观看视频的终端设备。存放在OBS中的视频文件还可以利用**跨区域复制**等功能进行备份，提升数据存储的安全性和可靠性。

建议搭配服务

弹性负载均衡 ELB，弹性云服务器 ECS

图 3-5 视频监控



备份归档

场景描述

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

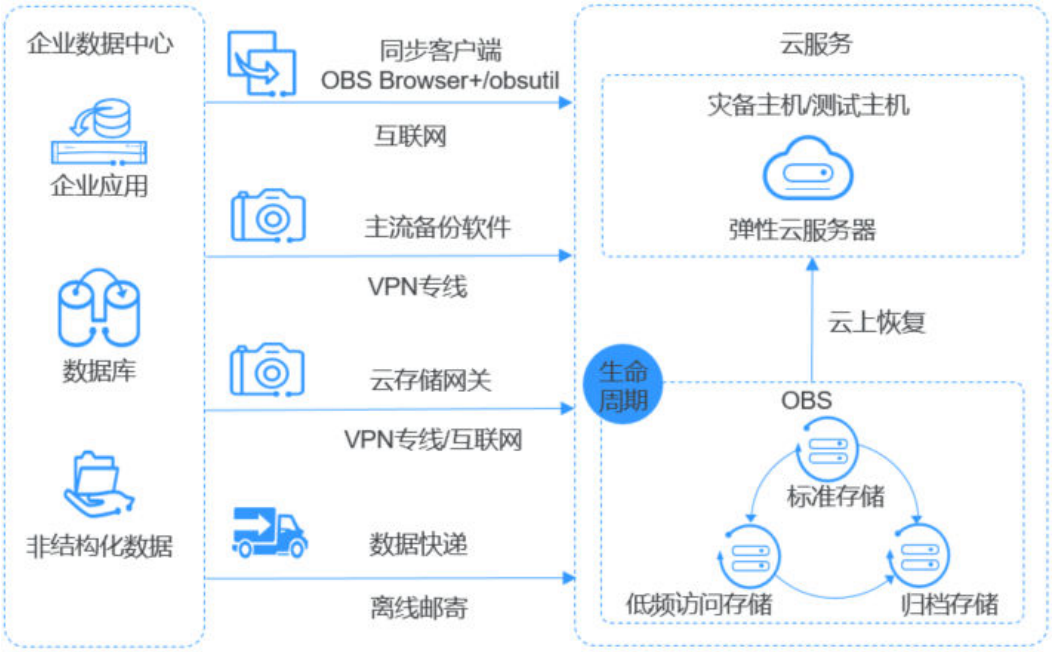
企业数据中心的各类数据通过使用同步客户端（如OBS Browser+、obsutil）、主流备份软件、云存储网关或数据快递服务DES，备份至对象存储服务OBS。OBS提供生命周期功能实现对象存储类别自动转换，以降低存储成本。在需要时，可将OBS中的数据恢复到云上的灾备主机或测试主机。

- 同步客户端：适用于单数据库/程序场景，手工备份，成本最低
- 备份软件：适用于多应用、多主机场景，自动备份，兼容性强
- 云存储网关：可无缝嵌入本地已有的备份系统
- 数据快递：适用于海量数据归档场景，离线邮寄上云

建议搭配服务

数据快递服务 DES，弹性云服务器 ECS

图 3-6 备份归档



HPC

场景描述

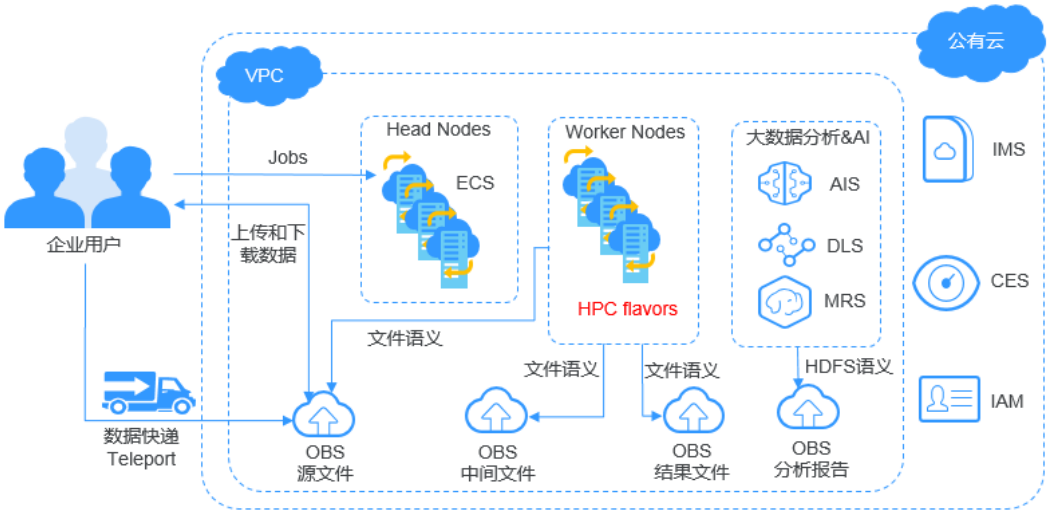
OBS配合弹性云服务器（ECS）、弹性伸缩（AS）、云硬盘（EVS）、镜像服务（IMS）、统一身份认证服务（IAM）和云监控服务（CES），为HPC提供大容量、大单流带宽、安全可靠的解决方案。

在HPC场景下，企业用户的数据可以通过直接上传或数据快递的方式上传到OBS。同时OBS提供的文件语义和HDFS语义支持将OBS直接挂载到HPC flavors的节点以及大数据&AI分析的应用下，为高性能计算各个环节提供便捷高效的数据读写和存储能力。

