对象存储服务

最佳实践

文档版本	32
发布日期	2025-09-17

华为技术有限公司

商标声明


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

注意

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

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

安全声明

漏洞处理流程

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

目 录

1 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，为每个实践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
面向AI场景使用OBS+SFS Turbo的存储加速实践	针对AI训练场景中面临的问题，华为云提供了基于对象存储服务OBS+高性能文件服务SFS Turbo的AI云存储解决方案。华为云高性能文件服务SFS Turbo HPC型支持和OBS数据联动，您可以通过SFS Turbo HPC型文件系统来加速对OBS对象存储中的数据访问，并将生成的结果数据异步持久化到OBS对象存储中长期低成本保存。
OBS安全配置建议	本章节提供了OBS使用过程中的安全最佳实践，旨在为提高整体安全能力提供可操作的规范性指导。
企业数据权限控制最佳实践	本最佳实践提供了企业开通OBS后可以设置的四种常见权限控制。 • 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。 • 设置权限允许其他部门/项目用户下载共享数据，禁止写删。 • 给各业务部门分配各自所需的IAM用户，通过桶策略给每个业务部门下的IAM用户授予独立的资源权限。 • 通过OBS Browser+添加外部桶的方式实现业务部门之间桶资源隔离。
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，并针对不同方式提供了对应操作流程及指导。

最佳实践	说明
迁移第三方云厂商的数据至OBS	本章节根据存储在第三方云厂商的数据量及迁移场景，介绍了几种迁移方式，并针对不同方式提供了对应操作流程及指导。
OBS之间数据迁移	本章节介绍如何在华为云对象存储服务OBS之间进行跨账号、跨地域、以及同地域内的数据迁移。
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。
OBS数据一致性校验	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。本章介绍如何利用OBS提供的通过计算MD5值的方式，对上传下载的数据进行一致性校验。
性能优化最佳实践	本章节介绍如何通过给对象添加随机前缀名，对高速率访问请求进行水平扩展，以达到提升访问速率，降低访问时延的效果。
将WordPress远程附件存储到OBS	本章节介绍如何通过插件，将WordPress远程附件存储到华为云OBS。
Web端通过PostObject接口直传OBS	本章节介绍一种在Web端利用PostObject接口直传文件至OBS的方法，即使用表单上传方式上传文件至OBS。该方案省去了应用服务器这一步骤，提高了传输效率，不会对服务器产生压力，且服务端签名后直传可以保证传输的安全性。
移动应用直传	本章节介绍了应用客户端访问OBS的两种方法，从而更好地保护应用数据，避免被攻击后数据泄露以及越权访问的风险。
小程序直传OBS	本章节通过一个示例程序演示了如何通过微信小程序上传文件至OBS。
通过Nginx反向代理访问OBS	本章节介绍如何通过在ECS上配置Nginx反向代理，实现通过固定IP地址访问OBS。

最佳实践	说明
大数据场景下使用OBS实现存算分离	华为云存算分离大数据方案相比传统大数据方案，在同样的业务规模下所使用的计算资源、存储资源以及服务器数量都会有明显下降，同时资源利用率也能得到显著提升，可帮助企业降低业务综合成本。

为帮助企业高效上云，华为云Solution as Code萃取丰富上云成功实践，提供一系列基于华为云可快速部署的解决方案，帮助用户降低上云门槛。同时开放完整源码，支持个性化配置，解决方案开箱即用，所见即所得。

表 1-2 Solution as Code 一键式部署类最佳实践汇总

一键式部署方案	说明	相关服务
CDN下载加速	该方案可以自动将存储在OBS中的数据按需缓存至各地CDN节点，有效加速实现静态资源访问和下载加速	CDN、OBS、DNS
全球数据传输加速	该解决方案基于华为云全站加速WSA服务的动态加速技术构建，有效提升动态页面的加载速度和访问成功率	WSA、OBS、DNS、EIP
文字识别-发票识别与验真	该解决方案基于华为云文字识别OCR服务增值税发票识别与发票验真技术构建，实现财税报销自动化	FunctionGraph、OCR、OBS
内容审核-图片审核	该解决方案可以自动识别图片中涉黄、广告、涉政涉暴、涉政敏感人物等违规内容，降低业务违规风险	FunctionGraph、Moderation、OBS
人证核身解决方案	该解决方案基于华为云人证核身IVS服务和人脸识别 FRS服务构建，快速实现对用户身份真实性的核验	FunctionGraph、IVS、OBS、FRS、APIG
语音识别解决方案	该方案支持中文普通话以及带方言口音的普通话识别以及方言（四川话、粤语和上海话）的识别	FunctionGraph、SIS、OBS
语音识别-隐私通话内容分析	适用于电商领域客服服务过程异常检测，电销领域违规、投诉、专项检测及金融领域机会点挖掘、信用分析等场景	FunctionGraph、语音识别、OBS、SIS
语音识别-客服中心语音质检	适用于货运出行行业隐私通话分析、金融保险领域业务洞察分析及安防风控领域反诈威胁分析等场景	FunctionGraph、语音识别、OBS、SIS

一键式部署方案	说明	相关服务
无服务器日志实时分析	该解决方案帮助您基于无服务器架构实现弹性云服务器 ECS日志的采集、分析、告警以及存档	FunctionGraph、OBS、ECS、LTS、SMN
无服务器图片生成缩略图	基于函数工作流 FunctionGraph快速实现生成图片缩略图，适用于各种Web网页场景	FunctionGraph、OBS
无服务器文件解压	基于函数工作流 FunctionGraph快速实现对象存储 OBS桶里的ZIP或者TAR类型压缩包的自动在线解压	FunctionGraph、OBS
CDN日志定时转储解决方案	基于函数工作流 FunctionGraph帮助用户定时转储CDN服务产生的日志到指定对象存储桶中	FunctionGraph、CDN、OBS
无服务器告警推送	提供一种免开发、易使用、低成本的方式，自动推送华为云的资源告警信息到您常用的通讯平台或统一告警平台	ECS、EVS、OBS、CES、SMN、FunctionGraph、DEW、VPC

2 数据直传 OBS

2.1 将 WordPress 远程附件存储到 OBS

背景信息

WordPress是一个基于PHP语言和MySQL数据库开发的博客平台，并逐步演化成一款内容管理系统软件，具有广泛的应用场景。

本文介绍如何通过插件，将WordPress远程附件存储到华为云OBS。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。

插件支持的功能如下：

- 支持自定义附件在桶的存储位置。
- 支持OBS图片处理特性。
- 支持在WordPress后台编辑图片。
- 支持OBS图片处理采用样式请求功能。
- 支持WordPress4.4+在不同分辨率设备上加载不同大小图片。

前提条件

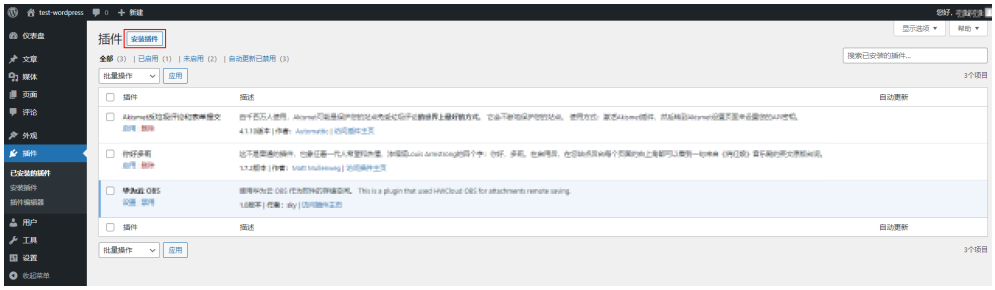
- 已搭建好WordPress，下载及搭建请参考**WordPress官网**。
- 已创建OBS桶，并确保账号具有OBS桶的上传权限，准备好账号对应的AK/SK。
- 已安装PHP 5.6或以上版本。
- 已经下载插件zip包，并将其解压上传至WordPress安装目录的“/wp-content/plugins/”目录中。
  下载链接：**release**

操作步骤

步骤1 打开WordPress，安装插件。

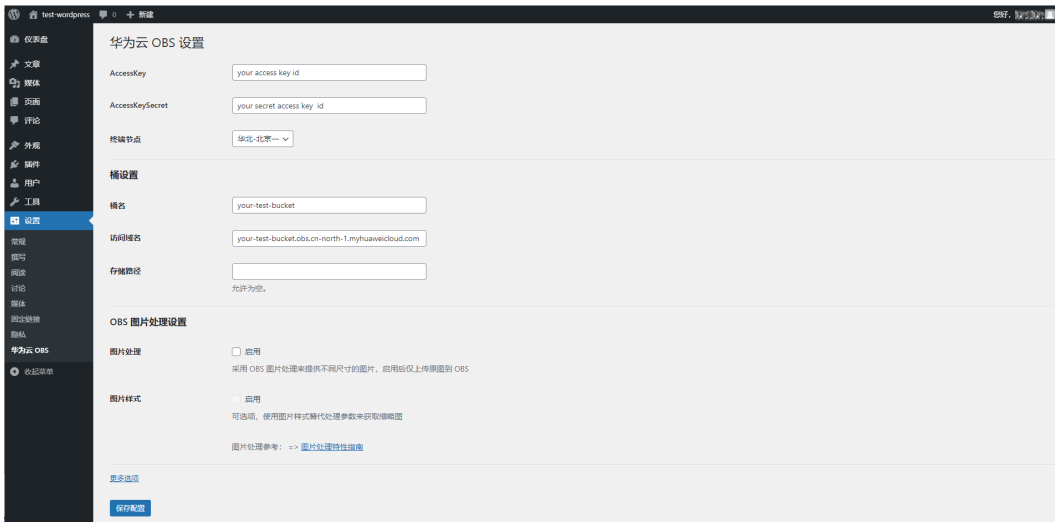
1. 选择左侧导航栏“插件”页签，进入“插件”页面。
2. 单击“安装插件”，选择上传本地的插件zip文件。

上传完成后，可以在插件列表中看到已上传的插件。



步骤2 选择左侧导航栏“设置”页签。

进入“华为云OBS设置”页面，设置插件的使用参数。



配置项		参数设置
AccessKey		用户访问密钥中的AK。
AccessKeySecret		用户访问密钥中的SK。
终端节点		连接OBS的region信息，当前支持华北-北京一、华东-上海二、华南-广州、中国-香港。
桶设置	桶名	保存上传文件至该指定桶中。
	访问域名	桶对应的桶的访问域名。

