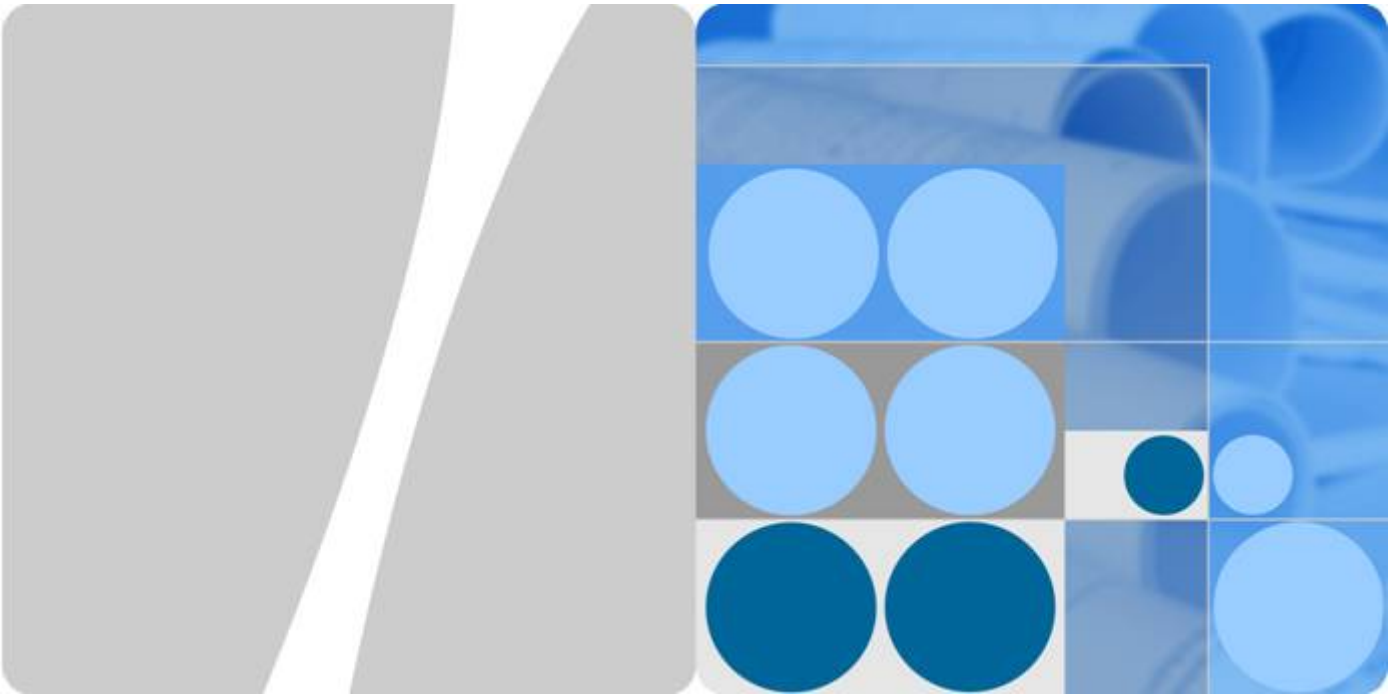


对象存储服务

最佳实践

文档版本　03

发布日期　2019-05-20

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默示的声明或保证。

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。

目 录

1 OBS 最佳实践汇总 1

2 搬迁本地数据至 OBS 2

2.1 概述 2

2.2 OBS 工具方式 3

2.3 云专线方式 3

3 使用备份软件实现本地数据备份至 OBS 5

3.1 概述 5

3.2 使用 Commvault 备份本地 SAP HANA 5

4 在 ECS 上通过内网访问 OBS 8

4.1 概述 8

4.2 在 Windows ECS 上使用 OBS Browser 通过内网访问 OBS 10

4.3 在 Linux ECS 上使用 obsutil 通过内网访问 OBS 12

5 通过 CDN 加速访问 OBS 16

5.1 概述 16

5.2 通过 CDN 实现 OBS 文件下载加速 18

6 使用自定义域名托管静态网站 21

6.1 概述 21

6.2 托管静态网站 22

6.3 更新静态网站 27

7 企业数据权限控制 29

7.1 OBS 权限控制概述 29

7.2 部门公共数据权限管理 32

7.3 部门/项目之间数据共享 35

7.4 企业合作伙伴之间数据隔离 38

A 修订记录 40

1 OBS 最佳实践汇总

本文汇总了基于对象存储服务（OBS，Object Storage Service）常见应用场景的操作实践，每个实践我们提供详细的方案描述和操作指导，帮助用户轻松构建基于OBS的存储业务。

表 1-1 OBS 最佳实践一览表

最佳实践	说明
搬迁本地数据至OBS	本章节根据用户本地（个人电脑或自建存储服务器）数据大小，介绍了几种将本地数据搬迁至OBS的方式方法，并针对不同方式提供了对应操作流程及指导。
使用备份软件实现本地数据备份至OBS	本章节描述了备份本地数据至OBS的背景以及OBS支持的备份软件，并以Commvault备份软件为例，介绍了备份本地数据至OBS的基本流程。
在ECS上通过内网访问OBS	ECS支持通过公网和华为云内网两种方式访问OBS，为优化性能、节省开支，建议通过华为云内网访问OBS。本章节详细描述了在ECS上如何通过华为云内网访问OBS服务。
通过CDN加速访问OBS	OBS支持通过CDN加速实现快速获取存储在OBS上的数据，提升终端用户体验，降低OBS流量开销。本章节以OBS文件下载加速为例，介绍了如何通过CDN加速访问OBS。
使用自定义域名托管静态网站	本章节详细描述了在OBS上使用自定义域名托管静态网站的操作流程及步骤，无需搭建网站服务器，即可快速发布个人及企业静态网站。
企业数据权限控制	OBS提供多种权限控制方式帮助用户管理存储在OBS上的数据。本章节以企业常见数据权限控制场景为例，介绍了如何对存储在OBS上的数据进行权限控制，保障数据安全。

2 搬迁本地数据至 OBS

2.1 概述

背景

传统的自建存储服务器已不能满足大量的数据存储需求，主要原因可以归类为以下三点：

- 数据存储量受限于搭建服务器时使用的硬件设备，如果存储量不够，需要重新购买存储硬盘，进行人工扩容。
- 前期安装难、设备成本高、初始投资大、自建周期长、无法匹配快速变更的企业业务。
- 需承担网络信息安全、技术漏洞、误操作等各方面的数据安全风险。

OBS提供海量、稳定、安全的云存储能力，无需事先规划存储容量，存储资源可线性无限扩展，用户永远不必担心存储容量不够用。在OBS上可以存储任何类型和大小的非结构化数据，多级可靠性架构以及服务端加密、日志管理、权限控制等功能，保障存储在OBS上的数据高度稳定和安全。在成本方面，OBS即开即用，免去了自建存储服务器带来的资金、时间及人力成本的投入，后期的设备维护也全部交由OBS处理。

华为云提供**搬迁方案**，帮助用户将自建存储服务器上的数据短时间、低成本、安全、高效地搬迁至OBS。用户可根据数据量、耗时、费用等需求选择适合的方案进行数据搬迁。

搬迁方案

针对不同的搬迁场景及需求，华为云提供如**表2-1**所示的两种搬迁方案。

表 2-1 搬迁方案

搬迁方式	适用数据量	要求	耗时	费用
OBS工具方式	不高于1TB的数据量	要求用户公网带宽空闲，需要人工操作客户端或脚本启动数据上传	家用100Mbps带宽，1TB耗时10天左右	数据传输不收取费用，仅OBS收取基本的存储费用
云专线方式	每月大于100TB的数据量，需要实时在线上传	需要部署专线	根据专线带宽决定	根据专线距离以及带宽收费，具体参见云专线价格详情

2.2 OBS 工具方式

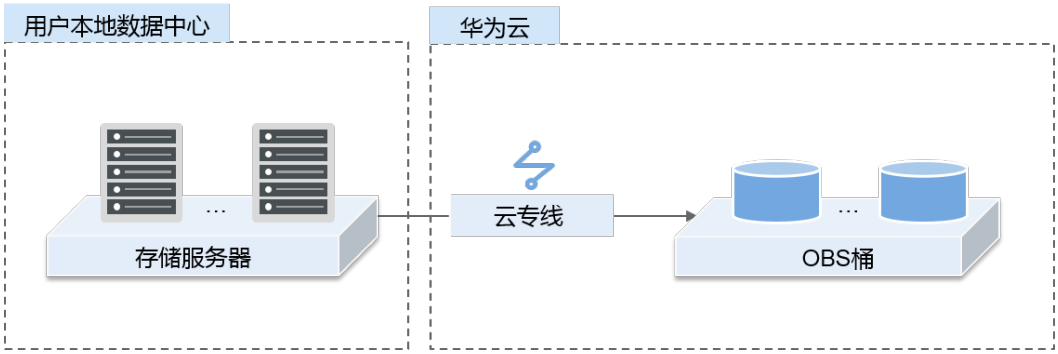
OBS工具方式适用于百GB规模的数据搬迁。OBS提供OBS Browser、obsutil等多种客户端工具，方便用户在本地直接将数据上传至OBS。由于上传需要占用用户公网带宽，为不影响用户在公网上主营业务，建议利用公网带宽空闲的时间上传数据。

各工具使用场景及操作指导，请参见**OBS工具指南**。

2.3 云专线方式

云专线方式由用户自己购买云专线服务（Direct Connect，DC），直接将用户本地的网络与华为云网络打通，实现专线直接访问OBS等服务。云专线方式适用于需要频繁或实时地将本地数据搬迁至OBS的场景。专线提供的低时延、高带宽，可以满足用户随时上传数据至OBS的需求。