建议搭配服务

数据快递服务 DES，弹性云服务器 ECS，弹性伸缩 AS，镜像服务 IMS，云监控服务 CES，统一身份认证服务 IAM

图 3-7 HPC



企业云盘（网盘）

场景描述

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

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

建议搭配服务

弹性云服务器 ECS，弹性负载均衡 ELB，关系型数据库 RDS，云硬盘备份VBS

图 3-8 企业云盘（网盘）

4 产品功能

表4-1列出了对象存储服务OBS提供的常用功能特性。

在使用对象存储服务OBS之前，建议您先了解对象存储服务OBS的基本概念，以便更好地理解对象存储服务OBS提供的各项功能。

表 4-1 对象存储服务 OBS 功能概览

功能名称	功能描述	发布区域	OBS 2.0支持	OBS 3.0支持
存储类别	OBS提供了标准存储、低频访问存储、归档存储、深度归档存储（受限公测中）四种存储类别，满足不同场景下客户对存储性能和成本的不同诉求。	全部 （深度归档存储受限公测，仅支持土耳其-伊斯坦布尔）	√ （深度归档存储OBS 2.0暂不支持）	√
桶管理	桶是OBS中存储对象的容器。OBS提供创建、列举、搜索、查看、删除等基本功能，帮助您便捷的进行桶管理。	全部	√	√
对象管理	对象是OBS中数据存储的基本单位。OBS提供上传、下载、列举、搜索、断点续传、多段操作等基本功能，满足您各个场景的对象管理需求。	全部	√	√
权限管理	OBS通过IAM权限、桶/对象策略和ACL三种方式配合进行权限管理。您可以对不同的账号和用户授予不同的访问权限，也可以对桶和对象设置不同的策略及ACL来控制桶和对象的读写权限。	全部	√	√

功能名称	功能描述	发布区域	OBS 2.0支持	OBS 3.0支持
服务端加密	您可以将数据加密后存储到OBS中，提高数据的安全性。OBS提供SSE-KMS、SSE-OBS和SSE-C三种服务端加密方式。	支持的区域请参见功能总览。 **说明** 服务端加密方式SSE-KMS和SSE-OBS分别支持的区域详情请在用户指南服务端加密查看。	√	√
WORM	您可以为对象设置WORM策略，以保护对象在指定时间内不被删除，不被篡改。	支持的区域请参见功能总览。	×	√
生命周期管理	您可以通过生命周期规则来管理对象的生命周期，例如定期将桶中的对象删除或者转换对象的存储类别。	全部	√	√
静态网站托管	您可以将静态网站文件上传至OBS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，以实现在OBS上托管静态网站。	全部	√	√
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。OBS支持CORS规范，允许跨域请求访问OBS中的资源。	全部	√	√
防盗链	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，同时支持访问白名单和访问黑名单的设置。	全部	√	√

功能名称	功能描述	发布区域	OBS 2.0支持	OBS 3.0支持
桶标签	桶标签用于标识OBS中的桶，以此来达到对OBS中的桶进行分类的目的。当为桶添加标签时，该桶上所有请求产生的计费话单里都会带上这些标签，从而可以针对话单报表做分类筛选，进行更详细的成本分析。	全部	√	√
自定义域名	您可以将自定义域名绑定到OBS桶，然后使用自定义域名访问桶中的数据。例如，您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，此时可以使用自定义域名绑定功能。	全部	×	√
跨区域复制	您可以创建跨区域复制规则，将您账号下一个桶（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。	全部	×	√
图片处理	您可以使用图片处理功能对存放在OBS中的图片进行瘦身、剪切、缩放、增加水印、转换格式等操作，并且可以快速获取到处理后的图片。	支持的区域请参见功能总览。	×	√
桶清单	您可以配置一个清单规则，定期扫描桶中指定的对象或拥有相同前缀的对象，生成这些对象的元数据内容，如对象大小、修改时间、存储类别等，并以CSV格式保存到指定的桶中。	支持的区域请参见功能总览。	×	√

功能名称	功能描述	发布区域	OBS 2.0支持	OBS 3.0支持
并行文件系统	并行文件系统（Parallel File System）是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。您可以按照标准的OBS接口读取并行文件系统中的数据，也可以利用obsfs工具将创建的并行文件系统挂载到云端Linux服务器上，并能像操作本地文件系统一样对并行文件系统内的文件和目录进行在线处理。	支持的区域请参见功能总览。	×	√
日志管理	您可以通过日志管理功能获取桶的访问数据。开启日志管理功能后，桶的每次操作将会产生一条日志，并将多条日志打包成一个日志文件保存在目标桶中，您可以基于日志文件进行请求分析或日志审计。	全部	√	√
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。	全部	√	√
追加写对象	您可以通过AppendObject接口在指定桶内的一个Appendable对象尾追加上传数据。通过AppendObject创建的对象为Appendable对象，通过PutObject创建的对象是Normal对象。	支持的区域请参见功能总览。	×	√
自定义元数据	您可以添加、修改或删除桶中已上传对象的元数据。	全部	√	√
桶配额	您可以设置桶空间配额，用以限制单个桶可存储的最大数据量，最大可设置为2^{63}-1，单位Byte（字节）。新创建的桶默认不限制配额。	全部	√	√

功能名称	功能描述	发布区域	OBS 2.0支持	OBS 3.0支持
归档数据直读	您可以开启桶归档数据直读，实现存储类别为归档存储的对象可以直接下载，无需提前恢复。归档数据直读会收取相应的费用。	支持的区域请参见功能总览。	×	√
对象分享	您可以将存放在OBS中的文件或文件夹以临时URL的形式分享给所有用户。分享强调临时性，所有分享的URL都是临时URL，存在有效期。	支持的区域请参见功能总览。	√	√
碎片管理	您可以通过桶的碎片管理功能，对多段上传时某些特殊情况下产生的碎片进行清理，以节省存储空间。	全部	√	√
企业项目	您可以在创建桶时指定桶所属的企业项目，更方便的进行桶资源和权限管理。	支持的区域请参见功能总览。	×	√
桶加密	您可以为桶配置默认加密，配置后，上传到桶中的对象都会自动进行加密。	支持的区域请参见功能总览。	×	√
多AZ	您可以在创桶的时候选择将桶中数据冗余存储在多个可用区，以获得更高的数据可靠性。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。	支持的区域请参见功能总览。	×	√
数据回源	您可以利用数据回源功能，实现向OBS请求数据不存在时，通过回源规则自动从源站获取对应数据。	支持的区域请参见功能总览。	×	√
在线解压	OBS支持在线解压。您可以将批量文件打包成ZIP包后上传至OBS，上传之后压缩包可以自动解压。	支持的区域请参见功能总览。	×	√
桶配置信息复制	OBS提供了桶配置信息复制功能，方便您在创建新桶之后，快速将已有桶的配置信息复制到新桶中。支持复制的配置信息包括：桶策略、CORS规则、生命周期规则、数据回源规则、图片处理样式、在线解压规则。	全部	×	√