配置项		参数设置
	存储路径	选填。置空时WordPress的附件将直接传至OBS桶根目录；填写后WordPress的附件将传至OBS桶的指定目录下。
OBS图片处理设置	图片处理	启用后，每次获取图片进行预览时，将根据原图通过调用图片处理接口获取不同尺寸的目标缩略图。
	图片样式	选填，启用后，可以通过设置样式内容获取更加灵活多样的图片处理结果。具体操作请参见**创建图片样式**。

须知

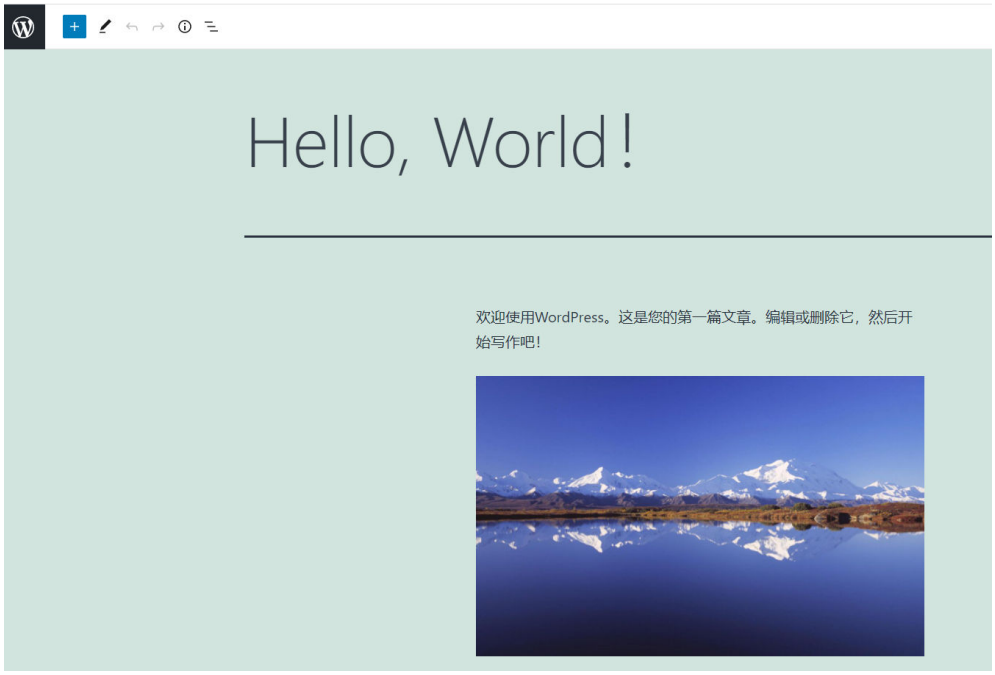
请谨慎开启“更多选项 > 清理服务器存储”功能。

开启“清理服务器存储”后，上传至媒体库的图片和其他附件在上传到OBS后会在本地删除，因此在停用插件后，无法利用本地数据做恢复和替换。

步骤3 单击“保存配置”，完成配置。

步骤4 测试配置是否成功。

1. 新建文章进行测试，在文章中插入图片，插入成功后发布文章。



2. 在图片右键复制图片地址，可以查看当前图片URL域名部分对应**步骤2**中配置的桶访问域名，说明配置成功。

----结束

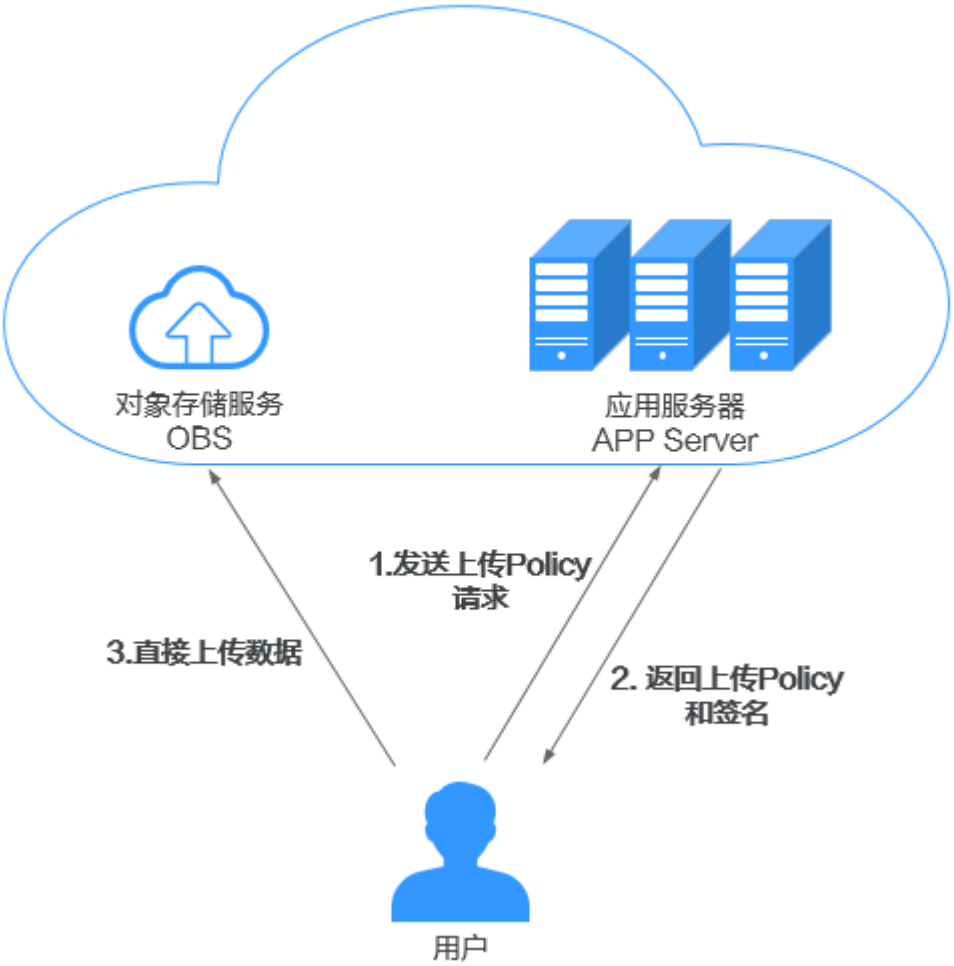
2.2 Web 端通过 PostObject 接口直传 OBS

背景信息

常见的Web端上传方法是用户通过浏览器上传文件至应用服务器，再由应用服务器上传至OBS，数据需要在应用服务器中转，传输效率较低，且多任务同时上传时应用服务器压力大。

本文介绍一种在Web端利用PostObject接口直传文件至OBS的方法，即使用表单上传方式上传文件至OBS。如图2-1所示，该方案省去了应用服务器这一步骤，提高了传输效率，不会对服务器产生压力，且服务端签名后直传可以保证传输的安全性。

图 2-1 Web 端 PostObject 直传流程图



前提条件

已创建桶。具体操作请参见创建桶。

操作步骤

配置分为两大步：配置跨域资源共享和使用表单上传。

第一步：配置跨域资源共享

在通常的网页请求中，由于同源安全策略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。

跨域资源共享CORS是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。OBS支持CORS规范，允许跨域请求访问OBS中的资源。

步骤1 在OBS管理控制台左侧导航栏选择“桶列表”。

步骤2 在桶列表单击待操作的桶，进入对象页面。

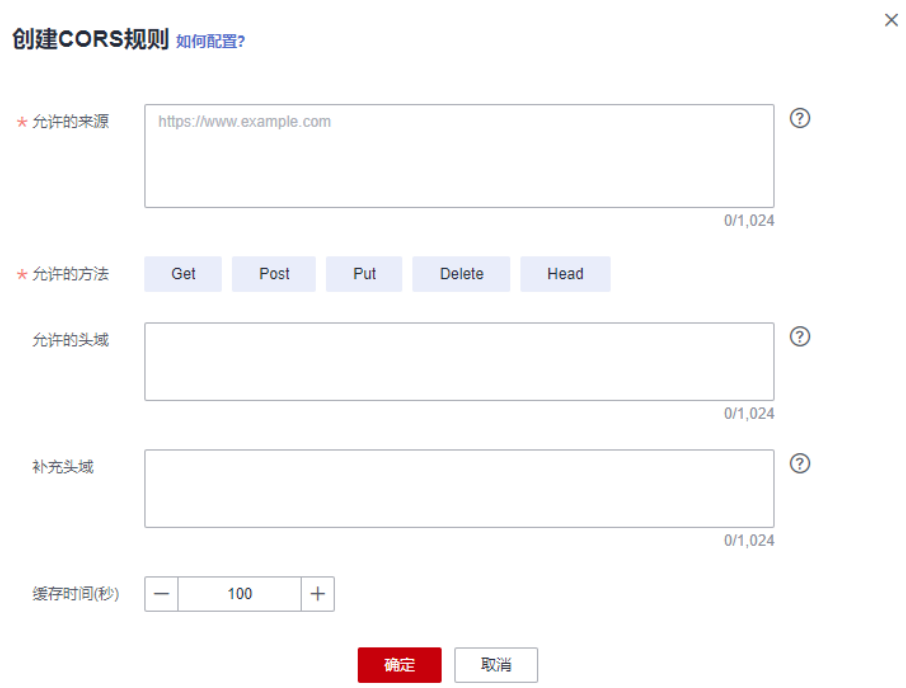
步骤3 在左侧导航栏，单击“权限控制 > CORS规则”。

步骤4 单击“创建”，系统弹出“创建CORS规则”对话框，如图2-2所示。

说明

一个桶最多可设置100条CORS规则。

图 2-2 创建 CORS 规则



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

说明

如果该OBS桶同时开启了CDN加速，CDN需配置HTTP header，详见HTTP header配置。

表 2-1 CORS 规则

参数	说明	配置建议
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。	全选
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	配置建议
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。 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。	• ETag • x-obs-request-id • x-obs-api • Content-Type • Content-Length • Cache-Control • Content-Disposition • Content-Encoding • Content-Language • Expires • x-obs-id-2 • x-reserved-indicator • x-obs-version-id • x-obs-copy-source-version-id • x-obs-storage-class • x-obs-delete-marker • x-obs-expiration • x-obs-website-redirect-location • x-obs-restore • x-obs-version • x-obs-object-type • x-obs-next-append-position
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。	根据实际业务设置。

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”，允许的头域配置为“*”，补充头域配置为“ETag”，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，允许响应中返回ETag值，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

第二步：使用表单上传

以BrowserJS为例，演示如何直接使用SDK计算签名。

基于表单上传是使用HTML表单形式上传对象到指定桶中，对象最大不能超过5GB。

您可以通过ObsClient.createPostSignatureSync生成基于表单上传的请求参数。使用BrowserJS代码模拟表单上传的完整代码示例，可单击此处下载：**post-object-sample**。您也可以通过如下步骤进行表单上传：