图 2-1 云专线方式搬迁数据示意图



1. 创建OBS桶

   登录OBS控制台，创建一个或多个用于存储用户数据的桶。

2. 开通云专线服务

   登录云专线控制台，根据业务需求填写专线申请并提交订单，待管理员审核通过后，用户支付订单，联系运营商安排工程师接通两端物理线路，华为工程师配合进行连接配置。具体操作步骤请参见**开通云专线**。

3. 启动数据传输

   专线搭建成功后，用户可以在本地通过控制台、API、SDK等多种方式将本地数据上传至OBS。

3 使用备份软件实现本地数据备份至 OBS

3.1 概述

传统的备份与恢复方案需要将备份数据写入磁带等存储设备，然后再运输至数据中心。在此过程中数据的安全及完整性依赖很多因素，比如硬件、人员等等。无论是从前期搭建数据中心还是后期的维护，都使得传统的备份与恢复方案面临着管理复杂、投入成本高的难题。

云存储定位于简单、安全、高效且低成本，使其成为磁带等传统存储设备的非常有吸引力的替代品。OBS即一种云存储服务，它提供海量、可弹性扩展的存储服务。OBS所有的业务、存储节点采用分布集群方式工作使得OBS的可扩展性更高。提供数据多份冗余、一致性检查等功能使得存储在OBS中的数据更加安全、可靠。OBS按照使用量付费，使得成本易于预测。

备份软件如Commvault、CloudBerry Backup、NetBackup、爱数云备份服务（AnyBackup Cloud）等，都支持对接OBS进行数据备份。通过这些备份软件，用户可以根据自身需求制定合适的备份策略，达到安全、高效的备份目的。

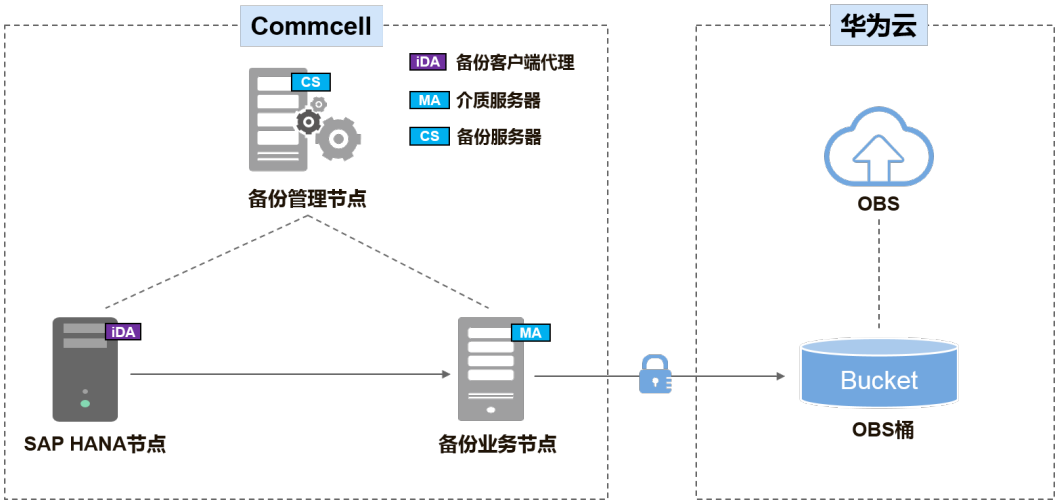
3.2 使用 Commvault 备份本地 SAP HANA

SAP HANA是基于内存计算技术的高性能实时数据计算平台，多应用于需要处理大量实时业务数据的企业。备份软件Commvault，与SAP HANA 、OBS无缝集成，支持在线数据库、日志的备份。当SAP HANA系统出现故障或业务迁移时，Commvault能帮助用户从OBS快速、轻松地恢复数据，从而为SAP HANA提供企业级数据保护。

逻辑架构

此处以使用Commvault备份本地单节点部署的SAP HANA为例，其逻辑架构如图3-1所示。

图 3-1 逻辑架构



逻辑架构中各组件说明如表3-1所示：

表 3-1 组件说明

Name	说明
iDataAgent (iDA)	备份客户端代理，Commvault备份软件的组成部分，部署在SAP HANA节点上，负责获取SAP HANA上需要备份的数据。
CommServe (CS)	备份服务器，Commvault备份软件的组成部分，部署在备份管理节点，负责全局备份策略的制定和备份业务的调度。
Media Agent (MA)	备份介质，Commvault备份软件的组成部分，部署在备份业务节点，负责直接将备份数据存储至OBS。
OBS	在备份场景下OBS负责存储备份数据，桶是OBS中存储数据的容器，最终数据都存储在OBS桶中。

说明

一个CommCell是一个备份管理域，是软件的逻辑组合，包含获取数据、传输数据、管理数据和信息的所有软件组件。

备份流程

1. 安装和预配置备份软件

   在备份SAP HANA场景下，需要安装和配置备份服务器（CommServe）、备份介质（MediaAgent）及SAP HANA备份客户端代理（iDataAgent）三个组件。

2. 创建备份存储空间（OBS桶）

   a. 登录OBS控制台，创建一个桶，作为备份数据存储空间。详细创建桶操作请参见创建桶。

   b. 在CommCell Console上创建云存储库，输入OBS终端节点地址、访问密钥、桶名，用以将Commvault的备份介质（MediaAgent）与OBS关联。

说明

CommCell Console是用于管理CommCell环境、监视和控制活动作业以及查看与活动相关的事件的图形用户界面。

3. 制定Commvault备份策略

   在Commcell Console上创建备份策略，指定数据备份的周期、时间以及加密方式等。

4. 检查备份执行情况

   备份策略执行期间，用户可以通过Commcell Console查看备份执行情况。

5. （可选）执行数据恢复

   在SAP HANA源机上执行数据恢复。

说明

Commvault的具体操作请参见**Commvault官方文档**。

4 在 ECS 上通过内网访问 OBS

4.1 概述

场景介绍

某企业基于弹性云服务器（Elastic Cloud Server，ECS）构建好基础的业务后，随着数据增长，硬盘已无法满足大量的图片、视频等数据存取需求。了解到华为云提供有海量、弹性的云存储服务OBS后，决定将OBS作为数据存储资源池，以减轻服务器负担。

在ECS上可以通过公网和华为云内网两种网络访问OBS。当有存取对象数据的需求时，公网方式响应速度会因为网络质量而受到影响，读取数据还将收取一定的流量费用。为最大化的优化性能、节省开支，企业管理者希望通过内网的方式访问OBS。

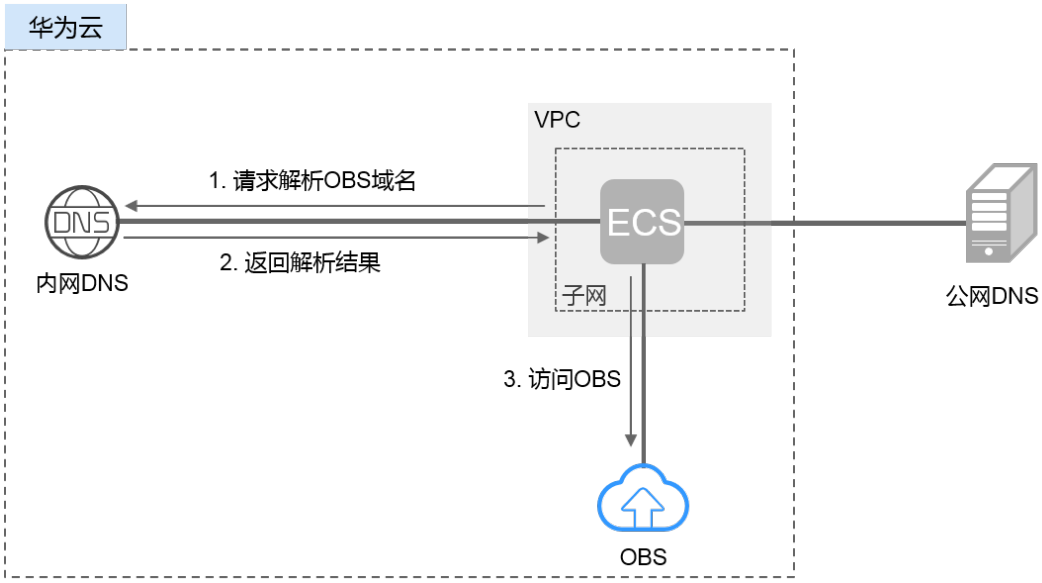
说明

当通过内网访问OBS时，需要确保待访问的OBS资源与ECS属于同一个区域，如果不属于同一个区域，将采用公网访问。

方案

在已搭建的ECS上通过配置内网DNS，由内网DNS解析OBS域名，即可实现在ECS上经由内网访问OBS。访问过程示意图如图4-1所示。

图 4-1 访问 OBS 示意图



示意图中各服务说明如表4-1所示。

表 4-1 服务说明

服务	说明
虚拟私有云（VPC）	VPC主要负责为ECS构建隔离的、用户自主配置和管理的虚拟网络环境，提升用户云中资源的安全性，简化用户的网络部署。 子网是VPC中用来为ECS提供IP地址管理、DNS服务的一个网络，子网内ECS的IP地址都属于该子网。
云解析服务（DNS）	DNS提供内网DNS，专门用于处理华为云内网域名以及OBS域名的解析请求，简化域名解析流程，减少因访问公网产生的流量费用。