功能名称	功能描述	发布区域	OBS 2.0支持	OBS 3.0支持
委托	您可以通过IAM委托其他云服务或华为云账号管理您的OBS资源。	全部	×	√
监控	您可以通过OBS控制台或者云监控服务（Cloud Eye）控制台监控桶的流量统计和请求次数等指标，方便您及时了解目前资源的使用状况、并合理规划使用计划。	支持的区域请参见功能总览。	√	√
审计	您可以通过云审计服务（CTS）对OBS中桶和对象的各类事件操作记录进行收集、存储和查询，用于安全分析、合规审计、资源跟踪和问题定位等。	全部	√	√
工具	OBS提供OBS Browser+、obsutil、obsfs等多种实用工具，满足不同场景下数据迁移和数据管理需求。	全部	√	√
API	OBS提供了REST（Representational State Transfer）风格API，支持您通过HTTP/HTTPS请求调用，实现创建、修改、删除桶，上传、下载、删除对象等操作。	全部	√	√
SDK	OBS提供多种开发语言的SDK，帮助您轻松实现二次开发。目前支持：Java、Python、C、Go、BrowserJS、.NET、Android、IOS、PHP、Node.js	全部	√	√

5 安全

5.1 责任共担

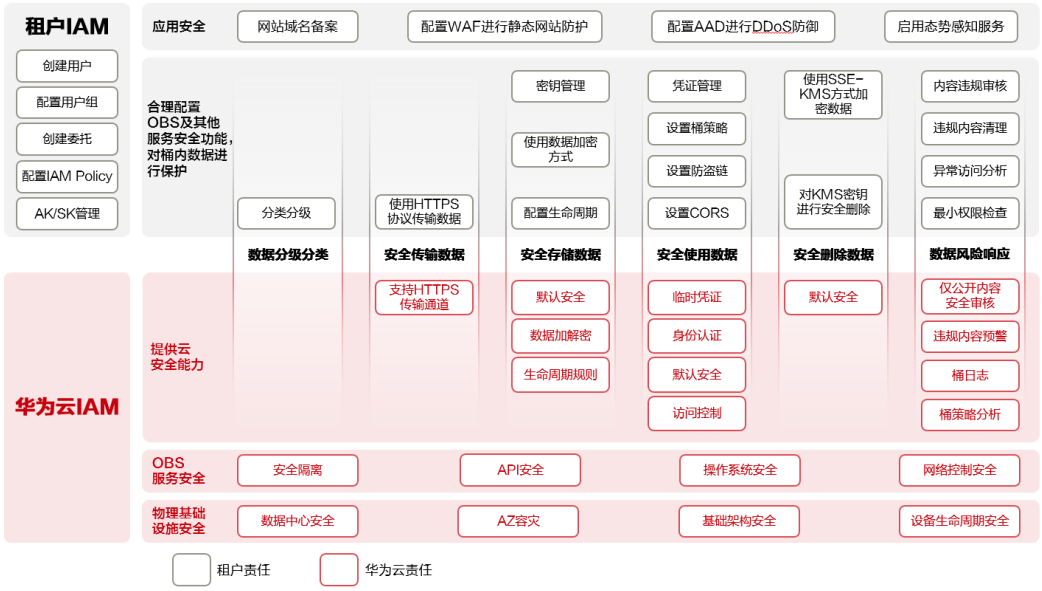
华为云秉承“将公司对网络和业务安全性保障的责任置于公司的商业利益之上”。针对层出不穷的云安全挑战和无孔不入的云安全威胁与攻击，华为云在遵从法律法规业界标准的基础上，以安全生态圈为护城河，依托华为独有的软硬件优势，构建面向不同区域和行业的完善云服务安全保障体系。

安全性是华为云与您的共同责任，如图5-1所示。

- **华为云**：负责云服务**自身**的安全，提供安全的云。华为云的安全责任在于保障其所提供的 IaaS、PaaS 和 SaaS 类云服务自身的安全，涵盖华为云数据中心的物理环境设施和运行其上的基础服务、平台服务、应用服务等。这不仅包括华为云基础设施和各项云服务技术的安全功能和性能本身，也包括运维运营安全，以及更广义的安全合规遵从。
- **租户**：负责云服务**内部**的安全，安全地使用云。华为云租户的安全责任在于对使用的 IaaS、PaaS 和 SaaS 类云服务内部的安全以及对租户定制配置进行安全有效的管理，包括但不限于虚拟网络、虚拟主机和访客虚拟机的操作系统，虚拟防火墙、API 网关和高级安全服务，各项云服务，租户数据，以及身份账号和密钥管理等方面的安全配置。

《华为云安全白皮书》《华为云安全白皮书》详细介绍华为云安全性的构建思路与措施，包括云安全战略、责任共担模型、合规与隐私、安全组织与人员、基础设施安全、租户服务与租户安全、工程安全、运维运营安全、生态安全。

图 5-1 华为云安全责任共担模型



5.2 身份认证与访问控制

身份认证

用户访问OBS的方式有多种，包括OBS控制台、OBS客户端（OBS Browser+）、OBS命令行工具（obsutil）、API、SDK，无论访问方式封装成何种形式，其本质都是通过OBS提供的REST风格的API接口进行请求。

OBS的接口既支持认证请求，也支持匿名请求。匿名请求通常仅用于需要公开访问的场景，例如静态网站托管。除此之外，绝大多数场景是需要经过认证的请求才可以访问成功。经过认证的请求总是需要包含一个签名值，该签名值以请求者的访问密钥（AK/SK）作为加密因子，结合请求体携带的特定信息计算而成。通过访问密钥（AK/SK）认证方式进行认证鉴权，即使用Access Key ID（AK）/Secret Access Key（SK）加密的方法来验证某个请求发送者身份。关于访问密钥的详细介绍及获取方式，请参见**访问密钥（AK/SK）**。

OBS支持如下请求方式：

- **通过永久访问密钥访问OBS**
- **通过临时访问密钥访问OBS**
- **通过临时URL访问OBS**
- **通过IAM委托访问OBS**

访问控制

OBS支持通过权限控制（IAM权限、桶策略、ACL）、防盗链和跨域资源共享（CORS）进行访问控制。

表 5-1 OBS 访问控制

访问控制方式		简要说明	详细介绍
权限控制	IAM权限	IAM权限是作用于云资源的，IAM权限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。管理员创建IAM用户后，需要将用户加入到一个用户组中，IAM可以对这个组授予OBS所需的权限，组内用户自动继承用户组的所有权限。	IAM权限介绍
	桶策略	桶策略是作用于所配置的OBS桶及桶内对象的。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精确的操作权限，是对桶ACL和对象ACL的补充（更多场景下是替代）。	桶策略介绍
	ACL	访问控制列表（Access Control List，ACL）是一个指定被授权者和所授予权限的授权列表。OBS桶和对象的ACL是基于账号或用户组的访问控制，默认情况下，创建桶和对象时会同步创建ACL，系统会授予拥有者桶和对象资源的完全控制权限。桶或对象的拥有者可以通过ACL向指定账号或用户组授予桶或对象基本的读、写权限。	ACL介绍
防盗链		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，同时支持访问白名单和访问黑名单的设置。	防盗链介绍
跨域资源共享（CORS）		OBS支持在桶上配置跨域规则，允许或禁止某些网站的跨域请求。	CORS介绍