步骤1 使用ObsClient.createPostSignatureSync生成用于鉴权的请求参数。

使用SDK生成用于鉴权的请求参数包括两个：

- Policy：对应表单中policy字段。
- Signature：对应表单中的signature字段。

代码示例如下：

```
// 创建ObsClient实例
var obsClient = new ObsClient({
    // 认证用的ak和sk硬编码到代码中或者明文存储都有很大的安全风险，建议在配置文件或者环境变量中密文存放，使用时解密，确保安全；本示例以ak和sk保存在环境变量中为例，运行本示例前请先在本地环境中设置环境变量AccessKeyID和SecretAccessKey。
    // 您可以登录访问管理控制台获取访问密钥AK/SK，获取方式请参见https://support.huaweicloud.com/usermanual-ca/ca_01_0003.html
    access_key_id: process.env.AccessKeyID,
    secret_access_key: process.env.SecretAccessKey,
    server : 'https://your-endpoint',
    signature : 'obs'
});

// 设置表单参数
var formParams = {
            // 设置对象访问权限为公共读
            'x-obs-acl': obsClient.enums.AclPublicRead,
            // 设置对象MIME类型
            'content-type': 'text/plain'
};

// 设置表单上传请求有效期，单位：秒
var expires = 3600;

var res = obsClient.createPostSignatureSync({Expires:expires, FormParams: formParams});

// 获取表单上传请求参数
console.log('\t' + res.Policy);
console.log('\t' + res.Signature);
```

步骤2 准备表单HTML页面。

表单HTML代码示例如下：

```
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
</head>
<body>

<form action="http://bucketname.your-endpoint/" method="post" enctype="multipart/form-data">
Object key
<!-- 对象名 -->
<input type="text" name="key" value="objectname" />
<p>
ACL
<!-- 对象ACL权限 -->
<input type="text" name="x-obs-acl" value="public-read" />
<p>
```

```
Content-Type
<!-- 对象MIME类型 -->
<input type="text" name="content-type" value="text/plain" />
<p>
<!-- policy的base64编码值 -->
<input type="hidden" name="policy" value="*** Provide your policy ***" />
<!-- AK -->
<input type="hidden" name="AccessKeyId" value="*** Provide your access key ***"/>
<!-- 签名串信息 -->
<input type="hidden" name="signature" value="*** Provide your signature ***"/>

<input name="file" type="file" />
<input name="submit" value="Upload" type="submit" />
</form>
</body>
</html>
```

说明

- HTML表单中的policy，signature的值均是从ObsClient.createPostSignatureSync的返回结果中获取。
- 表单HTML示例可单击此处下载：**PostDemo**。

步骤3 将生成的请求参数填入HTML页面。

步骤4 选择本地文件，进行表单上传。

----结束

结果验证

HTML表单中包含一个文件选择框和一个上传按钮，用户可以选择想要上传的文件然后提交表单。

当表单提交时，JavaScript代码会请求服务器获取本次上传所需要的签名信息，得到正确响应之后，会构造一个FormData对象， 然后填充所有必要数据，通过fetch方法发送POST请求到OBS的服务端，完成文件上传。

图 2-3 表单上传回调示例

通过表单上传一个名为“demo-object”的文件至桶“post-callback-demo”中，上传后在OBS桶列表中的“post-callback-demo”中可以看到“demo-object”文件，即表示成功通过表单上传文件。

图 2-4 查看所上传的文件

知识扩展

采用BrowserJS SDK直接计算签名时，AK/SK可能会展现在前端界面，有一定风险。

您还可以采用客户端-服务端模型，服务端可以采用Java、Python等SDK计算POST上传签名，客户端采用JavaScript向服务端获取签名信息后利用签名信息访问OBS。

其中，计算POST上传签名信息请参考各SDK语言：

- Java
- Python
- PHP
- BrowserJS
- Node.js

除POST上传外，在其他场景中，为了避免前端代码直接使用AK/SK访问OBS造成敏感信息泄露，可以通过后台计算临时URL，前端使用临时URL授权访问OBS。

利用GO SDK计算临时URL，前端JS使用临时URL列举OBS桶内对象。示例如下：

1. GO SDK后台计算列举桶临时URL。

```
// 引入依赖包
import (
	"fmt"
	"obs"
	"strings"
)

//推荐通过环境变量获取AKSK，这里也可以使用其他外部引入方式传入，如果使用硬编码可能会存在泄露风险。
//您可以登录访问管理控制台获取访问密钥AK/SK，获取方式请参见https://support.huaweicloud.com/usermanual-ca/ca_01_0003.html。
var ak = os.Getenv("AccessKeyID")
var sk = os.Getenv("SecretAccessKey")
var endpoint = "https://your-endpoint"

// 创建ObsClient结构体
var obsClient, _ = obs.New(ak, sk, endpoint)

func main() {
	input := &obs.CreateSignedUrlInput{}
```

```
        input.Expires = 3600

        // 生成列举对象临时URL
        // 指定为GET请求，传入桶名
        input.Method = obs.HttpMethodGet
        input.Bucket = "bucketname"
        output, _ := obsClient.CreateSignedUrl(input)
       // 获取生成的临时URL及请求头域信息
        fmt.Printf("SignedUrl:%s\n", output.SignedUrl)
        fmt.Printf("ActualSignedRequestHeaders:%v\n", output.ActualSignedRequestHeaders)
}
```

2. 前台获取到签名URL SignedUrl及请求头域信息ActualSignedRequestHeaders后，访问OBS进行列举桶操作。

```
// 使用GET请求获取对象列表
var bucketName = 'bucketname';
var method = 'GET';

// SignedUrl为上一步骤中后端服务计算得到的临时URL，
// ActualSignedRequestHeaders为上一步骤中后端服务计算临时URL时使用的请求头域，前台实际请求应保持一致；
var reopt = {
        method : method,
        url : SignedUrl,
        withCredentials: false,
        headers : ActualSignedRequestHeaders || {},
        validateStatus: function(status){
                return status >= 200;
        },
        maxRedirects : 0,
        responseType : 'text',
};

axios.request(reopt).then(function (response) {
        if(response.status < 300){
                console.log('Listing object using temporary signature succeed.');
        }else{
                console.log('Listing object using temporary signature failed!');
                console.log('status:' + response.status);
                console.log('\n');
        }
        console.log(response.data);
        console.log('\n');
}).catch(function (err) {
        console.log('Listing object using temporary signature failed!');
        console.log(err);
        console.log('\n');
});
```

其中，生成临时授权访问URL请参考各SDK语言：

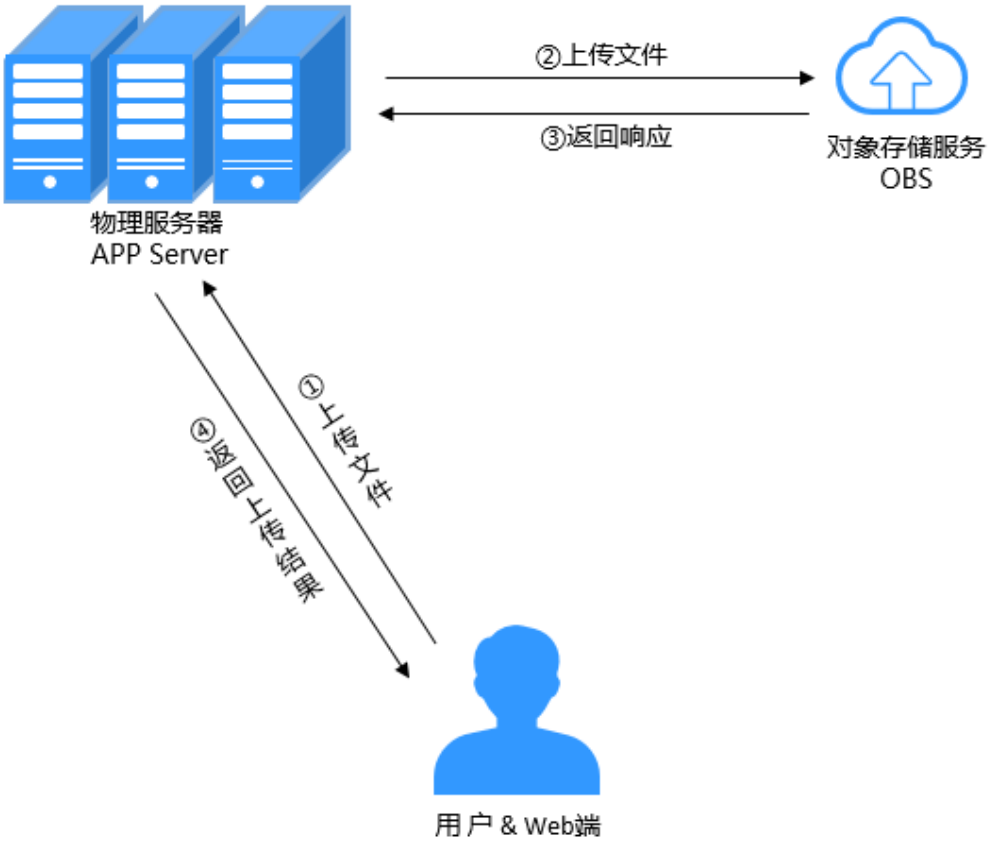
- Java
- Python
- Go
- Node.js

2.3 Web 端直传 OBS 并设置上传回调

应用场景

常见的Web端上传方式是用户通过浏览器上传文件至应用服务器，再由应用服务器上传至OBS，如图2-5所示，数据需要在应用服务器中转，传输效率较低，且多任务同时上传时应用服务器压力很大。