- 对于Windows ECS，推荐使用OBS Browser工具，实现内网访问OBS的目的，详细操作请参见：

  在Windows ECS上使用OBS Browser通过内网访问OBS
- 对于Linux ECS，推荐使用obsutil工具，实现内网访问OBS的目的，详细操作请参见：

  在Linux ECS上使用obsutil通过内网访问OBS

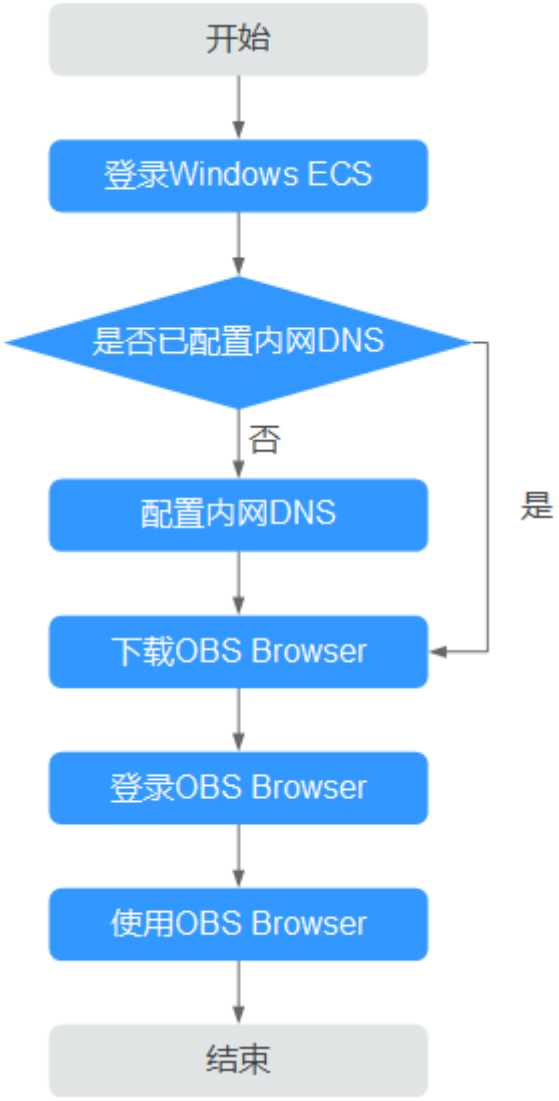
当在ECS上能够通过内网访问OBS时，即可在内网进行数据读取、备份归档等业务，而不影响外网带宽。

4.2 在 Windows ECS 上使用 OBS Browser 通过内网访问 OBS

OBS Browser是适用于Windows操作系统的图形化界面工具，支持通过配置内网DNS服务器地址的方式，使在华为云上的Windows ECS通过内网直接访问OBS，下面将介绍其具体操作流程和操作步骤。

流程

图 4-2 在 Windows ECS 上使用 OBS Browser 通过内网访问 OBS 的流程



操作步骤

步骤1　登录Windows ECS

1. 登录华为云，在页面右上角单击“控制台”，进入“管理控制台”页面。

2. 在打开的控制台首页，选择“计算 > 弹性云服务器”。
3. 选择待登录的云服务器，登录弹性云服务器。

   Windows弹性云服务器提供“VNC远程登录方式”和“MSTSC方式”两种登录方式，具体操作请参见登录Windows弹性云服务器。

步骤2 查看Windows ECS是否已配置内网DNS

在Windows ECS上，您可以通过图形界面和命令行两种方式查看当前的DNS配置。此处以通过命令行方式为例，介绍如何查看DNS配置。

1. 成功登录弹性云服务器后，打开cmd命令行。
2. 运行**ipconfig /all**命令，查看“DNS服务器”是否为当前ECS所在区域的内网DNS地址。

   说明

   华为云针对各区域提供了不同的内网DNS服务器地址，具体请参见**华为云提供的内网DNS服务器地址**。

   - 否，执行**步骤3**。
   - 是，执行**步骤4**。

步骤3 配置内网DNS

修改ECS的DNS服务器地址为华为云提供的内网DNS，可以通过修改VPC子网DNS地址和修改本地DNS配置两种方式实现。

- **方式一：修改VPC子网DNS地址**

  确定ECS所在VPC，并修改VPC子网的DNS服务器地址为内网DNS地址后，可以使整个VPC内的ECS都通过内网DNS进行解析，从而访问在华为云内网的OBS服务。详细操作请参见修改子网网络信息。

  说明

  内网DNS服务器地址需根据ECS所在区域选择内网DNS服务器地址，具体的地址信息请参见**华为云提供的内网DNS服务器地址**。

- **方式二：修改本地DNS配置**

  采用此方式配置的内网DNS会在ECS每次重启后失效，在重启后需要重新配置内网DNS才可以通过内网访问OBS。此处以通过命令行配置为例，介绍如何在本地修改DNS配置。

1. 打开cmd命令行。
2. 运行以下命令，配置首选DNS服务器地址。

   ```
   netsh interface ip set dns name="本地连接" source=static addr=内网DNS服务器地址
   register=primary
   ```

   说明

   - 本地连接：网卡名称，需要根据实际正在使用的网卡进行修改。
   - 内网DNS服务器地址：需要根据ECS所在区域选择内网DNS服务器地址，具体的地址信息请参见**华为云提供的内网DNS服务器地址**。

3. （可选）运行以下命令，配置备份DNS服务器地址。

   ```
   netsh interface ip add dns name="本地连接" addr=备选DNS服务器地址 index=2
   ```

   说明

   - 本地连接：网卡名称，需要根据实际正在使用的网卡进行修改。
   - 备选DNS服务器地址：是在首选DNS服务器出现故障、不可用或无法解析请求的域名时使用的DNS服务器，因此您可以设置为华为云内网DNS服务器的地址（需要根据ECS所在区域选择内网DNS服务器地址，具体的地址信息请参见**华为云提供的内网DNS服务器地址**。），也可以设置成公网DNS服务器地址，具体以实际业务为准。

步骤4　下载OBS Browser

步骤5　登录OBS Browser

由于OBS Browser默认使用公网访问OBS，因此在登录OBS Browser添加账号时，“存储类型”和“服务器地址”需要按照以下要求填写：

- 存储类型：选择“其他对象存储”。
- 服务器地址：根据ECS所在区域输入OBS在此区域的终端节点（Endpoint）和端口号（HTTPS协议端口号为“443”，HTTP协议端口号为“80”。系统默认服务器为HTTPS服务器，如需使用HTTP服务器，请单击OBS Browser页面右上角的  图标并单击“系统配置”，在弹出的“系统配置”窗口，取消对“启用HTTPS安全传输协议”的勾选。）。

  示例：obs.ap-southeast-1.myhuaweicloud.com:443

  说明

  OBS区域和终端节点信息请参见**地区和终端节点**。

步骤6　开始使用OBS Browser

成功登录OBS Browser后，便可以在Windows ECS上直接通过华为云内网访问OBS，进行基本的数据存取操作以及其他的高级设置操作。

常见的数据存储操作请参见：

- 上传文件或文件夹
- 下载文件或文件夹

详细使用指南请参见**对象存储服务工具指南（OBS Browser）**。

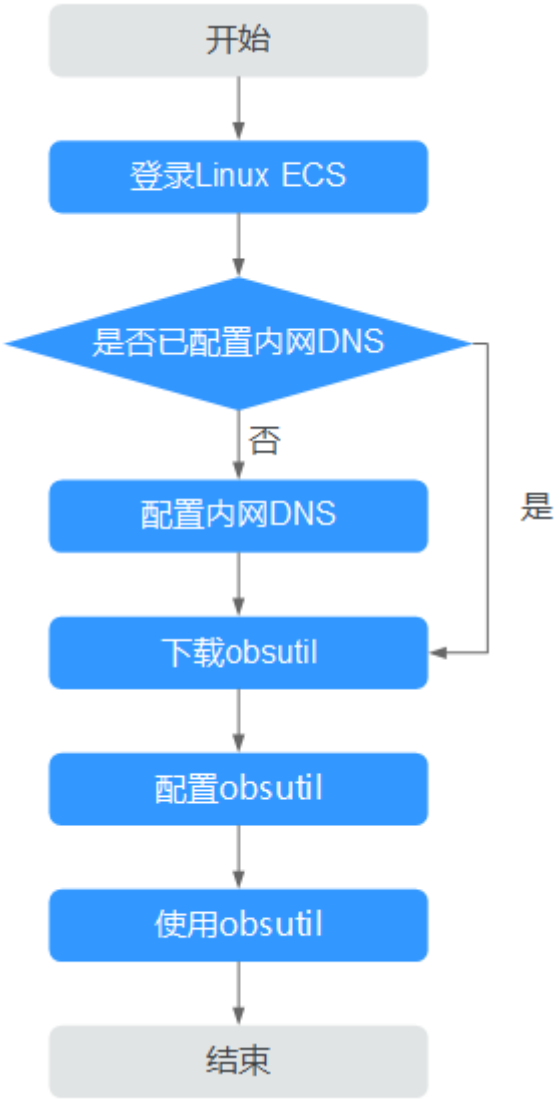
----结束

4.3 在 Linux ECS 上使用 obsutil 通过内网访问 OBS

obsutil是适用于Windows、macOS和Linux操作系统的命令行工具，支持通过配置内网DNS服务器地址的方式，使在华为云上的Linux ECS通过内网直接访问OBS，下面将介绍其具体操作流程和操作步骤。