5.3 数据保护技术

OBS通过多种数据保护手段和特性，保障存储在OBS中的数据安全可靠。

表 5-2 OBS 的数据保护手段和特性

数据保护手段	简要说明	详细介绍
传输加密（HTTPS）	OBS支持HTTP和HTTPS两种传输协议，为保证数据传输的安全性，推荐您使用更加安全的HTTPS协议。	构造请求

数据保护手段	简要说明	详细介绍
数据冗余存储	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。 OBS创建桶时支持选择数据冗余存储策略，选择多AZ存储时，数据冗余存储在同区域的多个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。	创建多AZ桶
数据完整性校验（MD5）	对象数据在上传下载过程中，有可能会因为网络劫持、数据缓存等原因，存在数据不一致的问题。OBS提供通过计算MD5值的方式对上传下载的数据进行一致性校验。	数据一致性校验
服务端加密	当启用服务端加密功能后，用户上传对象时，数据会在服务端加密成密文后存储。用户下载加密对象时，存储的密文会先在服务端解密为明文，再提供给用户。	服务端加密介绍和配置方法
跨区域复制	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。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。	跨区域复制介绍和配置方法
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。	多版本控制介绍和配置方法
敏感操作保护	OBS控制台支持敏感操作保护，开启后执行删除桶等敏感操作时，系统会进行身份验证，进一步保证OBS配置和数据的安全性。	敏感操作保护介绍

5.4 审计与日志

审计

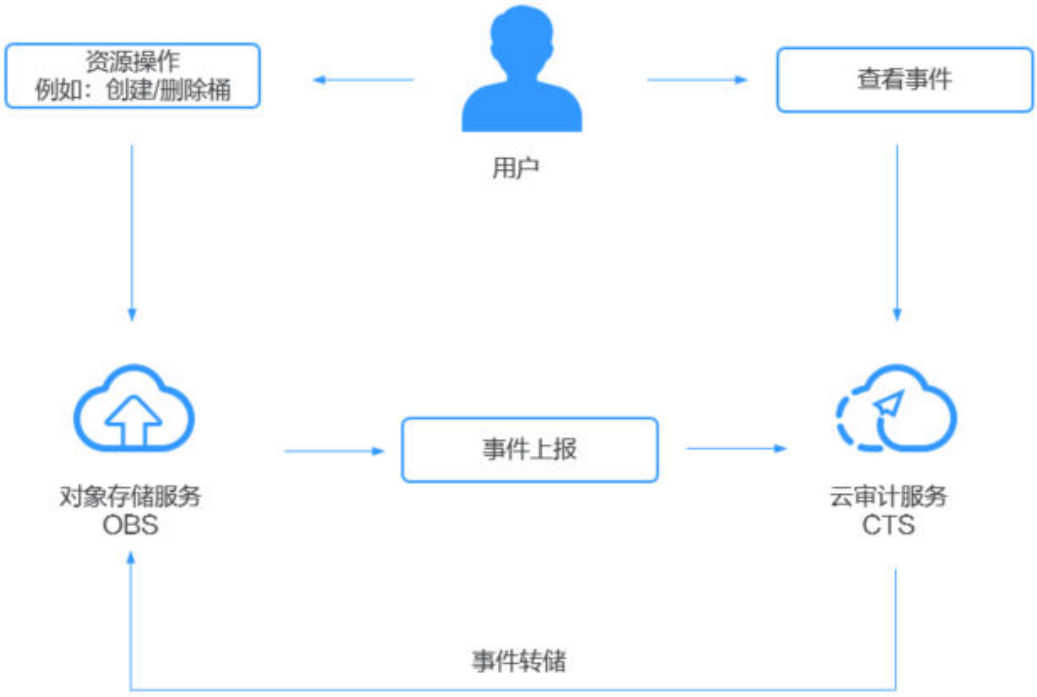
云审计服务（Cloud Trace Service，CTS），是华为云安全解决方案中专业的日志审计服务，提供对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、合规审计、资源跟踪和问题定位等常见应用场景。

用户开通云审计服务并创建和配置追踪器后，CTS可记录OBS的管理事件和数据事件用于审计。

CTS的详细介绍和开通配置方法，请参见**CTS快速入门**。

CTS支持追踪的OBS管理事件和数据事件列表，请参见**审计**。

图 5-2 云审计服务



日志

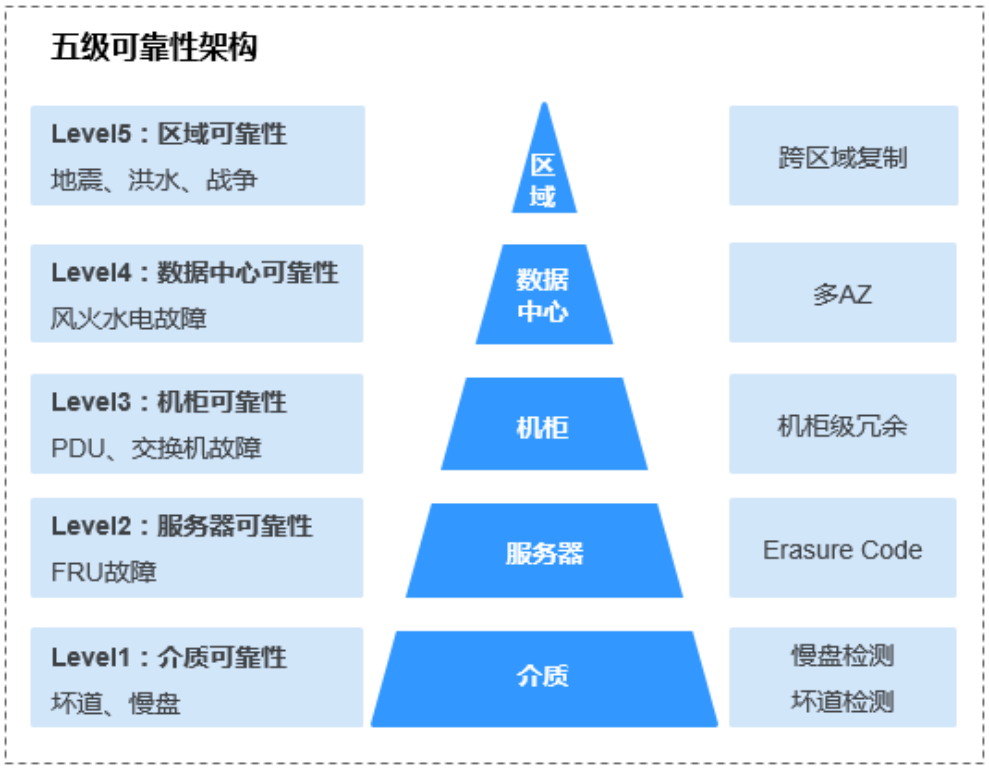
出于分析或审计等目的，用户可以开启桶的日志记录功能。通过访问日志记录，桶的拥有者可以深入分析访问该桶的用户请求性质、类型或趋势。当用户开启一个桶的日志记录功能后，OBS会自动对这个桶的访问请求记录日志，并生成日志文件写入用户指定的桶中。