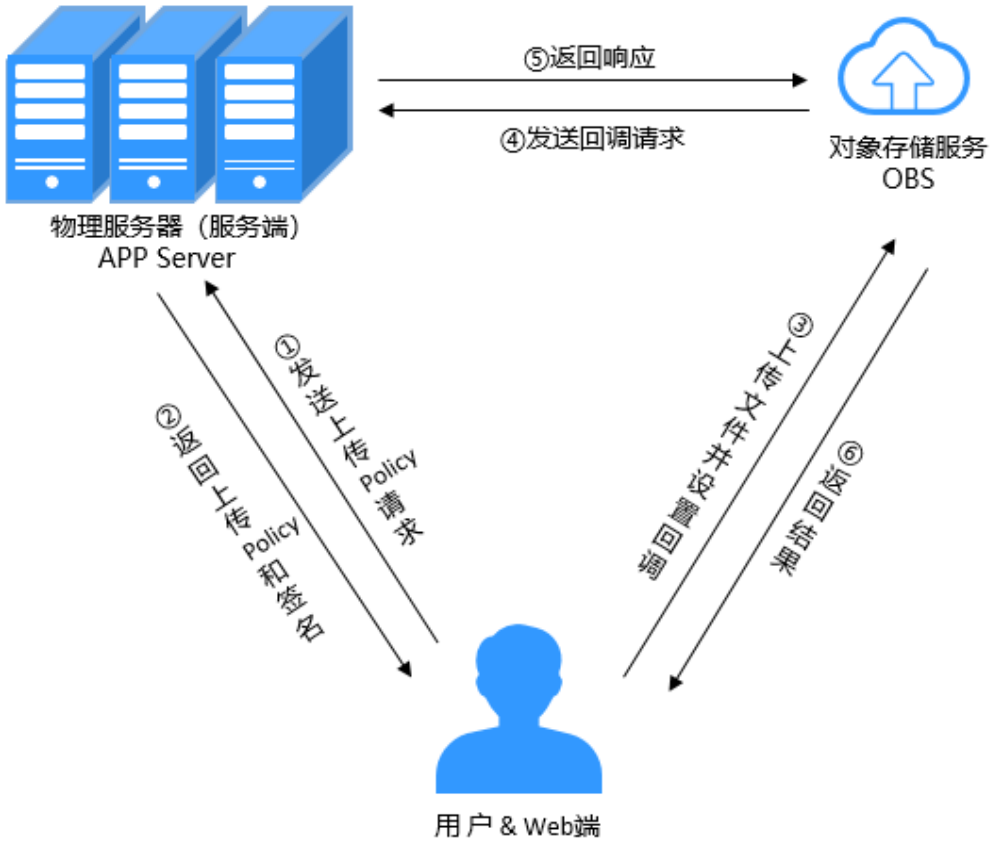
图 2-5 常见的 Web 端上传文件方式



本文介绍一种在Web端利用PostObject接口直传文件至OBS并设置上传回调的方法，即使用表单上传方式上传文件至OBS，上传成功后会回调指定的地址。如**方案架构**所示，该方案省去了在应用服务器中转文件这一步骤，由Web端直传文件至OBS，提高了传输效率，且不会对服务器产生压力，同时服务端签名后直传可以保证传输的安全性。

方案架构

图 2-6 Web 端 PostObject 直传并设置上传回调架构图



整个Web端直传文件至OBS并设置上传回调的请求流程如下：

1. 用户通过Web客户端向服务端发送上传安全策略请求；
2. 服务端使用访问凭证和上传安全策略计算签名，然后向Web端返回上传安全策略和签名；
3. 用户使用Web端构建的HTML表单上传文件至OBS并设置上传回调；
4. OBS向服务端发送回调请求；
5. 服务端返回响应至OBS；
6. OBS返回上传结果至Web端。

说明

安全策略（policy）的作用是限制表单上传的内容，例如规定表单上传对象的对象名前缀必须以“prefix01”开头，使用policy能够帮助您更好的管控桶中的文件。

资源和成本规划

表 2-2 资源规划

区域	资源	资源名称	资源说明	数量	费用
华北-北京四	OBS桶	post-callback-demo	用于存储用户上传文件的桶。 您需要在OBS控制台创建桶。	1	根据文件占用的存储空间收费，具体请参见**存储费用**。
-	文件	demo-object.txt	用于上传的文件。 您需要提前准备好上传的文件。	1	-
-	AK/SK	AK/SK	AK/SK为访问OBS的凭证，服务端使用AK/SK生成签名，进行用户鉴权。 AK/SK相关内容，详情请参见**访问密钥**。	1	-

操作流程

要实现Web端直传OBS并设置上传回调，需要以下三步：

1. **创建桶并配置CORS规则：**在OBS控制台创建一个桶，用于存储用户上传的文件；同时为桶配置跨域资源共享（CORS），以允许来自Web端的跨域名访问。
2. **服务端生成签名：**服务端使用访问凭证和上传策略（如：桶名称、对象名前缀、过期时间等）生成签名，授权用户在指定时间内完成文件上传。
3. **Web端通过表单上传对象并设置上传回调：**Web端在HTML表单中构建请求并设置上传回调，此请求使用POST表单上传来直接调用OBS的服务端，实现文件上传。

实施步骤

步骤一：创建桶并配置 CORS 规则

在OBS控制台创建一个桶，用于存储用户上传的文件；同时为桶配置跨域资源共享（CORS），以允许来自Web端的跨域名访问。

1. 创建桶

如果您已有桶，可跳过本步骤直接**配置CORS规则**。

步骤1 在OBS**管理控制台**左侧导航栏选择“桶列表”。

步骤2 在页面右上角单击“创建桶”。

步骤3 设置相关参数。

表 2-3 创建桶参数说明

参数名称	示例	说明
区域	**华北-北京四**	桶所属的区域。 ● **桶创建成功后，不支持变更区域，请谨慎选择。** ● 请选择靠近您业务的区域创建桶，以降低网络时延，提高访问速度。
桶名称	**post-callback-demo**	创建桶时，需要设置合适的桶名称。 **桶创建成功后，不支持修改桶名称。** 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或并行文件系统（包含其他用户创建的）名称重复。**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（.），且不能以中划线（-）或英文句号（.）开头及结尾。 ● 禁止两个英文句号（.）相邻，禁止英文句号（.）和中划线（-）相邻。 ● 禁止使用IP地址。
企业项目	**default**	将桶加入到企业项目中统一管理。如无特殊的企业项目划分和管理需求，此处可直接选择默认企业项目“default”。 如果您想要了解更多关于如何通过企业项目管理OBS桶，具体请参见**创建桶**中的“企业项目”参数说明。

步骤4 单击右下角的“立即创建”，确认提示信息，并单击“确定”。

步骤5 在“创建成功”弹窗，单击“确定”。在桶列表页可以看到新创建的桶，即表示创建成功。

----结束

2. 配置CORS规则

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。

跨域资源共享CORS是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。OBS支持CORS规范，允许跨域请求访问OBS中的资源。在OBS控制台配置CORS规则步骤如下：

步骤1 在OBS**管理控制台**左侧导航栏选择“桶列表”。

步骤2 在桶列表单击待操作的桶，进入对象页面。

步骤3 在左侧导航栏，单击“数据安全 > CORS规则”。

步骤4 单击“创建”系统弹出“创建CORS规则”弹窗。

步骤5 设置相关参数。

图 2-7 创建 CORS 规则

表 2-4 CORS 规则参数说明

参数名称	示例	说明
允许的来源	*	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。 允许填写的字符范围：1~1024。 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	**Get、Post、Put、Delete、Head**	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。 允许填写的字符范围：1~1024。 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。

参数名称	示例	说明
补充头域	• **ETag** • **x-obs-request-id** • **x-obs-api** • **Content-Type** • **Content-Length** • **Cache-Control** • **Content-Disposition** • **Content-Encoding** • **Content-Language** • **Expires** • **x-obs-id-2** • **x-reserved-indicator** • **x-obs-version-id** • **x-obs-copy-source-version-id** • **x-obs-storage-class** • **x-obs-delete-marker** • **x-obs-expiration** • **x-obs-website-redirect-location** • **x-obs-restore** • **x-obs-version** • **x-obs-object-type** • **x-obs-next-append-position** • **x-obs-callback**	可选参数，指定CORS响应中带的补充头域，给客户端提供额外的信息。 允许填写的字符范围：1~1024。 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	**300**	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。 输入值范围：0~9999999。

步骤6 单击“确定”。

“CORS规则”页签显示“创建CORS规则成功”提示即表示成功创建桶的CORS规则。CORS规则会在两分钟内生效。

----结束

步骤二：服务端生成签名

服务端使用访问凭证（AK/SK/securityToken[可选]）和上传策略（如：桶名称、对象名前缀、过期时间等）生成签名，授权用户在指定时间内完成文件上传。获取或新建AK/SK，请参见**访问密钥**。

⚠ 注意

建议先将访问凭证（AK/SK/securityToken[可选]）配置到环境变量，避免在代码中直接显示访问凭证而引起敏感信息泄露。

1. 配置环境变量

- **Linux系统**
  a. 在命令行中执行以下命令，将环境变量添加到~/.bashrc中。
  ```
  echo "export ACCESS_KEY_ID='your access key id'" >> ~/.bashrc
  echo "export SECRET_ACCESS_KEY_ID='your secret access key id'" >> ~/.bashrc
  ```
  b. 在命令行中执行以下命令，使**a**的设置生效。
  ```
  source  ~/.bashrc
  ```
  c. 在命令行中执行以下命令，确认环境变量是否配置成功。
  ```
  echo $ACCESS_KEY_ID
  echo $SECRET_ACCESS_KEY_ID
  ```
  - 如果命令行中显示**a**设置的信息，表示设置成功。
  - 如果命令行中未显示**a**设置的信息，表示设置失败，请重新设置。
- **Windows系统**
  a. 在Windows系统的命令行解释器（Command Prompt，CMD）中执行以下命令，设置环境变量。
  ```
  setx ACCESS_KEY_ID "your access key id"
  setx SECRET_ACCESS_KEY_ID "your secret access key id"
  ```
  b. 打开新的CMD窗口并执行以下命令，确认环境变量是否配置成功。
  ```
  echo %ACCESS_KEY_ID%
  echo %SECRET_ACCESS_KEY_ID%
  ```
  - 如果命令行中显示**a**设置的信息，表示设置成功。
  - 如果命令行中未显示**a**设置的信息，表示设置失败，请重新设置。
- **macOS系统**
  a. 打开bash终端，执行以下命令，将环境变量添加到~/.bash_profile中。
  ```
  echo "export ACCESS_KEY_ID='your access key id'" >> ~/.bash_profile
  echo "export SECRET_ACCESS_KEY_ID='your secret access key id'" >> ~/.bash_profile
  ```
  b. 在命令行中执行以下命令，使**a**的设置生效。
  ```
  source  ~/.bashrc
  ```
  c. 执行以下命令，确认环境变量是否配置成功。
  ```
  echo $ACCESS_KEY_ID
  echo $SECRET_ACCESS_KEY_ID
  ```
  - 如果命令行中显示**a**设置的信息，表示设置成功。
  - 如果命令行中未显示**a**设置的信息，表示设置失败，请重新设置。

2. 计算签名

您可以通过使用编程语言的Web框架和OBS的SDK计算POST上传签名。POST表单上传是通过安全策略（policy）来限制表单上传的内容，例如规定表单上传对象的对象名前缀必须以“prefix01”开头，使用policy能够帮助您更好的管控桶中的文件。更多关于安全策略的内容，请参见**基于浏览器上传的表单中携带签名**。