流程

图 4-3 在 Linux ECS 上使用 obsutil 通过内网访问 OBS 的流程



操作步骤

步骤1 登录Linux ECS

1. 登录华为云，在页面右上角单击“控制台”，进入“管理控制台”页面。
2. 在打开的控制台首页，选择“计算 > 弹性云服务器”。
3. 选择待登录的云服务器，登录弹性云服务器。

   由于购买Linux ECS时设置的登录鉴权方式不同，登录方式因此也存在差异，不同方式登录的具体操作请参见登录Linux弹性云服务器。

步骤2 查看Linux ECS是否已配置内网DNS

1. 成功登录Linux ECS后，打开命令行终端。
2. 运行**cat /etc/resolv.conf**命令，查看首行“nameserver”后的IP地址是否为当前ECS所在区域的内网DNS地址。

说明

华为云针对各区域提供了不同的内网DNS服务器地址，具体请参见**华为云提供的内网DNS服务器地址**。

- 否，执行**步骤3**。
- 是，执行**步骤4**。

步骤3 配置内网DNS

修改ECS的DNS服务器地址为华为云提供的内网DNS，可以通过修改VPC子网DNS地址和修改本地DNS配置两种方式实现。

- **方式一：修改VPC子网DNS地址**

  确定ECS所在VPC，并修改VPC子网的DNS服务器地址为内网DNS地址后，可以使整个VPC内的ECS都通过内网DNS进行解析，从而访问在华为云内网的OBS服务。详细操作请参见**修改子网网络信息**。

  说明

  内网DNS服务器地址需根据ECS所在区域选择内网DNS服务器地址，具体的地址信息请参见**华为云提供的内网DNS服务器地址**。

- **方式二：修改本地DNS配置**

  此处以CentOS 6.x 64bit弹性云服务器为例，介绍如何修改本地DNS配置。

  a. 打开命令行终端。

  b. 运行以下命令，打开“/etc/resolv.conf”文件。

  ```
  vi /etc/resolv.conf
  ```

  c. 按下**i**键进入编辑模式，在“/etc/resolv.conf”文件中按照以下格式，在原有的DNS服务器地址之前新增内网DNS服务器地址。

  ```
  nameserver 内网DNS服务器地址
  ```

  说明

  - 内网DNS服务器地址：需要根据ECS所在区域选择内网DNS服务器地址，具体的地址信息请参见**华为云提供的内网DNS服务器地址**。
  - 新增的DNS服务器地址必须位于所有原有的DNS服务器地址之前。
  - DNS服务器按照nameserver顺序选择，且仅在前一个DNS服务器出现故障、不可用或无法解析请求的域名时，才选择下一个DNS服务器。因此，后续如果想切换成公网方式，需要将首行DNS地址改为公网的DNS，或者在已有DNS服务器地址前增加一条公网DNS服务器地址。

  d. 按下**Esc**键，并输入**:wq!**，保存并退出文件。

  说明

  修改后的DNS地址在保存“/etc/resolv.conf”文件的修改操作后立即生效。

步骤4 下载obsutil

obsutil最新版本和下载链接请参见**下载obsutil**。

步骤5 配置obsutil

使用obsutil之前，您需要配置obsutil与OBS的对接信息，包括OBS终端节点（Endpoint）和访问密钥（AK和SK）。具体操作请参见obsutil指南的**初始化配置**章节。

说明

其中OBS终端节点（Endpoint）需要根据ECS所在区域输入。OBS区域和终端节点信息请参见**地区和终端节点**。

步骤6 使用obsutil

obsutil配置成功后，便可以在Linux ECS上直接通过内网访问OBS，进行基本的数据存取操作以及其他的高级设置操作。

常见的数据存储操作请参见：

- 上传对象
- 下载对象

详细使用指南请参见**对象存储服务工具指南（obsutil）**。

----结束

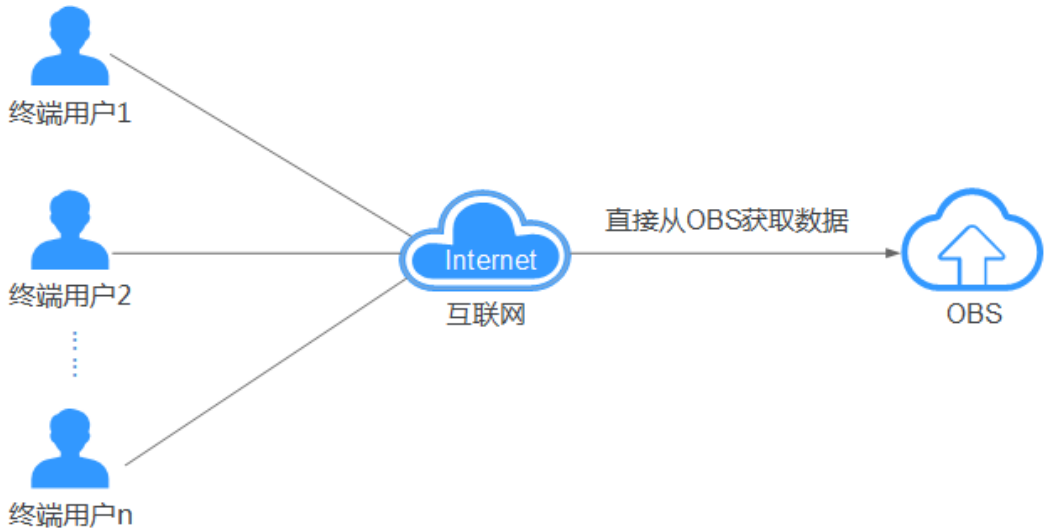
5 通过 CDN 加速访问 OBS

5.1 概述

背景介绍

现在越来越多的行业使用OBS存储图片、视频、软件包等静态资源文件，并将OBS作为网站、论坛、APP、游戏等业务的存储源。在需要获取这些静态资源时，用户通过URL直接从OBS请求数据，数据请求过程如图5-1所示。OBS能够很好的解决本地存储不够用的难题，但一般情况下文件只存储在一个区域，不同区域的用户访问OBS的响应速度存在差异。在需要频繁访问的场景下，直接访问OBS来获取相应文件，还会消耗大量的流量费用。

图 5-1 从 OBS 获取数据过程

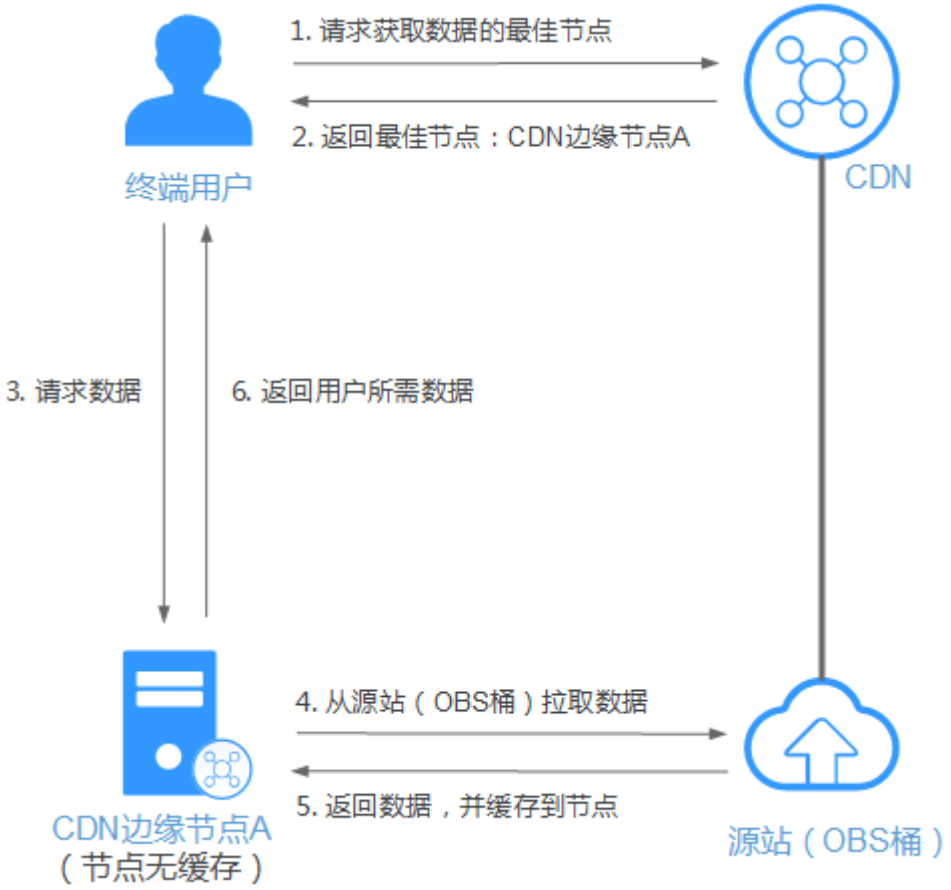


方案说明

OBS提供低成本的存储，华为云CDN可以提供网站加速、文件下载加速和点播加速。将数据存放在OBS中然后通过配置CDN加速，这样构造的业务系统可以在降低成本的同时，提高终端用户使用感受。当终端用户发起访问请求时，会首先通过CDN查找对此域名响应速度最快的CDN节点，并查询此节点是否有缓存终端用户请求的内容。