关于OBS日志记录的详细介绍和配置方法，请参见**日志记录**。

5.5 服务韧性

OBS提供五级可靠性架构，通过跨区域复制、AZ之间数据容灾、AZ内设备和数据冗余、存储介质的慢盘/坏道检测等技术方案，保障数据的持久性和可靠性。

图 5-3 五级可靠性架构保证数据稳定，业务可靠



5.6 监控安全风险

OBS提供基于云监控服务CES的资源和操作监控能力，帮助用户监控账号下的OBS桶，执行自动实时监控、告警和通知操作。用户可以实时掌握桶中所产生的各类请求、流量、带宽、错误响应和存储用量等信息。

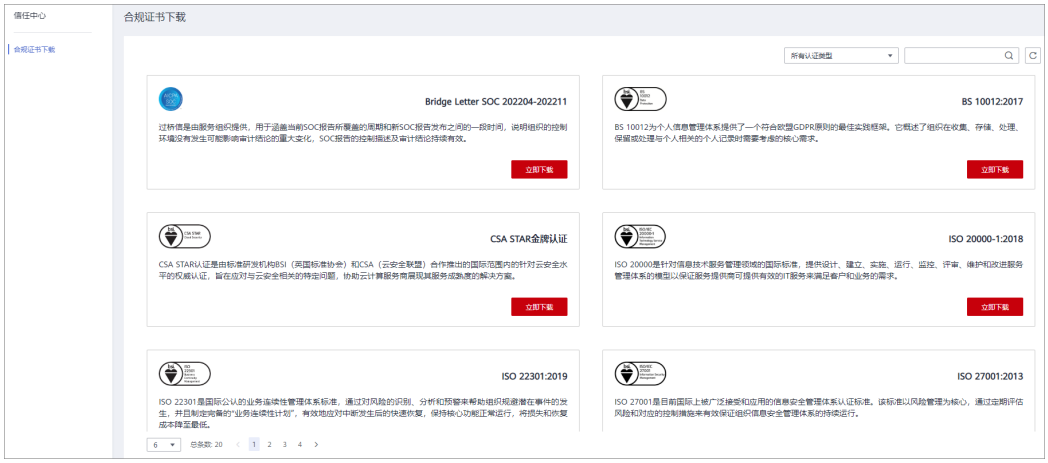
关于OBS支持的监控指标，以及如何创建监控告警规则等内容，请参见**监控**。

5.7 认证证书

合规证书

华为云服务及平台通过了多项国内外权威机构（ISO/SOC/PCI等）的安全合规认证，用户可自行**申请下载**合规资质证书。

图 5-4 合规证书下载



资源中心

华为云还提供以下资源来帮助用户满足合规性要求，具体请查看**资源中心**。

图 5-5 资源中心

6 权限管理

如果您需要对购买的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，您可以在华为云账号中给员工创建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。

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

IAM是华为云提供权限管理的基础服务，无需付费即可使用，您只需要为您账号中的资源进行付费。关于IAM的详细介绍，请参见**《IAM产品介绍》**。

OBS 权限

默认情况下，管理员创建的IAM用户没有任何权限，需要将其加入用户组，并给用户组授予策略和角色，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，用户就可以基于被授予的权限对云服务进行操作。

OBS部署时不区分物理区域，为全局级服务。授权时，在全局级服务中设置权限，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。由于华为云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，OBS支持的API授权项请参见**权限和授权项说明**。

说明

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

表6-1为OBS的所有系统权限。

表 6-1 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
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 Buckets Viewer	拥有该权限的用户可以执行列举桶、获取桶基本信息、获取桶元数据的操作。	系统角色	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。 **说明** 拥有该权限的用户如果在控制台上列举对象失败，可能是因为桶中存在多版本对象。此时需要额外授予该用户列举多版本对象的权限（obs:bucket:ListBucketVersions），才能在控制台正常看到对象列表。	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。 **说明** 拥有该权限的用户如果在控制台上列举对象失败，可能是因为桶中存在多版本对象。此时需要额外授予该用户列举多版本对象的权限（obs:bucket:ListBucketVersions），才能在控制台正常看到对象列表。	系统策略	无

表6-2列出了OBS常用操作与系统权限的授权关系，您可以参照该表选择合适的系统权限。

表 6-2 OBS 操作与资源权限关系

操作名称	Tenant Administrator	Tenant Guest	OBS Administrator	OBS Buckets Viewer	OBS ReadOnlyAccess	OBS Operate Access
列举桶	可以	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	不可以
删除桶	可以	不可以	可以	不可以	不可以	不可以
获取桶基本信息	可以	可以	可以	可以	可以	可以
管理桶访问权限	可以	不可以	可以	不可以	不可以	不可以
管理桶策略	可以	不可以	可以	不可以	不可以	不可以
修改桶存储类别	可以	不可以	可以	不可以	不可以	不可以
列举对象	可以	可以	可以	不可以	可以	可以
列举多版本对象	可以	可以	可以	不可以	不可以	不可以
上传文件	可以	不可以	可以	不可以	不可以	可以
新建文件夹	可以	不可以	可以	不可以	不可以	可以
删除文件	可以	不可以	可以	不可以	不可以	可以
删除文件夹	可以	不可以	可以	不可以	不可以	可以
下载文件	可以	可以	可以	不可以	不可以	可以
删除多版本文件	可以	不可以	可以	不可以	不可以	可以
下载多版本文件	可以	可以	可以	不可以	不可以	可以
修改对象存储类别	可以	不可以	可以	不可以	不可以	不可以
恢复文件	可以	不可以	可以	不可以	不可以	不可以
取消删除文件	可以	不可以	可以	不可以	不可以	可以
删除碎片	可以	不可以	可以	不可以	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	不可以