参考如下**Java**示例代码获取访问凭证并计算签名：

```
@Controller
public class FormUploadCallbackController {
    String bucket = "post-callback-demo";
    // 以北京四的OBS地址为例
    String host = "obs.cn-north-4.myhuaweicloud.com";
    String endpoint = "https://" + host;
    String callbackUrl = "http://obs-demo.huaweicloud.com:12345/callback";
    //限定上传到OBS的文件前缀
    String prefix = "demo";

    @GetMapping("/obs-post-callback-signature")
    public ResponseEntity<Map<String, String>> getSignature() throws Exception {
        // 您可以通过环境变量获取访问密钥AK/SK，也可以使用其他外部引入方式传入。如果使用硬编码可能会存在泄露风险。
        // 您可以登录访问管理控制台获取访问密钥AK/SK
        String ak = System.getenv("ACCESS_KEY_ID");
        String sk = System.getenv("SECRET_ACCESS_KEY_ID");
        // 【可选】如果使用临时AK/SK和SecurityToken访问OBS，同样建议您尽量避免使用硬编码，以降低信息泄露风险。
        // 您可以通过环境变量获取访问密钥AK/SK/SecurityToken，也可以使用其他外部引入方式传入。
        // String securityToken = System.getenv("SECURITY_TOKEN");

        // 创建ObsClient实例
        // 【可选】使用临时AK/SK和SecurityToken初始化客户端
//      try ( ObsClient obsClient = new ObsClient(ak, sk, securityToken, enpoint)){
        // 使用永久AK/SK初始化客户端
        try ( ObsClient obsClient = new ObsClient(ak, sk, endpoint)){
            // 1. 创建策略条件
            // 生成基于表单上传的请求
            PostSignatureRequest request = new PostSignatureRequest();
            // 设置表单参数
            Map<String, Object> formParams = new HashMap<>();
            // 设置对象ACL为公共读，需要其它配置可自行修改
            formParams.put("x-obs-acl", "public-read");
            request.setFormParams(formParams);
            List<String> conditions = new ArrayList<>();
            // 设置Post上传请求的签名条件
            conditions.add("[\"starts-with\", \"$key\", \"demo/\"]");
            conditions.add("{\"bucket\": \"post-callback-demo\"}");
            request.setConditions(conditions);
            // 设置表单上传请求有效期，单位：秒
            request.setExpires(3600);
            PostSignatureResponse response = obsClient.createPostSignature(request);
            System.out.println("createPostSignature successfully");
            // 获取表单上传请求参数
            System.out.println("Policy:" + response.getPolicy());
            System.out.println("Signature:" + response.getSignature());
            Map<String, String> signResponse = new HashMap<>();
            signResponse.put("prefix", prefix);
            signResponse.put("accessKeyId", ak);
            signResponse.put("policy", response.getPolicy());
            signResponse.put("signature", response.getSignature());
            // 【可选】如果使用临时AK/SK和SecurityToken访问OBS,此处返回securityToken
//          signResponse.put("securityToken",securityToken);
            signResponse.put("host", host);
            signResponse.put("bucket", bucket);
            signResponse.put("callbackUrl", callbackUrl);
            signResponse.put("callbackBody", "key=$(key)&hash=$(etag)&fname=$(fname)&fsize=$(size)");
            signResponse.put("callbackBodyType", "application/json");
            return ResponseEntity.ok(signResponse);

        } catch (ObsException e) {
```

```
            System.out.println("createPostSignature failed");
            // 请求失败,打印http状态码
            System.out.println("HTTP Code:" + e.getResponseCode());
            // 请求失败,打印服务端错误码
            System.out.println("Error Code:" + e.getErrorCode());
            // 请求失败,打印详细错误信息
            System.out.println("Error Message:" + e.getErrorMessage());
            // 请求失败,打印请求id
            System.out.println("Request ID:" + e.getErrorRequestId());
            System.out.println("Host ID:" + e.getErrorHostId());
            e.printStackTrace();
            throw e;
        }
    }
}
```

步骤三：Web 端通过表单上传文件并设置上传回调

Web端接收到服务端返回的上传Policy和签名后，使用HTML表单构建请求并设置上传回调。此请求使用POST表单上传来直接调用OBS的服务端，实现文件上传。

Web端接收到服务端的响应示例如下：

```
{
    "accessKeyId": "*****************", // 密钥AK
    "bucket": "post-callback-demo",    // 需要上传的桶名
    "callbackBodyType": "application/json", // 响应体格式
    "signature": "24******************u8=", // POST上传的签名
    "prefix": "demo",   // POST上传对象名前缀
    "host": "obs.cn-north-4.myhuaweicloud.com", // POST上传host地址
    "callbackUrl": "http://obs-demo.huaweicloud.com:23450/callback",  // POST上传回调的地址
    "policy": "eyJleHBpcmF****************************************ifV19",  // POST上传policy
    "callbackBody": "key=$(key)&hash=$(etag)&fname=$(fname)&fsize=$(size)"   // POST上传回调的请求体
}
```

使用HTML表单构建请求并设置上传回调的示例代码如下：

```
<!DOCTYPE html>
<html>
<head>
    <meta charset="UTF-8">
    <title>华为云OBS表单上传</title>
</head>
<body>
<h1>OBS表单上传回调示例</h1>
<form>
    <div class="form-group">
        <label for="file" class="form-label">选择文件:</label>
        <input type="file" class="form-control" id="file" name="file" required/>
    </div>

    <button name="submit" value="Upload" type="submit">上传到OBS</button>
</form>
<div id="result"></div>

<script type="text/javascript">
    document.addEventListener('DOMContentLoaded', function () {
        const form = document.querySelector("form");
        const fileInput = document.querySelector("#file");
        const resultDiv = document.getElementById("result");

        form.addEventListener("submit", async (event) => {
            event.preventDefault();

            if (!fileInput.files.length) {
                resultDiv.innerHTML = '<p style="color:red">请选择文件</p>';
                return;
            }
```

```
        const file = fileInput.files[0];
        if (!file) {
            alert('请选择一个文件再上传。');
            return;
        }

        const filename = file.name;
        try {
            // 1. 获取签名参数
            resultDiv.innerHTML = '获取签名中...';
            const response = await fetch(`/obs-post-callback-signature`);
            const params = await response.json();

            // 2. 构建表单数据
            const formData = new FormData();
            formData.append('key', params.prefix + "/" + filename);
            formData.append('x-obs-acl', 'public-read');
            formData.append('policy', params.policy);
            formData.append('AccessKeyId', params.accessKeyId);
            formData.append('signature', params.signature);
            formData.append('callbackUrl', params.callbackUrl);
            formData.append('callbackBody', params.callbackBody);
            formData.append('callbackBodyType', params.callbackBodyType);
            // 【可选】如果服务端签名使用了SecurityToken，在Form表单中也需要设置
            // formData.append('x-obs-security-token', params['x-obs-security-token']);
            formData.append('file', file);

            // 3. 提交到OBS
            resultDiv.innerHTML = '上传中...';
            const obsEndpoint = `https://${params.bucket}.${params.host}`;

            const uploadResponse = await fetch(obsEndpoint, {
                method: 'POST',
                body: formData
            });

            if (uploadResponse.status === 200) {
                resultDiv.innerHTML = `<p style="color:green">上传成功! OBS路径: ${params.key}</p>
                        <p>回调通知将发送到: ${new
URLSearchParams(atob(params.callback)).get('callbackUrl')}</p>`;
            } else {
                const error = await uploadResponse.text(); // 使用await
                resultDiv.innerHTML = `<p style="color:red">上传失败! 状态码: ${uploadResponse.status}</p>
                        <p>${error}</p>`;
            }
        } catch (error) {
            resultDiv.innerHTML = `<p style="color:red">发生错误: ${error.message}</p>`;
        }
    });
});
</script>
</body>
</html>
```

结果验证

HTML表单中包含一个文件选择框和一个上传按钮，用户可以选择想要上传的文件然后提交表单。

当表单提交时，JavaScript代码会请求服务器获取本次上传所需要的签名和回调信息，得到正确响应之后，会构造一个FormData对象， 然后填充所有必要数据，通过fetch方法发送POST请求到OBS的服务端，完成文件上传，上传成功后会回调callbackUrl设置的地址。

图 2-8 表单上传回调示例

通过表单上传一个名为“demo-object”的文件至桶“post-callback-demo”中，上传后在OBS桶列表中的“post-callback-demo”中可以看到“demo-object”文件，即表示成功通过表单上传文件。

图 2-9 查看所上传的文件

相关文档

使用其它编程语言的Web框架和OBS的SDK计算POST上传签名信息，具体参考如下：

Java	Python	C不支持	Go不支持	BrowserJS	.NET不支持	Android	iOS不支持	PHP	Node.js

2.4 移动应用直传

2.4.1 移动应用直传方案概述

在互联网中，使用OBS作为存储在移动APP（手机Android、iOS应用）中获得了越来越广泛的应用。Android和iOS应用使用OBS服务时，不能直接存储访问密钥（AK/

SK），这样可能会导致访问密钥（AK/SK）被黑客软件破解获取，进而可能导致存放在云存储中的文件数据被窃取，甚至被篡改。

为了更好地保护应用数据，避免被攻击后数据泄露以及越权访问的风险，为您推荐以下两种方法。

- **方法一：使用临时安全凭证直传OBS**
- **方法二：使用预签名URL访问OBS**

方法一使用临时的AK/SK，可以避免AK/SK泄露的风险。推荐您优先使用临时安全凭证直传OBS。

2.4.2 使用临时安全凭证直传 OBS

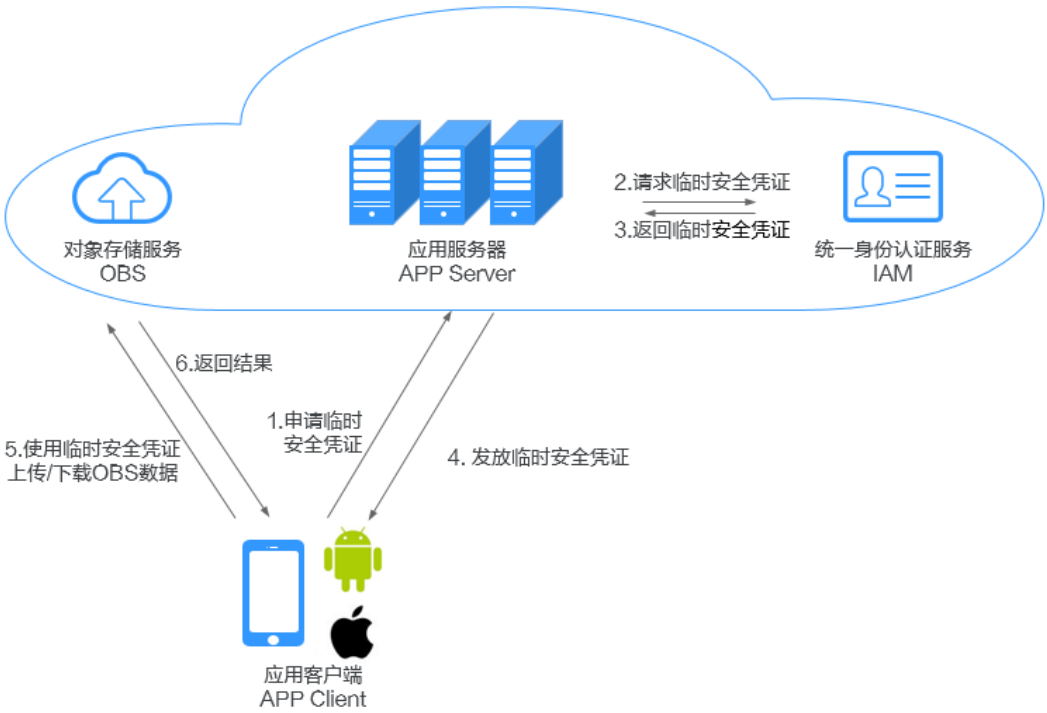
方案架构

使用的方式，可以将应用客户端的数据直传至OBS，或者将存储在OBS里的数据进行下载。具体流程如**图2-10**。

OBS支持使用临时安全凭证（临时AK/SK和securitytoken）进行授权访问，同时支持为临时安全凭证配置权限策略来指定使用该临时安全凭证时允许执行的操作。**什么是临时安全凭证?**