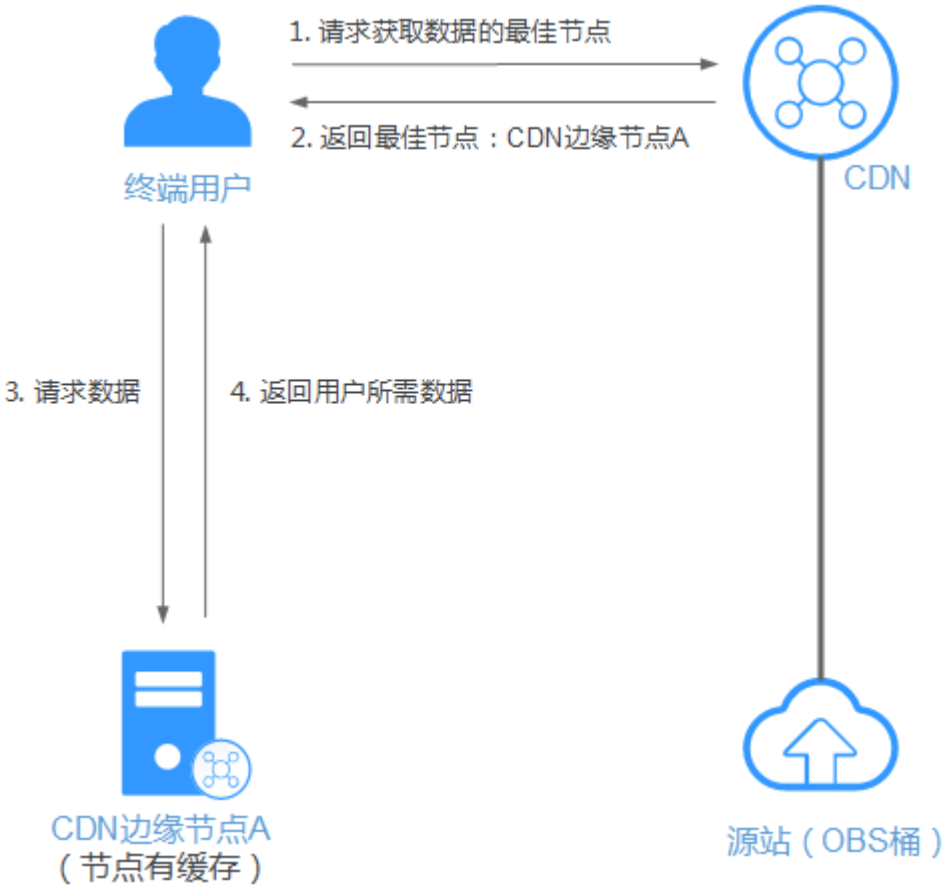
在CDN节点没有缓存用户请求的数据或缓存到期的情况下，CDN加速访问OBS的示意图如图5-2所示。

图 5-2 CDN 加速访问 OBS 示意图（CDN 无缓存）



当其他终端用户再次访问相同的数据时，CDN将直接返回缓存的数据给终端用户，而无需再向OBS发起访问请求。在CDN有缓存的情况下，CDN加速访问OBS的示意图如图5-3所示。

图 5-3 CDN 加速访问 OBS 示意图（CDN 有缓存）



方案优势

- **低成本**：当数据缓存至CDN节点时，后续请求都将通过CDN下行流量计费，从而减少OBS费用。
- **高效率**：华为云CDN具有加速资源丰富、节点分布广泛优势，保证将用户请求精准调度至最佳边缘节点，提供有效且稳定的加速效果。

适用场景

- 通过OBS提供文件下载业务的应用或服务。例如：通过http/https提供文件下载业务的网站、工具下载、游戏客户端、APP商店等。
- 通过OBS提供音视频点播业务的应用或服务。例如：在线教育类网站、在线视频分享网站、互联网电视点播平台、音乐视频点播APP等。

约束与限制

只有桶版本号为3.0及以上的桶支持此方案。桶版本号可以在OBS控制台上，进入桶概览页面后，在“基本信息”中查看。

5.2 通过 CDN 实现 OBS 文件下载加速

本章节以某游戏网站的游戏下载、更新业务为例，介绍如何通过华为云CDN实现加速下载存储在OBS中的游戏安装包以及更新包。

场景介绍

某游戏网站目前已购买OBS服务，并存放了大量游戏软件、图片视频等文件在OBS中。随着用户不断增长，游戏下载、图片加载都存在响应较慢的问题，特别是离文件存放区域较远的用户。基于以上诉求，该网站决定采用CDN加速访问OBS方案，以最低成本实现游戏下载加速，提升用户访问体验。

数据准备

表 5-1 数据准备

准备项	说明	示例
网站域名	游戏网站域名。根据中国《互联网管理条例》的要求，此域名必须在工信部已备案并在有效期内才可以使用CDN加速。	download.game-apk.com
OBS桶	存放图片、软件包等静态资源的桶，存储类别为“标准存储”，桶策略为“私有”。	game-apk

前提条件

已将网站所需图片、软件包等静态资源存储至已准备的OBS桶中。

说明

如果上述操作还未完成，可通过OBS控制台、OBS Browser、SDK等多种方式创建桶、上传文件，具体操作请参考各自帮助文档。

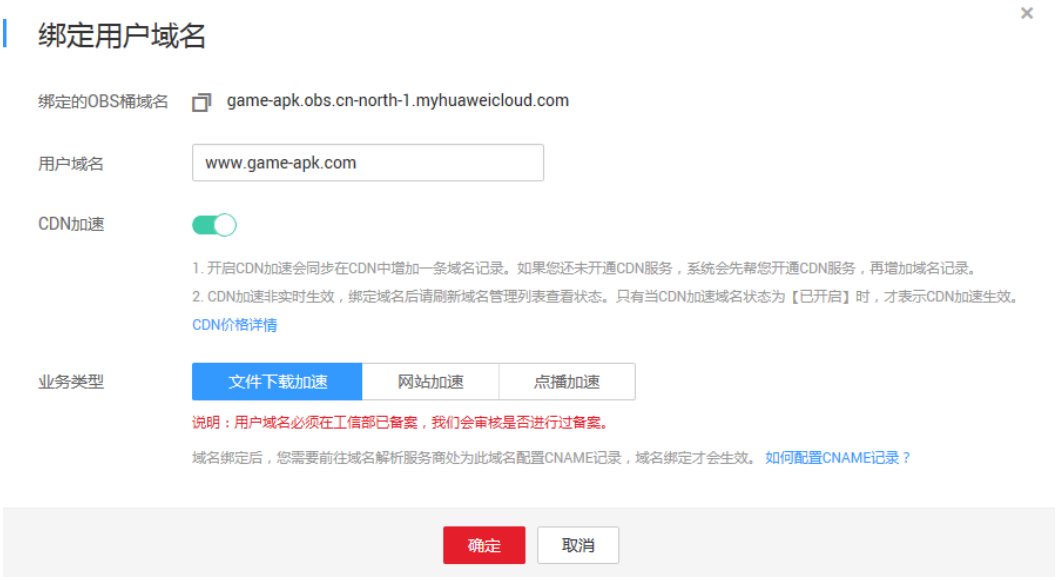
配置步骤

步骤1 配置CDN文件下载加速

OBS支持域名管理功能，在OBS上绑定用户域名即可实现使用自定义域名访问OBS，并可以直接在绑定过程中开启CDN加速，而不用前往CDN开启。

1. 登录华为云控制台，选择“所有服务 > 存储 > 对象存储服务”，进入OBS管理控制台。
2. 单击存放软件包的桶名称，此处以game-apk为例。
3. 在左侧导航栏选择“域名管理”，单击“绑定用户域名”。
4. 在“绑定用户域名”弹框中配置域名及CDN加速等信息，如图5-4所示。
   - 用户域名：输入游戏网站域名，此处以download.game-apk.com为例。
   - CDN加速：开启CDN加速。
   - 业务类型：选择“文件下载加速”。

图 5-4 绑定用户域名



5. 单击“确定”。

步骤2 配置CNAME

在OBS绑定用户域名时开启CDN加速后，CDN会自动生成一条CNAME域名。通过在域名服务商处配置CNAME记录，将加速域名以CNAME方式指向CDN服务中对应的CNAME域名，域名解析生效后，该域名的所有请求都将转向CDN节点。具体操作请参见**配置CNAME**。

步骤3 开启私有桶回源

由于当前存储软件包的桶为私有桶，需要前往CDN开启私有桶回源，CDN才能从OBS中回源获取数据。具体操作请参见**私有桶回源配置**。

步骤4 配置文件下载URL

将代码中需要加速下载的文件URL地址配置为：游戏网站域名+文件在OBS桶中的存储路径+文件名称。

以**步骤2**配置的游戏网站域名**download.game-apk.com**以及存储在game-apk桶中的**game/3.2.1/**文件夹下的**android.apk**文件为例，文件下载URL的配置如下：

```
https://download.game-apk.com/game/3.2.1/android.apk
```

步骤5 验证业务

待游戏网站重新部署后，登录游戏网站，浏览网页图片、进行游戏下载。

如果图片可以成功显示、游戏可以成功下载，则表示加速配置成功。

----结束

6 使用自定义域名托管静态网站

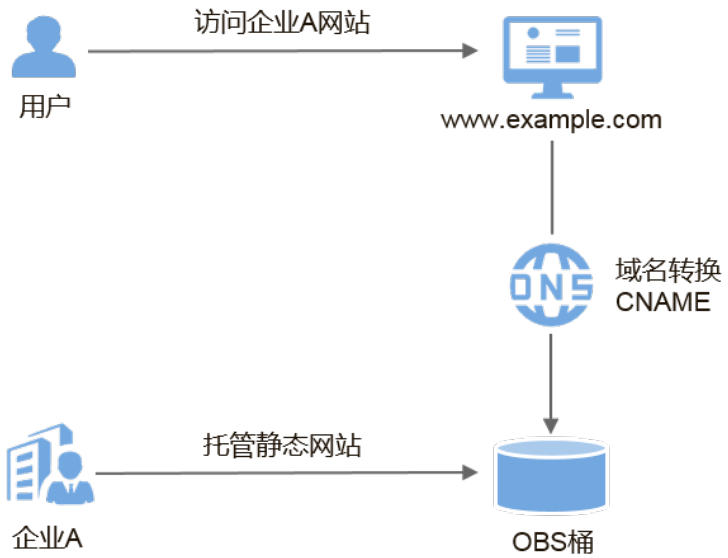
6.1 概述

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

场景介绍

企业A有大量静态网站文件需要存档，但并不希望花费大量的人力、物力在存储资源上。因此该企业开通了OBS，用于托管静态网站，并希望使用自定义域名让该企业下的用户访问这些静态资源，如**图6-1**所示。