操作名称	Tenant Administrator	Tenant Guest	OBS Administrator	OBS Buckets Viewer	OBS ReadOnlyAccess	OBS Operate Access
设置对象元数据	可以	不可以	可以	不可以	不可以	不可以
获取对象元数据	可以	可以	可以	不可以	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	不可以
管理日志记录	可以	不可以	可以	不可以	不可以	不可以
管理标签	可以	不可以	可以	不可以	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	不可以
管理静态网站托管	可以	不可以	可以	不可以	不可以	不可以
管理CORS规则	可以	不可以	可以	不可以	不可以	不可以
管理防盗链	可以	不可以	可以	不可以	不可以	不可以
域名管理	可以	不可以	可以	不可以	不可以	不可以
管理跨区域复制	可以	不可以	可以	不可以	不可以	不可以
管理图片处理	可以	不可以	可以	不可以	不可以	不可以
追加写对象	可以	不可以	可以	不可以	不可以	可以
设置对象ACL	可以	不可以	可以	不可以	不可以	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	不可以
获取对象ACL	可以	可以	可以	不可以	不可以	可以
获取指定版本对象ACL	可以	可以	可以	不可以	不可以	可以
多段上传	可以	不可以	可以	不可以	不可以	可以

操作名称	Tenant Administrator	Tenant Guest	OBS Administrator	OBS Buckets Viewer	OBS ReadOnlyAccess	OBS Operate Access
列举已上传段	可以	可以	可以	不可以	不可以	可以
取消多段上传任务	可以	不可以	可以	不可以	不可以	可以
在线解压	可以	不可以	不可以	不可以	不可以	不可以

OBS 资源权限管理

OBS桶和对象的权限可以通过IAM用户权限、桶策略和ACL共同控制。

更多关于OBS资源权限管理的内容请参见**权限管理**。

OBS 控制台功能依赖的权限

表 6-3 OBS 控制台依赖服务的角色或策略

控制台功能	依赖服务	需配置角色/策略
获取已有域名列表（在配置自定义域名和加速域名时，获取在华为云已有的域名列表）	域名注册服务 Domains	需要增加Domains:domains:getDetails权限后才能访问已有的域名列表。
设置镜像回源规则	对象存储服务 OBS	• 需要增加Tenant Administrator权限后才能设置镜像回源规则 • 镜像回源需使用IAM委托功能，创建云服务委托，委托OBS获取源站数据。委托需要给OBS服务授予obs:object:HeadObject、obs:object:PutObject权限。 • 如果桶开启了SSE-KMS服务端加密功能，对OBS的云服务委托中还需要配置kms:cmk:get、kms:cmk:list、kms:cmk:create、kms:dek:create、kms:dek:crypto、kms:dek:crypto权限。
获取镜像回源规则	对象存储服务 OBS	需要增加Tenant Administrator权限后才能获取镜像回源规则
删除镜像回源规则	对象存储服务 OBS	需要增加Tenant Administrator权限后才能删除镜像回源规则
设置在线解压策略	对象存储服务 OBS	需要增加Tenant Administrator权限后才能设置在线解压策略

控制台功能	依赖服务	需配置角色/策略
获取在线解压策略	对象存储服务 OBS	需要增加Tenant Administrator权限后才能获取在线解压策略
删除在线解压策略	对象存储服务 OBS	需要增加Tenant Administrator权限后才能删除在线解压策略
服务端加密	密钥管理服务 KMS	当桶或者桶内对象开启了SSE-KMS服务端加密功能，需要为请求者配置kms:cmk:get、kms:cmk:list、kms:cmk:create、kms:dek:create、kms:dek:crypto、kms:dek:crypto权限，才能上传下载对象。

相关链接

- **IAM产品介绍**
- **IAM基础概念**
- **创建用户组、用户并授予OBS对象存储权限**
- **细粒度策略支持的授权项**

7 约束与限制

本章介绍OBS一些主要特性的使用限制。

表 7-1 OBS 使用限制

限制项	说明
带宽	单个华为云账号默认的读写（GET/PUT）带宽上限是16Gbit/s。如果带宽达到该阈值，请求会触发流控。 如果您的业务有更大的带宽需求，请**提交工单**申请。
每秒请求数（Query Per Second, QPS）	• 单个华为云账号默认的写请求（PUT Object）上限是6000请求每秒。 • 单个华为云账号默认的读请求（GET Object）上限是10000请求每秒。 • 单个华为云账号默认的列举类请求（LIST）上限是1000请求每秒。 **说明** 如果用户在对象命名规则上使用了顺序前缀（如时间戳或字母顺序），可能导致大量对象的请求访问集中于某个特定分区，造成访问热点。会使热点分区上的请求速率受限，访问时延上升。 推荐使用随机前缀对象名，这样请求就会均匀分布在多个分区，达到水平扩展的效果。使用随机前缀对象名的方法，请参见**性能优化最佳实践**。 如果您的业务有更大的QPS需求，请**提交工单**申请。

限制项	说明
资源包	• 资源包为区域专属，不支持共享给其他区域使用，请根据资源所在地谨慎选择。 • OBS只对部分计费项提供了资源包，其他计费项支持按需计费模式。详情请参见**计费说明**。 • 当月使用量超出已购资源包的额度，将自动转为按需计费。新购资源包不能抵扣已产生的资源用量。 • 资源包类型需要和桶的数据冗余存储策略（单AZ存储、多AZ存储）以及桶的存储类别（标准存储、低频访问存储、归档存储、深度归档）相匹配，否则会产生按需计费。 • 购买的标准存储包、归档存储包和公网流出流量包可同时应用于并行文件系统和对象存储桶。由于并行文件系统暂时不支持跨区域复制和回源，所以无法使用对应流量包。
访问规则	OBS基于DNS解析性能和可靠性的考虑，要求凡是携带桶名的请求，在构造URL的时候都必须将桶名放在domain前面，形成三级域名形式，又称为虚拟主机访问域名。 例如，如果您有一个位于ap-southeast-1区域的名为test-bucket的桶，期望访问桶中一个名为test-object对象的acl，正确的访问URL为https://test-bucket.obs.ap-southeast-1.myhuaweicloud.com/test-object?acl
桶	• 在OBS中，桶名必须是全局唯一的且不能修改，即用户创建的桶不能与自己已创建的其他桶名称相同，也不能与其他用户创建的桶名称相同。 • 桶创建成功后，桶名、所属区域和数据冗余存储策略均不允许修改。 • 一个账号及账号下的所有IAM子用户可创建的桶+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。例如，建议在桶内根据对象前缀划分不同的目录，通过**细粒度权限控制**实现不同目录在不同业务部门之间的权限隔离。 • 默认情况下，OBS系统和单个桶都没有总数据容量和对象数量的限制。 • 删除桶之前必须确保桶内所有对象已彻底删除。 • 用户删除桶后，需要等待30分钟才能创建同名桶和并行文件系统。
桶清单	详见**桶清单简介**