移动应用客户端可以使用指定了权限策略的临时安全凭证来访问OBS，实现数据直传，整个过程不会暴露用户的永久AK/SK，降低了账号泄露带来的安全风险。

图 2-10 使用临时安全凭证直传 OBS 流程



角色分析如下：

- 应用客户端：即最终用户手机上的APP，负责向应用服务器发出申请临时安全凭证的请求，以及访问OBS完成数据上传或下载。

- 应用服务器：即提供该Android/iOS应用的开发者开发的APP后台服务，用于用户管理和授权管理等。
- 对象存储服务：即华为云对象存储服务，负责处理移动应用的数据请求。
- 统一身份认证服务：即华为云统一身份认证服务，负责生成临时安全凭证。

实现流程如下：

1. 应用客户端向应用服务器申请一个临时操作凭证。
2. 应用服务器向统一身份认证服务请求临时安全凭证。
3. 统一身份认证服务向应用服务器返回临时安全凭证。
4. 应用服务器将临时安全凭证发放给应用客户端。
5. 应用客户端使用安全凭证完成OBS数据上传下载。

前提条件

已创建桶，并将桶权限设置为私有读写或者公共读私有写。

详细操作步骤请参见**创建桶**和**配置桶策略**。

资源和成本规划

最佳实践中涉及的资源如下：

表 2-5 资源说明

资源	资源说明
应用客户端（APP Client）	最终用户手机上的APP，负责向应用服务器发出申请临时安全凭证的请求，以及访问OBS完成数据上传或下载。
应用服务器（APP Server）	提供该Android/iOS应用的开发者开发的APP后台服务，用于用户管理和授权管理等。
对象存储服务（OBS）	华为云对象存储服务，负责处理移动应用的数据请求。
统一身份认证服务（IAM）	华为云统一身份认证服务，负责生成临时安全凭证。

实施步骤

步骤1 获取OBS SDK开发包和IAM SDK开发包。

OBS SDK请在**SDK开发指南**中获取。

IAM SDK开发包请在**IAM开发工具包**获取。

步骤2 模拟应用服务器向IAM请求临时安全凭证和返回安全凭证。

过程如下：

1. 获取用户的IAM用户Token。
   API请参见**获取IAM用户Token（使用密码）**，SDK请参见**SDK中心**。

2. 使用Token获取临时安全凭证（临时AK/SK和securitytoken），获取时需要通过Policy字段指定该安全凭证允许执行的操作权限。

   API请参见**通过token获取临时访问密钥和securitytoken**，SDK请参见**SDK中心**。

示例：获取一个有效期为900秒的临时安全凭证，该凭证只允许上传数据到桶hi-company的APPClient/APP-1/目录下。

```
{
    "auth":{
        "identity":{
            "policy":{
                "Version":"1.1",
                "Statement":[
                    {
                        "Action":[
                            "obs:object:PutObject"
                        ],
                        "Resource":[
                            "obs:*:*:object:hi-company/APPClient/APP-1/*"
                        ],
                        "Effect":"Allow"
                    }
                ]
            },
            "token":{
                "duration-seconds":900,
                "id":"MIIDkgYJKoZIhvcNAQcCoIIDgzCCA38CAQExDTALMEXXXXX..."
            },
            "methods":[
                "token"
            ]
        }
    }
}
```

步骤3 初始化应用客户端中OBS client。

初始化示例：

- Android

```
String endPoint = "https://your-endpoint";
// 认证用的ak和sk硬编码到代码中或者明文存储都有很大的安全风险，建议在配置文件或者环境变量中密文存放，使用时解密，确保安全；本示例以ak和sk保存在环境变量中为例，运行本示例前请先在本地环境中设置环境变量ACCESS_KEY_ID和SECRET_ACCESS_KEY_ID。
// 您可以登录访问管理控制台获取访问密钥AK/SK，获取方式请参见https://support.huaweicloud.com/usermanual-ca/ca_01_0003.html
String ak = System.getenv("ACCESS_KEY_ID");
String sk = System.getenv("SECRET_ACCESS_KEY_ID");
String token = System.getenv("Security_Token");

// 创建ObsConfiguration配置类实例
ObsConfiguration config = new ObsConfiguration();
config.setEndPoint(endPoint);
config.setSocketTimeout(30000);
config.setConnectionTimeout(10000);

// 创建ObsClient实例
ObsClient obsClient = new ObsClient(ak, sk,token,config);

// 使用访问OBS

// 关闭obsClient
obsClient.close();
```


说明

- endPoint即终端节点，可通过**地区和终端节点**查询。
- ak和sk即临时AK/SK，token即securitytoken，获取方式请参见**访问密钥（AK/SK）**。

- iOS

```
NSString *endPoint = @"your-endpoint";
// 认证用的ak和sk硬编码到代码中或者明文存储都有很大的安全风险，建议在配置文件或者环境变量中密文存放，使用时解密，确保安全；本示例以ak和sk保存在环境变量中为例，运行本示例前请先在本地环境中设置环境变量AccessKeyID和SecretAccessKey。
// 您可以登录访问管理控制台获取访问密钥AK/SK，获取方式请参见https://support.huaweicloud.com/usermanual-ca/ca_01_0003.html
NSString *SK = getenv("AccessKeyID");
NSString *AK = getenv("SecretAccessKey");
// 初始化身份验证
OBSStaticCredentialProvider *credentailProvider = [[OBSStaticCredentialProvider alloc] initWithAccessKey:AK secretKey:SK];
securityTokencredentailProvider.securityToken = @"*** Provide your Security Token ***";
// 初始化服务配置
OBSServiceConfiguration *conf = [[OBSServiceConfiguration alloc] initWithURLString:endPoint credentialProvider:credentialProvider];
// 初始化
clientOBSClient *client  = [[OBSClient alloc] initWithConfiguration:conf];
```

说明

- endPoint即终端节点，可通过**地区和终端节点**查询。
- ak和sk即临时AK/SK，token即securitytoken，获取方式请参见**访问密钥（AK/SK）**。

- web js

```
// 未引入AMD，直接通过构造函数创建ObsClient实例
var obsClient = new ObsClient({
        // 认证用的ak和sk硬编码到代码中或者明文存储都有很大的安全风险，建议在配置文件或者环境变量中密文存放，使用时解密，确保安全；本示例以ak和sk保存在环境变量中为例，运行本示例前请先在本地环境中设置环境变量AccessKeyID和SecretAccessKey。
        // 您可以登录访问管理控制台获取访问密钥AK/SK，获取方式请参见https://support.huaweicloud.com/usermanual-ca/ca_01_0003.html
        access_key_id: process.env.AccessKeyID,
        secret_access_key: process.env.SecretAccessKey,
        security_token: process.env.SecurityToken,
        server : 'https://your-endpoint'
});
// 使用访问OBS

// 引入AMD，通过依赖注入的构造函数创建ObsClient实例
var obsClient;
define(['ObsClient'], function(ObsClient){
    obsClient = new ObsClient({
        // 认证用的ak和sk硬编码到代码中或者明文存储都有很大的安全风险，建议在配置文件或者环境变量中密文存放，使用时解密，确保安全；本示例以ak和sk保存在环境变量中为例，运行本示例前请先在本地环境中设置环境变量AccessKeyID和SecretAccessKey。
        // 您可以登录访问管理控制台获取访问密钥AK/SK，获取方式请参见https://support.huaweicloud.com/usermanual-ca/ca_01_0003.html
        access_key_id: process.env.AccessKeyID,
        secret_access_key: process.env.SecretAccessKey,
        security_token: process.env.SecurityToken,
        server : 'https://your-endpoint'
    });
    // 使用访问OBS
});
```

说明

- endPoint即终端节点，可通过**地区和终端节点**查询。
- ak和sk即临时AK/SK，token即securitytoken，获取方式请参见**访问密钥（AK/SK）**。

步骤4 使用临时安全凭证完成OBS数据上传下载，示例如下。

- Android

```
// obsClient 是步骤3创建的ObsClient实例

// 流式上传
String content = "Hello OBS";
obsClient.putObject("bucketname", "objectname", new ByteArrayInputStream(content.getBytes()));

// 流式下载
ObsObject obsObject = obsClient.getObject("bucketname", "objectname");
// 读取对象内容
Log.i("GetObject", "Object content:");
InputStream input = obsObject.getObjectContent();
byte[] b = newbyte[1024];
ByteArrayOutputStream bos = new ByteArrayOutputStream();
int len;
while ((len=input.read(b)) != -1){
    bos.write(b, 0, len);
}
Log.i("GetObject", new String(bos.toByteArray()));
bos.close();
input.close();
```