图 6-1 使用自定义域名访问静态网站示意图



数据规划

执行配置操作前，需要提前规划如**表6-1**所示的数据。

表 6-1 数据规划

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

- index.html的内容为：

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

- error.html的内容为：

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

6.2 托管静态网站

托管静态网站流程

您需要先在OBS管理控制台上创建一个桶，用于存放静态网站资源，并启用该桶的静态网站托管，然后通过OBS提供的绑定自定义域名功能，将自定义域名与新创建的桶绑定，再通过云解析服务（Domain Name Service，DNS）创建和配置域名托管，实现自定义域名访问托管在OBS上的静态网站。具体操作流程如下：

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

托管静态网站步骤

步骤1 注册域名

如果您拥有一个已注册的域名，可跳过本步骤。

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

步骤2 创建桶

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

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

     说明

     您也可以根据网站的访问频率以及对响应速度的要求，选择“低频访问存储”或“归档存储”。存储类别详情介绍请参见**桶存储类别简介**。
   - **桶名称**：输入“example”。
   - **桶策略**：选择“公共读”使桶内对象能够被任何用户访问。
4. 单击“立即创建”，完成桶创建。

步骤3 上传静态网站文件

整理好待上传的静态网站文件，在OBS控制台重复执行以下步骤，直至所有的静态网站文件都上传至**步骤2**创建的桶中。

说明

OBS控制台不支持上传文件夹、上传超过50MB的单个文件以及批量上传，如果网站文件较多，建议使用OBS Browser上传，具体操作步骤请参见**使用OBS Browser上传文件或文件夹**。

1. 单击待操作的桶名称，进入桶概览页面后在左侧导航栏单击“对象”。
2. 单击“上传对象”，系统将弹出如**图6-2**所示对话框。

图 6-2 上传对象

3. 单击 图标，选择待上传文件。

   说明

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

4. 单击“上传”完成文件上传。

步骤4 配置静态网站托管

上传完静态网站文件后，您需要执行以下步骤，将当前桶设置为静态网站托管模式。

说明

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

1. 单击桶名称，进入桶概览页面后单击“基础配置 > 静态网站托管”。
2. 单击“配置静态网站托管”按钮。
3. 在弹出的对话框中，开启静态网站托管并选择**“配置到当前桶”**，将**“默认首页”**配置为数据规划中的index.html，将**“默认404错误页面”**配置为数据规划中的error.html，如图6-3所示。

图 6-3 配置静态网站托管

说明

您也可以根据业务需求配置重定向规则，实现网站内容重定向，具体操作请参见**配置静态网站托管**。

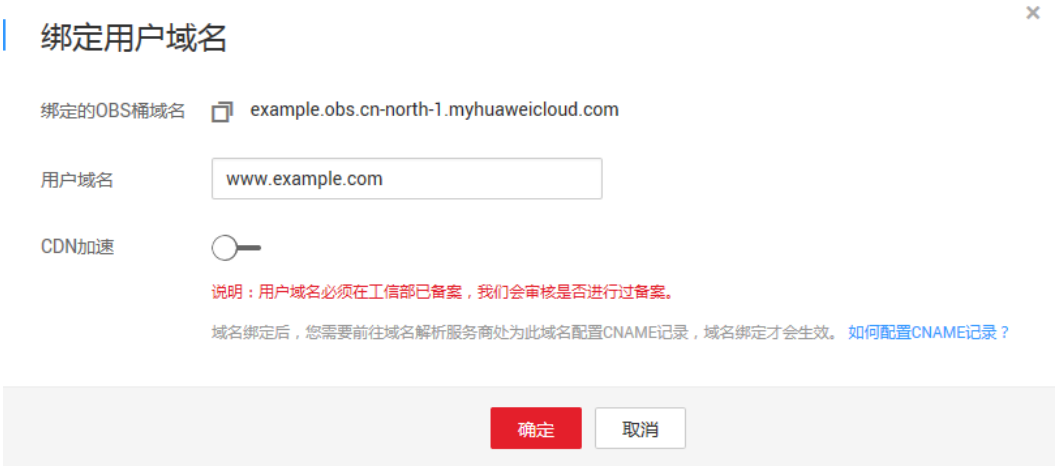
4. 单击“确定”。

步骤5 绑定自定义域名

通过OBS绑定自定义域名的操作步骤如下：

1. 单击桶名称进入“概览”页面，在左侧导航栏选择“域名管理”。
2. 单击“绑定用户域名”，在“用户域名”输入“www.example.com”，如**图6-4**所示。

图 6-4 绑定用户域名



3. （可选）配置CDN加速。

   使能CDN加速后，根据托管的静态网站类型选择网站加速、文件下载加速或点播加速。CDN加速需收费，具体请参见**CDN价格说明**。
4. 单击“确定”，完成自定义域名绑定到桶域名。
5. （可选）如果开启了CDN加速，需要按照以下步骤配置CDN源站信息。
   a. 在已绑定的自定义域名操作列，单击“管理CDN加速”。
   b. 在打开的CDN控制台页面，单击域名，进入域名基本配置页面。
   c. 在“源站配置”区域单击“编辑”按钮，在弹出的“修改源站信息”弹框中，主源站“类型”选择“源站域名”，并在“源站”输入框中输入OBS静态网站托管域名。

      说明

      OBS静态网站托管域名可以进入托管静态网站的桶，在左侧导航栏单击“基础配置 > 静态网站托管”，在页面上方的“访问地址”即静态网站托管域名。

   d. 单击“确定”。

步骤6 创建和配置域名托管。

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

说明

- 若绑定自定义域名时未开启CDN加速，则添加的别名记录需指向桶的访问域名。例如：桶“www.example.com”所处区域“亚太-香港”，则需要在域名注册商添加一条值为“www.example.com CNAME www.example.com.obs-website.ap-southeast-1.myhuaweicloud.com”的记录。

使用云解析服务创建和配置域名托管的操作步骤如下：

1. 创建公网域名。

   在云解析服务中创建公网域名，使用**步骤1**中注册的根域名“example.com”作为创建公网域名。详细的创建方法请参见**配置公网域名解析**章节中的“添加域名”部分内容。

2. 添加别名记录。

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

   - **主机记录**：输入“www”。
   - **类型**：选择“CNAME-规范名称记录”。
   - **线路类型**：选择“全网默认”。
   - **TTL(秒)**：保持默认。
   - **值**：需指向的域名。若绑定自定义域名时没有开启CDN加速，此处填写OBS的桶访问域名；若开启了CDN加速，此处填写CDN提供的加速域名（即CNAME）。

   详细的创建方法请参见**增加CNAME类型记录集**。

3. 在域名注册商处修改域名解析服务器地址。

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

   详细的更改域名解析服务器地址的方法请参见**配置公网域名解析**章节中的“更改域名的DNS服务器”部分。

   说明

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

步骤7 验证。

- 在浏览器中输入访问地址：www.example.com，验证能否访问到配置的默认首页，如**图6-5**所示。

图 6-5 默认首页

- 在浏览器中输入一个桶中不存在的静态文件访问地址，例如：www.example.com/imgs，验证能否访问到配置的404错误页面，如**图6-6**所示。

图 6-6 404 错误页面

说明

由于浏览器缓存等原因，您可能需要清除浏览器缓存后才能查看到预期效果。

----结束

6.3 更新静态网站

后续如果需要对网站某个静态文件（如：图片、音乐、html文件、css文件等）进行更新，您可以重新上传该静态文件。但需要注意的是，默认情况下，在OBS同一路径下新上传的文件会覆盖OBS上已存在的同名文件。为避免文件覆盖的情况，您可以选择启用OBS的多版本控制功能。利用多版本控制，可以保留静态文件的多个版本，使您更方便地检索和还原各个版本，在意外操作或应用程序故障时快速恢复数据。

启用多版本控制

步骤1 登录OBS管理控制台。

步骤2 在桶列表中单击待操作的桶，进入“概览”页面。

步骤3 在“基本信息”区域的“多版本控制”后，单击“编辑”，如图6-7所示。

图 6-7 多版本控制

步骤4 勾选“启用”后单击“确定”，启用目标桶中对象的多版本控制。

----结束

关于多版本控制的更多介绍以及操作指导，请参见多版本控制。

更新静态文件

步骤1 登录OBS管理控制台。

步骤2 在桶列表中单击待操作的桶，进入“概览”页面。

步骤3 在左侧导航栏，单击“对象”。

步骤4 单击“上传对象”，或选择待更新文件所在文件夹后单击“上传对象”，系统将弹出如图6-8所示对话框。

图 6-8 上传对象

步骤5 单击 图标，选择待上传文件。

说明

- 不可加密上传静态网站文件。
- 存储类别建议选择“标准存储”。如果静态网站文件的存储类别为“归档存储”，则需要先恢复才能被访问，具体恢复步骤请参见**恢复归档存储文件**。