限制项	说明
上传对象	• 通过OBS管理控制台上传的文件有大小和数量限制。 – 在部分支持批量上传的区域，每次最多支持100个文件同时上传，总大小不超过5GB。如果只上传1个文件，则这个文件最大为5GB。 – 在部分不支持批量上传的区域，每次只能上传1个文件，大小不超过50MB。 • OBS Browser+、obsutil、API和SDK上传的单个对象最大是48.8TB。 • 支持批量上传功能需要满足以下条件： 1. OBS桶所在区域支持批量上传功能。 2. OBS桶的版本号为“3.0”。 • 在未开启多版本控制功能的情况下，如果新上传的文件和桶内文件重名，则新上传的文件会自动覆盖老文件，且不会保留老文件的ACL等信息；如果新上传的文件夹和桶内文件夹重名，则上传后会将新老文件夹合并，合并过程如遇重名文件，会使用新上传的文件夹中的文件进行覆盖。 • 在开启了多版本控制功能的情况下，如果新上传的文件和桶内文件重名，则会在老文件上新增一个版本。 • 对象键（对象名）虽然可以使用任何UTF-8字符，但是建议按照**对象键命名指导原则**进行命名，有助于最大程度符合DNS、Web安全字符、XML分析器和其他API的要求。
删除对象	桶没有开启多版本控制功能时，对象删除后不可恢复，请谨慎操作。
深度归档存储（受限公测中）	• 转为深度归档对象之后的追加写对象不支持追加写。 • 不支持批量恢复。
恢复归档或深度归档存储对象	• 归档存储或深度归档存储的对象正在恢复的过程中，不允许暂停或删除恢复任务。 • 对象的恢复状态为恢复中时，对象不能再次恢复。 • 数据恢复后，会产生一个标准存储类别的对象副本，即对象同时存在标准存储类别的对象副本和归档或深度归档存储类别的对象。在恢复的有效期内，会同时收取这份数据在标准存储和归档存储或深度归档存储中的存储费用。恢复有效期到期后标准存储类别的对象副本会自动删除。
生命周期管理	单个桶的生命周期规则条数没有限制，但一个桶中所有生命周期规则的XML描述总大小不能超过20KB。
跨区域复制	详见**跨区域复制简介**

限制项	说明
自定义域名绑定	• 桶版本号为3.0及以上的桶支持自定义绑定域名功能。 • 每个桶默认最多绑定20个自定义域名，部分区域支持最多绑定30个自定义域名（如华南-广州），各区域支持绑定的最大值请以控制台自定义域名绑定页面的实际规格为准。 • OBS自定义域名绑定暂时不支持HTTPS访问自定义域名，只支持HTTP访问自定义域名。 客户自定义域名绑定成功后，如果想使用HTTPS进行访问，需同时使用CDN，通过CDN管理控制台进行HTTPS证书管理，即可使用HTTPS访问。 CDN管理控制台HTTPS证书管理方式，详情请参见**HTTPS配置**。 • 一个自定义域名只能绑定到一个桶域名上。 • 绑定的自定义域名后缀目前支持的范围为2~6个英文大小写字母。
数据回源	详见**数据回源简介**
ACL	• 一个桶的桶ACL最多支持100条授权，所有桶ACL策略大小总和不超过50KB。 • 一个对象的对象ACL最多支持100条授权，所有对象ACL策略大小不超过50KB。
桶策略	单个桶的桶策略条数（statement）没有限制，但一个桶中所有桶策略的JSON描述总大小不能超过20KB。
并行文件系统	详见**《并行文件系统特性指南》**
图片处理	详见**《图片处理特性指南》**

8 与其他服务的关系

表 8-1 与其他服务的关系

交互功能	相关服务	位置
通过相关服务将数据迁移到OBS	云专线（Direct Connect，DC）	搬迁本地数据至OBS_云专线方式
在ECS上实现通过华为云内网访问OBS	弹性云服务器（Elastic Cloud Server，ECS）	在ECS上通过内网访问OBS
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）	用户权限 设置用户权限
通过CES服务监控桶的上传流量、下载流量、GET类请求次数、PUT类请求次数、GET类请求首字节平均时延、4xx异常次数和5xx异常次数。	云监控服务（Cloud Eye Service）	Cloud Eye控制台监控指标
通过CTS服务收集OBS资源操作记录，便于日后的查询、审计和回溯。	云审计服务（Cloud Trace Service，CTS）	审计
标签用于标识OBS中的桶，以实现对OBS中的桶进行分类。	标签管理服务（Tag Management Service，TMS）	标签
通过密钥管理KMS功能对上传到OBS中的文件进行加密。	数据加密服务（Data Encryption Workshop, DEW）	服务端加密
通过CDN服务为OBS桶绑定的自定义域名加速。	CDN（Content Delivery Network，内容分发网络）	自定义域名绑定

交互功能	相关服务	位置
通过DNS服务为托管在OBS上的静态网站做域名解析。	云解析服务（Domain Name Service，DNS）	**使用自定义域名托管静态网站** **自定义域名绑定**

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），云审计服务（Cloud Trace Service，CTS）等。

9 基本概念

9.1 对象

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

对象包括了Key，Metadata，Data三部分：

- Key：键值，即对象的名称，为经过UTF-8编码的长度大于0且不超过1024的字符序列。一个桶里的每个对象必须拥有唯一的对象键值。
- Metadata：元数据，即对象的描述信息，包括系统元数据和用户元数据，这些元数据以键值对（Key-Value）的形式被上传到OBS中。
  - 系统元数据由OBS自动产生，在处理对象数据时使用，包括Date，Content-length，Last-modify，ETag等。
  - 用户元数据由用户在上传对象时指定，是用户自定义的对象描述信息。
- Data：数据，即文件的数据内容。

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

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

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

对象的相关操作请参见**对象管理**。

9.2 桶

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

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

对象存储服务设置有四类桶存储类别，分别为：标准存储、低频访问存储、归档存储、深度归档存储（受限公测中），从而满足客户业务对存储性能、成本的不同诉求。创建桶时可以指定桶的存储类别，桶的存储类别可以修改。