说明

  - Android SDK更多上传场景示例请参考**上传对象**。
  - Android SDK更多下载场景示例请参考**下载对象**。

- iOS

```
// obsClient 是步骤3创建的ObsClient实例

// 流式上传
OBSPutObjectWithDataRequest *request = [[OBSPutObjectWithDataRequest
alloc]initWithBucketName:@"bucketname" objectKey:@"objectname" uploadData:[@"hello"
dataUsingEncoding:NSUTF8StringEncoding]];

// 流式下载
OBSGetObjectToDataRequest *request = [[OBSGetObjectToDataRequest
alloc]initWithBucketName:@"bucketname" objectKey:@"objectname"];
// 下载进度
request.downloadProgressBlock = ^(int64_t bytesWritten, int64_t totalBytesWritten, int64_t
totalBytesExpectedToWrite) {
 NSLog(@"%0.1f%%",(float)(totalBytesWritten)*100/(float)totalBytesExpectedToWrite);
};
// 下载的数据
__block NSMutableData *objectData = [NSMutableData new];
request.onReceiveDataBlock = ^(NSData *data) {
    [objectData appendData:data];
};
// 下载结果
[client getObject:request completionHandler:^(OBSGetObjectResponse *response, NSError *error){
    NSLog(@"%@",response);
}] ;
```

说明

  - IOS SDK更多上传场景示例请参考**上传对象**。
  - IOS SDK更多下载场景示例请参考**下载对象**。

- web js

```
// obsClient 是步骤3创建的ObsClient实例

// 文本上传
obsClient.putObject({
        //使用Body参数指定待上传的字符串。
        Bucket: 'bucketname',
        Key: 'objectname',
        Body: 'Hello OBS'
}, function (err, result) {
```

```
        if(err){
            console.error('Error-->' + err);
        }else{
            console.log('Status-->' + result.CommonMsg.Status);
        }
});

// 文本下载
obsClient.getObject({
        Bucket : 'bucketname',
        Key : 'objectname'
}, function (err, result) {
        if(err){
            console.error('Error-->' + err);
        }else{
            console.log('Status-->' + result.CommonMsg.Status);
            if(result.CommonMsg.Status < 300 && result.InterfaceResult){
                // 读取对象内容
                console.log('Object Content:');
                console.log(result.InterfaceResult.Content);
            }
        }
});
```

说明

- BrowserJS SDK 属于web js，可以运用在浏览器端。
- BrowserJS SDK更多上传场景示例请参考**上传对象**。
- BrowserJS SDK更多下载场景示例请参考**下载对象**。

----结束

2.4.3 使用临时安全凭证直传 OBS 并设置上传回调

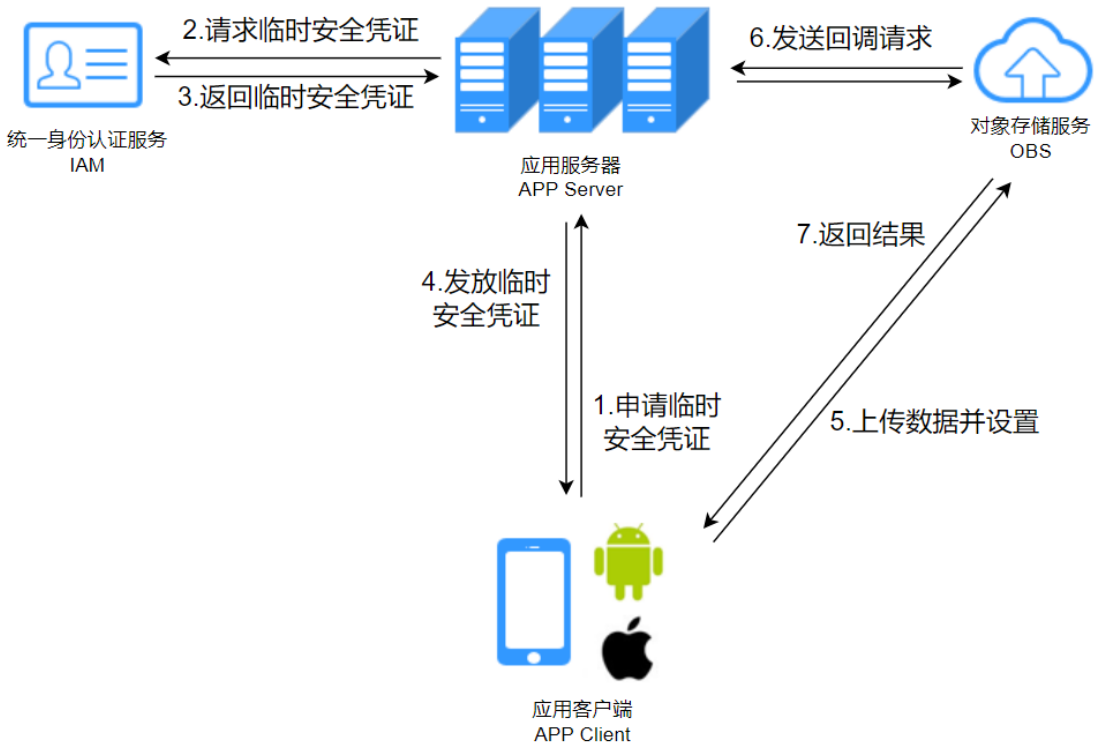
应用场景

OBS支持使用临时安全凭证（临时AK/SK和securitytoken）进行授权访问，同时支持为临时安全凭证配置权限策略来指定使用该临时安全凭证时允许执行的操作。临时安全凭证的含义请参见**什么是临时安全凭证?**

移动应用客户端可以使用指定了权限策略的临时安全凭证来访问OBS，实现数据直传并设置上传回调，如**图2-11**所示。整个过程不会暴露用户的永久AK/SK，降低账号泄露带来的安全风险。

方案架构

图 2-11 使用临时安全凭证直传 OBS 并设置上传回调流程



角色分析如下：

- 应用客户端：即最终用户手机上的APP，负责向应用服务器发出申请临时安全凭证的请求，以及访问OBS完成数据上传或下载。
- 应用服务器：即提供该Android/iOS应用的开发者开发的APP后台服务，用于用户管理和授权管理，接收回调请求等。
- 对象存储服务：即华为云对象存储服务，负责处理移动应用的数据请求。
- 统一身份认证服务：即华为云统一身份认证服务，负责生成临时安全凭证。

实现流程如下：

1. 应用客户端向应用服务器申请一个临时操作凭证。
2. 应用服务器向统一身份认证服务请求一个临时安全凭证。
3. 统一身份认证服务向应用服务器返回一个临时安全凭证。
4. 应用服务器将临时安全凭证发放给应用客户端。
5. 应用客户端使用安全凭证完成OBS数据上传并设置回调参数。
6. OBS上传完成后回调客户的回调Server。
7. OBS返回给应用客户端结果。

前提条件

已创建桶，并将桶权限设置为私有读写或者公共读私有写。

详细操作步骤请参见**创建桶**和**配置桶策略**。

资源规划

最佳实践中涉及的资源如下：

表 2-6 资源说明

资源	资源说明
应用客户端（APP Client）	最终用户手机上的APP，负责向应用服务器发出申请临时安全凭证的请求，以及访问OBS完成数据上传或下载。
应用服务器（APP Server）	提供该Android/iOS应用的开发者开发的APP后台服务，用于用户管理和授权管理，接收回调请求等。
对象存储服务（OBS）	华为云对象存储服务，负责处理移动应用的数据请求。
统一身份认证服务（IAM）	华为云统一身份认证服务，负责生成临时安全凭证。

实施步骤

步骤1 获取OBS SDK开发包和IAM SDK开发包。

OBS SDK请在**SDK开发指南**中获取。

IAM SDK开发包请在**IAM开发工具包**获取。

步骤2 模拟应用服务器向IAM请求临时安全凭证和返回安全凭证。

过程如下：

1. 获取用户的IAM用户Token。
   API请参见**获取IAM用户Token（使用密码）**，SDK请参见**SDK中心**。
2. 使用Token获取临时安全凭证（临时AK/SK和securitytoken），获取时需要通过Policy字段指定该安全凭证允许执行的操作权限。
   API请参见**通过token获取临时访问密钥和securitytoken**，SDK请参见**SDK中心**。

示例：获取一个有效期为900秒的临时安全凭证，该凭证只允许上传数据到桶hi-company的APPClient/APP-1/目录下。

```
{
    "auth":{
        "identity":{
            "policy":{
                "Version":"1.1",
                "Statement":[
                    {
                        "Action":[
                            "obs:object:PutObject"
                        ],
                        "Resource":[
                            "obs:*:*:object:hi-company/APPClient/APP-1/*"
                        ],
                        "Effect":"Allow"
                    }
                ]
            },
```

```
        "token":{
            "duration-seconds":900,
            "id":"MIIDkgYJKoZIhvcNAQcCoIIDgzCCA38CAQExDTALMEXXXXX..."
        },
        "methods":[
            "token"
        ]
    }
  }
}
```

步骤3 初始化应用客户端中OBS client。

初始化示例：

- Android

```
String endPoint = "https://your-endpoint";
// 认证用的ak和sk硬编码到代码中或者明文存储都有很大的安全风险，建议在配置文件或者环境变量中密文存放，使用时解密，确保安全；本示例以ak和sk保存在环境变量中为例，运行本示例前请先在本地环境中设置环境变量ACCESS_KEY_ID和SECRET_ACCESS_KEY_ID。
// 您可以登录访问管理控制台获取访问密钥AK/SK，获取方式请参见https://support.huaweicloud.com/usermanual-ca/ca_01_0003.html
String ak = System.getenv("ACCESS_KEY_ID");
String sk = System.getenv("SECRET_ACCESS_KEY_ID");
String token = System.getenv("Security_Token");

// 创建ObsConfiguration配置类实例
ObsConfiguration config = new ObsConfiguration();
config.setEndPoint(endPoint);
config.setSocketTimeout(30000);
config.setConnectionTimeout(10000);

// 创建ObsClient实例
ObsClient obsClient = new ObsClient(ak, sk,token,config);

// 使用访问OBS

// 关闭obsClient
obsClient.close();
```

说明

  - endPoint即终端节点，可通过**地区和终端节点**查询。
  - ak和sk即临时AK/SK，token即securitytoken，获取方式请参见**访问密钥（AK/SK）**。

- iOS

```
NSString *endPoint = @"your-endpoint";
// 认证用的ak和sk硬编码到代码中或者明文存储都有很大的安全风险，建议在配置文件或者环境变量中密文存放，使用时解密，确保安全；本示例以ak和sk保存在环境变量中为例，运行本示例前请先在本地环境中设置环境变量AccessKeyID和SecretAccessKey。
// 您可以登录访问管理控制台获取访问密钥AK/SK，获取方式请参见https://support.huaweicloud.com/usermanual-ca/ca_01_0003.html
NSString *SK = getenv("AccessKeyID");
NSString *AK = getenv("SecretAccessKey");
// 初始化身份验证
OBSStaticCredentialProvider *credentailProvider = [[OBSStaticCredentialProvider alloc] initWithAccessKey:AK secretKey:SK];
securityTokencredentailProvider.securityToken = @"*** Provide your Security Token ***";
// 初始化服务配置
OBSServiceConfiguration *conf = [[OBSServiceConfiguration alloc] initWithURLString:endPoint credentialProvider:credentialProvider];
// 初始化
clientOBSClient *client  = [[OBSClient alloc] initWithConfiguration:conf];
```