步骤6 单击“上传”完成文件上传。

在同一路径下新上传的同名文件会作为“最新版本”显示在对象列表，每次访问此文件时，都是访问的此文件的最新版本，以此达到更新静态网站文件的效果。

----结束

7 企业数据权限控制

7.1 OBS 权限控制概述

默认情况下，只有资源拥有者可以访问OBS资源，其他用户在未经授权的情况下均无OBS访问权限。OBS提供多种方式将OBS资源权限授予给他人，资源拥有者可以根据业务需求制定不同的权限控制方案，从而确保数据安全。

OBS 权限控制方式

OBS提供多种权限控制方式，包括IAM策略、IAM委托、对象限时访问、对象ACL、桶ACL和桶策略。

- **IAM策略**

  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策略的OBS权限详情请参见用户权限。

  IAM策略的应用场景如下：

  - 使用策略控制整个云资源的权限时，使用IAM策略授权。
  - 使用策略控制OBS所有的桶和对象的权限时，使用IAM策略授权。

- **IAM委托**

  委托其他账号或云服务访问OBS，被委托方可以通过切换委托的方式替委托方管理OBS资源，实现安全高效的代维工作。

- **对象ACL**

  基于账号或用户组的对象级访问控制，对象的拥有者可以通过对象ACL向指定账号或用户组授予对象基本的读、写权限。

  默认情况下，创建对象时会同步创建ACL，授权对象拥有者拥有对象的完全控制权限。

  说明

  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。

  对象ACL的权限控制粒度不如IAM策略和桶策略，一般情况下，建议使用IAM策略和桶策略进行权限访问控制。

- **桶ACL**

  基于账号或用户组的桶级权限控制，桶的拥有者可以通过桶ACL向指定账号或用户组授予桶基本的读、写权限。

  默认情况下，创建桶时会同步创建ACL，授权拥有者对桶的完全控制权限。

  桶ACL的权限控制粒度不如IAM策略和桶策略，一般情况下，建议使用IAM策略和桶策略进行权限访问控制。

- **桶策略**

  桶策略提供对OBS资源的集中访问控制，可以精确的描述被授权的资源集和操作集，是对桶ACL和对象ACL的扩展和补充。

  桶策略的应用场景如下：

  - 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。

具体到被授权用户、被授权资源等权限控制主体时，各个方式的详细描述如表7-1所示。

表 7-1 OBS 权限控制方式

方式	被授权用户	被授权资源	被授权操作	是否支持配置条件
IAM用户组权限	IAM用户	OBS所有资源，但不支持指定的OBS资源或资源集	OBS所有操作权限	不支持
IAM委托方式	● 账号 ● 云服务	OBS所有资源，但不支持指定的OBS资源或资源集	OBS所有操作权限	支持配置时间限制（永久或一天）
对象ACL	● 账号 ● 匿名用户 ● 注册用户组	对象	● 获取对象内容及元数据 ● 获取指定版本对象内容及元数据 ● 获取对象ACL相关信息 ● 获取指定版本对象ACL相关信息 ● 设置对象ACL ● 设置指定版本对象ACL	不支持

方式	被授权用户	被授权资源	被授权操作	是否支持配置条件
桶ACL	● 账号 ● 匿名用户 ● 注册用户组 ● 日志投递用户组	桶	● 判断桶是否存在 ● 列举桶内对象，获取桶元数据 ● 列举桶内多版本对象 ● 列举多段上传任务 ● PUT上传，POST上传，上传段，初始化上传段任务，合并段 ● 删除对象 ● 删除特定版本的对象 ● 获取桶ACL的相关信息 ● 设置桶ACL	不支持
桶策略	● 账号 ● IAM用户 ● 匿名用户	OBS所有资源	OBS所有操作权限，详情请参见动作	支持

OBS 权限控制原则

- 最小权限原则

  仅授予IAM用户或账号执行任务所需的最小权限。例如，一个IAM用户仅需执行向指定目录上传、下载对象任务，则无需为其配置整个桶的读写权限。
- 责任分离原则

  同一账号下建议使用不同IAM用户分别管理OBS资源和权限。例如，IAM用户A负责权限分配，而其他IAM用户负责管理OBS资源。
- 条件限制原则

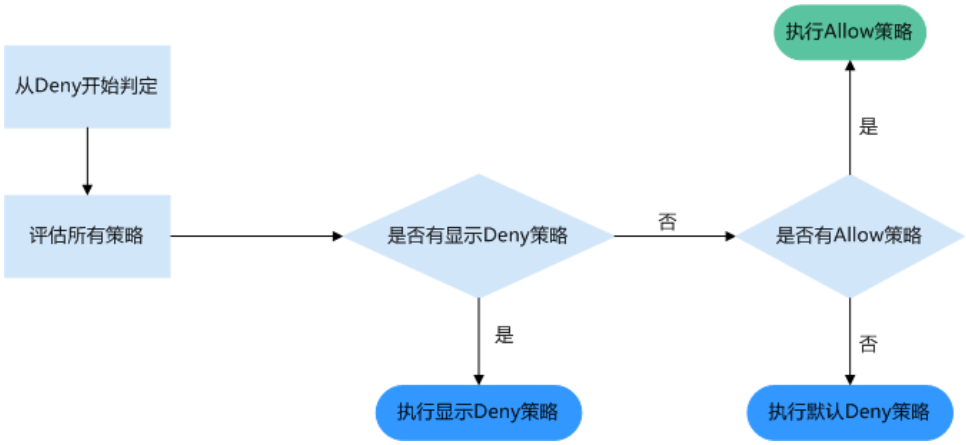
  尽可能的为桶策略定义更精细化的条件，约束桶策略生效的场景，强化桶内资源的安全性。例如，约束OBS只接受来自某特定IP地址发起的访问请求。

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。

图 7-1 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7-2所示。

图 7-2 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

相关概念

- 账号：账户注册华为云后自动创建，该账号对其所拥有的资源和IAM用户具有完全的访问控制权限。
- 管理员：为确保账号及资源的安全性，由账号在IAM中创建的具有“admin”权限的用户，代替账号管理IAM用户。

  说明

  “admin”是IAM系统预置的、拥有所有操作权限的用户组。管理员加入“admin”用户组后，将与账号拥有相同的资源和用户管理权限。
- IAM用户：由管理员在IAM中创建的用户，是云服务的使用者，对应员工、系统或应用程序，具有身份凭证（密码和访问密钥），可以登录管理控制台或者访问API。

7.2 部门公共数据权限管理

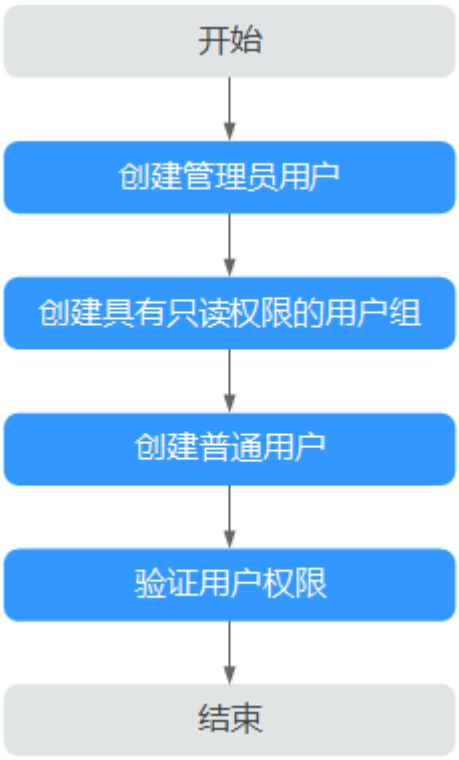
企业日常有大量工作文件需要存档，但并不希望花费大量的人力、物力在存储资源上。因此该企业开通了OBS，用于存储日常工作文件，并希望为不同职能部门的员工设置不同的访问权限，以此达到不同部门人员访问公司数据的权限隔离。

对于存储在OBS中的部门公共数据，企业希望管理员用户拥有完全控制权限，普通用户仅拥有只读权限，可以在OBS执行基本的数据读取操作。

方案及流程

通过简单的**IAM策略**方式进行授权。将普通用户所在用户组权限设置为“Tenant Guest”，即可使普通用户以访客角色访问OBS，对OBS仅拥有只读权限。操作流程如图7-3所示。

图 7-3 部门公共数据权限管理流程



1. **创建管理员用户**

   在IAM控制台创建一个用户并将其加入“admin”用户组，使其具有管理员用户权限。若已经创建管理员用户，可以跳过此步骤。

2. **创建具有只读权限的用户组**

   在IAM控制台创建用户组，并授予对象存储服务权限为“Tenant Guest”。

3. **创建普通用户**

   在IAM控制台创建普通用户，并将其加入2创建的用户组。

4. **验证用户权限**

   通过OBS控制台或OBS Browser验证普通用户的只读权限。

详细配置步骤

步骤1 创建管理员用户

1. 在IAM控制台，单击左侧导航栏中的“用户”。
2. 单击“创建用户”，在“创建用户”界面，输入“用户名”并配置以下参数：

- 凭证类型：选择“密码”。
- 所属用户组：选择“admin”用户组。

3. 单击“下一步”，选择“密码生成方式”为“自定义”。
4. 输入“邮箱”、“手机”、“密码”和“确认密码”。
5. 单击“确定”，完成创建管理员用户。

步骤2 创建具有只读权限的用户组

1. 在IAM控制台，单击左侧导航栏中的“用户组”。
2. 单击“创建用户组”，输入“用户组名称”及“描述”。
3. 单击“确定”。

   返回用户组列表，用户组列表中将显示新创建的用户组。
4. 单击新创建用户组“操作”列的“权限配置”。
5. 在“用户组权限”区域，单击“对象存储服务”项目后的“设置策略”。
6. 在可选策略列表中，选择“Tenant Guest”策略。
7. 单击“确定”，保存用户组权限。