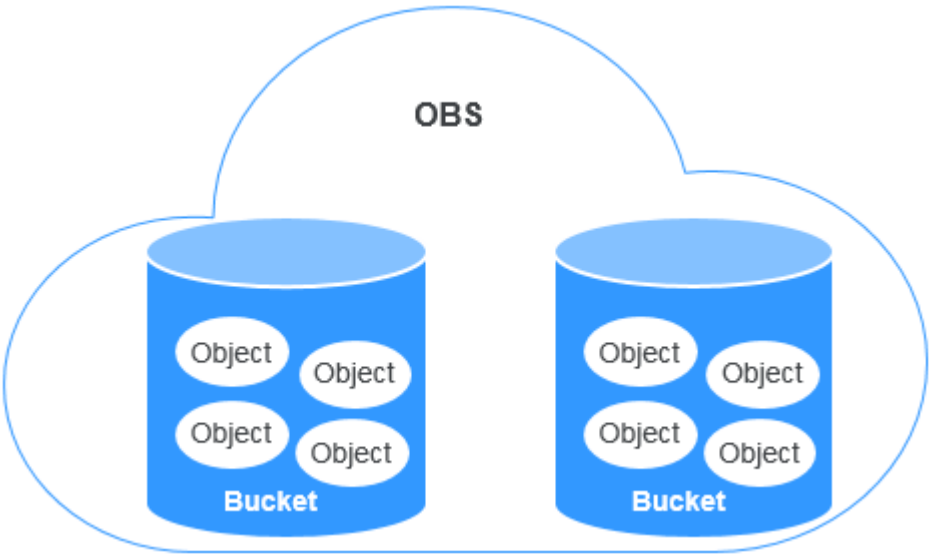
在OBS中，桶名必须是全局唯一的且不能修改，即用户创建的桶不能与自己已创建的其他桶名称相同，也不能与同账号、其他账号及账号下的所有IAM子用户创建的桶名称相同。桶所属的区域在创建后也不能修改。每个桶在创建时都会生成默认的桶ACL（Access Control List，访问控制列表），桶ACL的每项包含了对被授权用户授予什么样的权限，如读取权限、写入权限等。用户只有对桶有相应的权限，才可以对桶进行操作，如创建、删除、显示、设置桶ACL等。

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9-1**所示：

图 9-1 桶和对象



桶的相关操作请参见**桶管理**。

9.3 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。

也支持通过部署在弹性云服务器中的PFS客户端（obsfs工具），按照POSIX文件语义读写数据；通过obsfs用户可以将创建的并行文件系统挂载到云端Linux服务器上并能像操作本地文件系统一样对并行文件系统内的文件和目录进行在线处理，包括：创建、删除文件/目录，重命名文件/目录，修改写文件等操作。

并行文件系统的详细介绍和使用说明，请参见《并行文件系统特性指南》。

9.4 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，是您的长期身份凭证，您可以通过访问密钥对**API的请求进行签名**。华为云通过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 9-1 OBS 资源管理工具

工具	AK/SK配置方式
OBS Browser+	在配置登录账号时配置AK和SK，详情请参见**登录OBS Browser+**。
obsutil	在初始化配置时配置AK和SK，详情请参见**初始化配置**。
obsfs	在初始化配置时配置AK和SK，详情请参见**初始化配置**。
SDK	在初始化阶段设置AK和SK。详情请见**SDK参考**。

工具	AK/SK配置方式
API	在计算签名时添加AK和SK到请求中。详情请参见**用户签名验证**。

相关参考

获取永久AK/SK的方法，请参见**获取访问密钥**。

获取临时AK/SK和securitytoken的方法，请参见**获取临时AK/SK和securitytoken**。

9.5 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。各区域的终端节点详情请参见**地区和终端节点**。

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9-2**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 9-2 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	【结构】 **Endpoint** 【示例】 obs.ap-southeast-1.myhuaweicloud.com	不同的区域分配各自对应的域名，即各区域的终端节点。 各区域的终端节点详情请参见**地区和终端节点**。 OBS每个区域对应一个Endpoint，不区分内外网。当配置了**内网访问**之后，即可通过内网访问OBS。	HTTPS HTTP
桶访问域名	【结构】 **BucketName.Endpoint** 【示例】 bucketname.obs.ap-southeast-1.myhuaweicloud.com	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管理控制台或OBS Browser+上查看桶基本信息获取。	HTTPS HTTP

域名类型	域名结构	说明	协议类型
对象访问域名	【结构】 **BucketName.Endpoint/ObjectName** 【示例】 bucketname.obs.ap-southeast-1.myhuaweicloud.com/object.txt	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，或在SDK上通过调用GetObjectUrl接口获取。	HTTPS HTTP
静态网站访问域名	【结构】 **BucketName.obs-website.Endpoint** 【示例】 bucketname.obs-website.ap-southeast-1.myhuaweicloud.com	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

9.6 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）：从地理位置和网络时延维度划分，同一个Region内共享弹性计算、块存储、对象存储、VPC网络、弹性公网IP、镜像等公共服务。Region分为通用Region和专属Region，通用Region指面向公共租户提供通用云服务的Region；专属Region指只承载同一类业务或只面向特定租户提供业务服务的专用Region。
- 可用区（AZ，Availability Zone）：一个AZ是一个或多个物理数据中心的集合，有独立的风火水电，AZ内逻辑上再将计算、网络、存储等资源划分成多个集群。一个Region中的多个AZ间通过高速光纤相连，以满足用户跨AZ构建高可用性系统的需求。

图9-2阐明了区域和可用区之间的关系。

图 9-2 区域和可用区

目前，华为云已在全球多个地域开放云服务，您可以根据需求选择适合自己的区域和可用区。更多信息请参见**华为云全球站点**。

如何选择区域?

选择区域时，您需要考虑以下几个因素：

- 地理位置

  一般情况下，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。不过，在基础设施、BGP网络品质、资源的操作与配置等方面，中国大陆各个区域间区别不大，如果您或者您的目标用户在中国大陆，可以不用考虑不同区域造成的网络时延问题。
  - 在除中国大陆以外的亚太地区有业务的用户，可以选择“亚太-曼谷”或“亚太-新加坡”等区域。
  - 在非洲地区有业务的用户，可以选择“南非-约翰内斯堡”区域。
  - 在欧洲地区有业务的用户，可以选择“欧洲-巴黎”区域。
- 资源的价格

  不同区域的资源价格可能有差异，请参见**华为云服务价格详情**。

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。有关区域和终端节点的更多信息，请参阅**地区和终端节点**。