步骤3 创建普通用户

1. 在IAM控制台，单击左侧导航栏中的“用户”。
2. 单击“创建用户”，在“创建用户”界面，输入“用户名”并配置以下参数：
   - 凭证类型：选择“密码”。
   - 所属用户组：选择步骤2创建的用户组。
3. 单击“下一步”，选择“密码生成方式”为“自定义”。
4. 输入“邮箱”、“手机”、密码和“确认密码”。
5. 单击“确定”，完成创建用户。

步骤4 验证用户权限

权限授予成功后，普通用户可以通过OBS控制台、OBS Browser以及API&SDK等多种方式验证。此处以在OBS控制台上的操作为例，介绍如何验证普通用户对部门公共数据的只读权限。

1. 使用普通用户登录OBS控制台，查看是否有权限访问OBS页面。
   - 若显示“没有该页面的访问权限”类似提示，表示当前用户无桶内数据的读取权限，请检查用户权限配置是否正确。
   - 若能显示桶列表，表示当前用户拥有桶列表读取权限，请执行下一步骤。
2. 单击待操作的桶，进入桶概览页面，单击“对象”查看对象列表。
   - 若无法获取对象列表数据，并显示“拒绝访问，请检查相应权限。”等类似提示，表示当前用户无桶内数据的读取权限，请检查用户权限配置是否正确。
   - 若能显示对象列表，表示当前用户拥有读取权限，请执行下一步骤。
3. 在“对象”页面，进行上传、删除对象等写删操作。
   - 若能够进行写删，表示普通用户的只读权限配置失败，请检查用户权限配置是否正确。
   - 若不能写删对象，表示普通用户的只读权限配置正确。

----结束

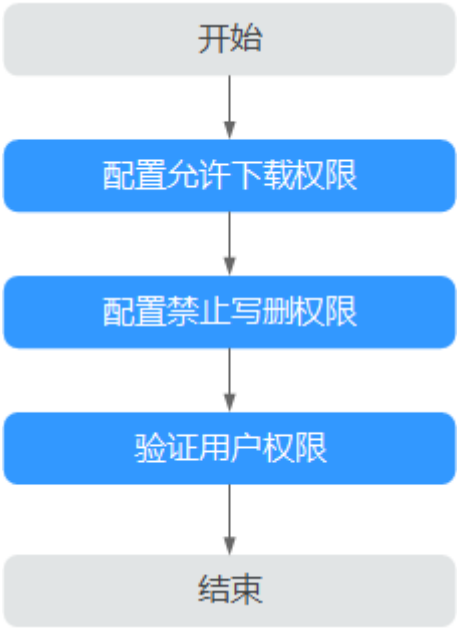
7.3 部门/项目之间数据共享

企业不同部门/项目之间需要共享的数据，本部门/项目允许其他部门/项目用户下载共享数据，禁止写删，以降低共享数据被误删、篡改的风险。

方案及流程

通过IAM策略和桶策略两种OBS权限控制方式，共同配置允许下载和禁止写删共享数据的权限，具体配置流程如7.3 部门/项目之间数据共享所示。

图 7-4 共享数据权限控制流程



1. 配置允许下载权限

   在IAM控制台为其他部门/项目用户配置OBS权限，使其能够读取OBS对象列表、下载OBS对象。

2. 配置禁止写删权限

   在OBS控制台对存放共享数据的桶创建桶策略，禁止其他部门/项目用户写删共享数据。

3. 验证用户权限

   通过OBS控制台或OBS Browser验证其他部门/项目用户对共享数据的下载和写删权限。

前提条件

其他部门/项目用户在IAM中已创建，创建IAM用户的操作步骤请参见。

详细配置步骤

步骤1 配置允许下载权限

1. 登录华为云控制台首页，选择“所有服务 > 管理与部署 >统一身份认证服务（IAM）”。
2. 在IAM控制台，单击左侧导航栏的“用户组”。
3. 单击其他部门/项目用户所在用户组对应操作列的“权限配置”。
4. 单击“对象存储服务”项目对应操作列的“设置策略”，在“设置策略”弹窗中，勾选表7-2所示的任意一种OBS权限。

表 7-2 OBS 用户权限

权限	说明
Tenant Guest	拥有该权限的用户可以查询OBS资源的利用情况，即仅拥有OBS读权限。
OBS Buckets Viewer	拥有该权限的用户可以执行获取桶列表、获取桶中对象列表、查询桶元数据和位置信息的操作。

5. 单击“确定”，完成允许其他部门/项目用户下载OBS对象的权限配置。

步骤2 配置禁止写删权限

1. 在华为云控制台页面上方，选择“服务列表 > 存储 > 对象存储服务”。
2. 进入OBS桶列表页面，单击待操作桶的桶名称。
3. 在左侧导航栏单击“权限”，单击“桶策略”页签。
4. 单击“高级桶策略”下的“ 创建桶策略”按钮。
5. 按照如下参数创建一条高级桶策略，如图7-5所示。
   - 策略模式：选择“自定义模式”。
   - 效果：选择“Deny”。
   - 被授权用户：选择“包含”、“当前账号”，并单击下方的下拉框，选择被授权用户。此处需要选择禁止写删数据的其他部门/项目用户。
   - 资源：输入通配符“*”，表示当前桶内的所有对象。

     说明

     若只需要禁止对桶内部分数据写删，比如某个文件夹或某一类对象，请参考以下示例:

     - example/
     - example*

     也可以输入多个资源，多个资源之间以英文逗号（,）分隔。
   - 动作：选择“包含”，然后单击下方的下拉框，选择“Object”下如表7-3所示的6个动作。

表 7-3 写删对象相关的动作

动作	说明
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
PutObjectAcl	设置对象ACL

动作	说明
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）
AbortMultipartUpload	取消多段上传任务

图 7-5 创建桶策略

6. 单击“确定”，当界面出现类似“桶策略创建成功”的提示时，表示禁止其他部门/项目用户写删共享数据的权限配置成功。

步骤3 验证用户权限

权限授予成功后，其他部门/项目用户可以通过OBS控制台、OBS Browser以及API&SDK等多种方式验证。此处以在OBS控制台上的操作为例，介绍如何验证其他部门用户对部门/项目共享数据的只读权限。

1. 使用其他部门/项目用户登录OBS控制台。
2. 在OBS桶列表页面，单击待操作桶的桶名称。
3. 在左侧导航栏单击“对象”，进入对象列表页面。
4. 单击任一公共数据所在行的“下载”，或者单击“更多 > 下载为”。
   - 下载失败，表示下载权限配置失败，请检查用户组权限配置是否正确。
   - 下载成功，表示下载权限配置成功，请执行下一步骤。
5. 单击“上传对象”，选择文件后单击“上传”。
   - 上传成功，表示写删权限配置失败，请检查桶策略配置是否正确。

- 上传失败，表示写删权限配置成功，执行下一步骤。

6. 单击任一公共数据所在行的“删除”。
   - 删除成功，表示写删权限配置失败，请检查桶策略配置是否正确。
   - 删除失败，表示写删权限配置成功。

----结束

7.4 企业合作伙伴之间数据隔离

对于合作伙伴，企业希望内部数据能够与伙伴数据实现隔离，即合作伙伴只可见被授权的桶，对其他通过不可见，也不可操作。

前提条件

合作伙伴用户已由企业账号创建完成，且创建过程中不加入任何用户组，或者加入一个无OBS权限的用户组，具体操作步骤请参见**创建用户**。

详细配置步骤

通过对存放合作伙伴数据的桶配置桶策略，以允许合作伙伴用户访问此桶。

步骤1 在华为云控制台首页，选择“所有服务 > 存储 > 对象存储服务”。

步骤2 在OBS桶列表页面，单击待操作桶的桶名称。

步骤3 在左侧导航栏单击“权限”，单击“桶策略”页签。

步骤4 单击“高级桶策略”下的“创建桶策略”按钮。

步骤5 按照如下参数创建一条高级桶策略，如**图7-6**所示。

- 策略模式：选择“自定义模式”。
- 效果：选择“Allow”。
- 被授权用户：选择“包含”、“当前账号”，并单击下方的下拉框，选择合作伙伴用户。
- 资源：不输入，表示此条桶策略将作用于整个桶。
- 动作：选择“General”下的“*”。

图 7-6 创建桶策略

步骤6 单击“确定”，完成桶策略创建。

步骤7 验证权限。

权限授予成功后，合作伙伴用户可以通过OBS Browser挂载外部桶的方式验证。

1. 使用合作伙伴用户登录OBS Browser。
2. 单击“添加桶”，在弹出的“添加桶”窗口，选择“添加外部桶”，并输入被授权桶的桶名称。
3. 单击“确定”。

   桶挂载成功，并且可以进行正常访问，则表示权限授予成功。

----结束

A 修订记录

发布日期	修订记录
2019-05-20	第三次正式发布。 本次更新说明如下： ● 新增“通过CDN加速访问OBS”章节。
2018-11-30	第二次正式发布。 本次更新说明如下： ● 新增“OBS最佳实践汇总”章节。
2018-09-30	第一次正式发布。