说明

- endPoint即终端节点，可通过**地区和终端节点**查询。
- ak和sk即临时AK/SK，token即securitytoken，获取方式请参见**访问密钥（AK/SK）**。

- web js

```
// 未引入AMD，直接通过构造函数创建ObsClient实例
var obsClient = new ObsClient({
        // 认证用的ak和sk硬编码到代码中或者明文存储都有很大的安全风险，建议在配置文件或者环境变量中密文存放，使用时解密，确保安全；本示例以ak和sk保存在环境变量中为例，运行本示例前请先在本地环境中设置环境变量AccessKeyID和SecretAccessKey。
        // 您可以登录访问管理控制台获取访问密钥AK/SK，获取方式请参见https://support.huaweicloud.com/usermanual-ca/ca_01_0003.html
        access_key_id: process.env.AccessKeyID,
        secret_access_key: process.env.SecretAccessKey,
        security_token: process.env.SecurityToken,
        server : 'https://your-endpoint'
});
// 使用访问OBS

// 引入AMD，通过依赖注入的构造函数创建ObsClient实例
var obsClient;
define(['ObsClient'], function(ObsClient){
    obsClient = new ObsClient({
        // 认证用的ak和sk硬编码到代码中或者明文存储都有很大的安全风险，建议在配置文件或者环境变量中密文存放，使用时解密，确保安全；本示例以ak和sk保存在环境变量中为例，运行本示例前请先在本地环境中设置环境变量AccessKeyID和SecretAccessKey。
        // 您可以登录访问管理控制台获取访问密钥AK/SK，获取方式请参见https://support.huaweicloud.com/usermanual-ca/ca_01_0003.html
        access_key_id: process.env.AccessKeyID,
        secret_access_key: process.env.SecretAccessKey,
        security_token: process.env.SecurityToken,
        server : 'https://your-endpoint'
    });
    // 使用访问OBS
});
```

说明

- endPoint即终端节点，可通过**地区和终端节点**查询。
- ak和sk即临时AK/SK，token即securitytoken，获取方式请参见**访问密钥（AK/SK）**。

步骤4 使用临时安全凭证完成OBS数据上传并设置上传回调，示例如下。回调的详细参数设置请参考API说明**回调**。

- Android

```
// obsClient 是步骤3创建的ObsClient实例

// 流式上传并设置callback，下面示例中对象上传到OBS后，会向http://www.example.com/callback地址发送POST回调请求
String content = "Hello OBS";
obsClient.putObject("bucketname", "objectname", new ByteArrayInputStream(content.getBytes()));
Callback callback = new Callback();
callback.setCallbackBody("{\"bucket\":\"$(bucket)\",\"key\":\"$(key)\",\"override\":\"$(override)\"}");
callback.setCallbackBodyType("application/json");
callback.setCallbackUrl("http://www.example.com/callback");
PutObjectRequest putReq = new PutObjectRequest();
putReq.setCallback(callback);
putReq.setBucketName("BucketName");
putReq.setObjectKey("ObjectName");
putReq.setInput(new ByteArrayInputStream("Hello OBS".getBytes()));
obsClient.putObject(putReq);
```

- iOS

```
// obsClient 是步骤3创建的ObsClient实例
NSString* exampleCallbackUrl = @"http://www.example.com/callback";
NSString* exampleCallbackBody = @"bucket=$(bucket)&key=$(key)&override=$(override)";
NSString* exampleCallbackBodyType = @"application/json";
```

```
// 流式上传
OBSPutObjectWithDataRequest *putObjectRequest = [[OBSPutObjectWithDataRequest
alloc]initWithBucketName:@"bucketname" objectKey:@"objectname" uploadData:[@"hello"
dataUsingEncoding:NSUTF8StringEncoding]];
putObjectRequest.callback = [[OBSCallback alloc] initWithUrl:exampleCallbackUrl
                                                    withBody:exampleCallbackBody
                                                    withBodyType:exampleCallbackBodyType
                                                    withHost:exampleCallbackHost];
// 初始化上传对象异步任务
OBSBFTask* putObjectTask = [client putObject:putObjectRequest
completionHandler:^(OBSPutObjectResponse *response, NSError *error) {
    if(error){
        // 上传失败
        NSLog(@"PutObject failed:%@", error);
    }
    if(response){
        NSLog(@"PutObject response:%@", response);
        NSString* callbackResponseString = [[NSString alloc] initWithData:response.responseRawData
                                                                  encoding:NSUTF8StringEncoding];
        NSLog(@"PutObject callbackResponseString:%@", callbackResponseString);
    }
}];
// 等待上传对象异步任务完成
[putObjectTask waitUntilFinished];
```

- web js

```
// obsClient 是步骤3创建的ObsClient实例

// 文本上传并设置上传回调参数
obsClient.putObject({
        //使用Body参数指定待上传的字符串
        Bucket: 'bucketname',
        Key: 'objectname',
        Body: 'Hello OBS',
        CallbackUrl: 'http://www.example.com/callback',
        CallbackBody: 'bucket=$(bucket)&key=$(key)&override=$(override)',
        CallbackBodyType: 'application/json'
}, function (err, result) {
        if(err){
            console.error('Error-->' + err);
        }else{
            console.log('Status-->' + result.CommonMsg.Status);
        }
});
```

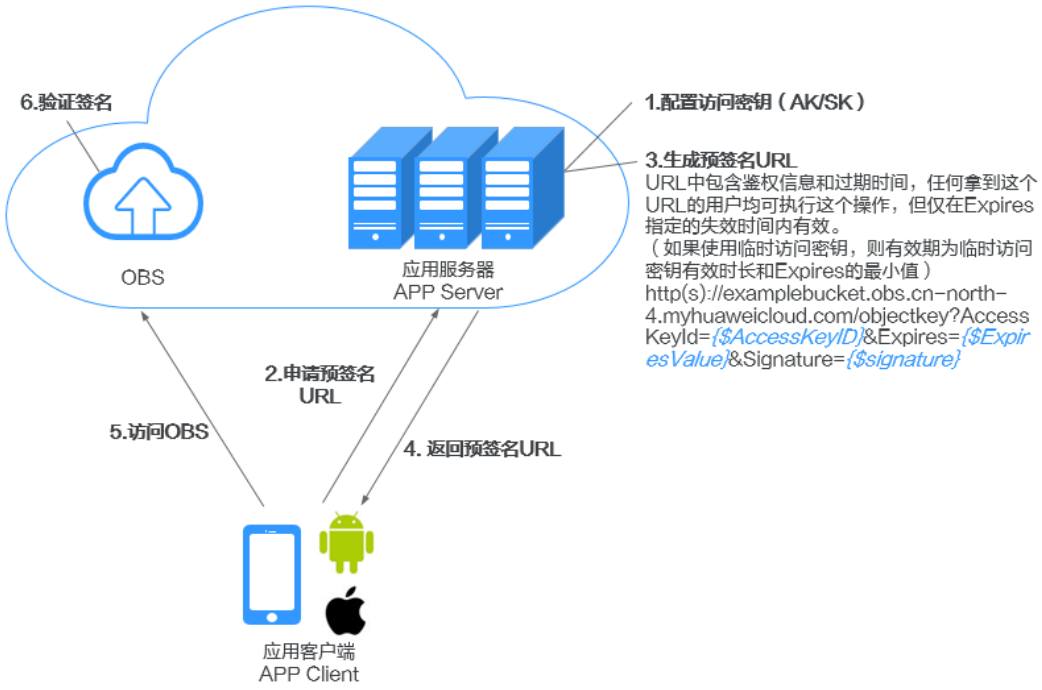
----结束

2.4.4 使用预签名 URL 直传 OBS

方案架构

应用客户端每个请求都将向应用服务器申请预签名URL，该预签名URL有效期由应用服务器管理。具体流程如图2-12。

图 2-12 移动应用访问 OBS 数据流程



角色分析如下：

- 应用客户端：即最终用户手机上的APP，负责向应用服务器申请包含预签名的URL，以及访问OBS完成数据上传或下载。
- 应用服务器：即提供该Android/iOS应用的开发者开发的APP后台服务，用于管理凭证信息以及发放预签名URL。
- OBS：即华为云对象存储，负责处理移动应用的数据请求。

实现流程如下：

1. 移动应用客户端向应用服务器申请一个预签名的URL。

   Android和iOS应用使用OBS服务时，不需要存储访问密钥（AK/SK）。应用在上传前必须向用户的应用服务器申请访问OBS的URL，并携带必须信息，包括请求类型、资源路径和资源名称。比如上传操作需要标识该URL为上传请求，需要包含上传的路径以及上传对象的名称；下载操作需要标识该URL为下载请求，需要包含所下载对象的名称。

2. 应用服务器作为可信设备，在应用服务器上存储访问密钥（AK/SK）。应用服务器在验证客户端身份合法之后，使用应用服务器保存的访问密钥（AK/SK）以及客户端访问的资源、操作类型生成预签名URL。举例：

   ```
   https://examplebucket.obs.cn-north-4.myhuaweicloud.com/objectkey?
   AccessKeyId=AccessKeyID&Expires=1532779451&Signature=0Akylf43Bm3mD1bh2rM3dmVp1Bo%3D
   ```

3. Android/iOS移动应用获取此URL，直接使用该URL操作数据，比如上传或者下载操作。

   URL中会包含用户的AK、签名、有效期、资源等信息，任何拿到这个URL的人均可执行这个操作。OBS服务收到这个请求并验证签名后，认为该请求就是签发URL的用户自己在执行操作。例如构造一个携带签名信息的下载对象URL，拿到相应URL的人能下载这个对象，但该URL只在Expires指定的失效时间内有效（如果使用临时访问密钥，有效期为临时访问密钥有效时长和Expires的最小值）。URL中携带签名主要用于在不提供给其他人SK的情况下，让其他人能用预签发的URL来进行身份认证，并执行预定义的操作。

前提条件

- 创建桶。
  在OBS控制台上创建桶。需要将桶权限设置为私有读写或者公共读私有写。
  详细操作步骤请参见**创建桶**和**配置桶策略**。
- 获取访问密钥（AK/SK）。
  预签名URL需要通过访问密钥生成，请参考**访问密钥（AK/SK）**获取。其中访问密钥（AK/SK）对应的用户需设置所需的最小权限，具体权限设置方法参考**向IAM用户授予OBS资源权限**。

资源和成本规划

最佳实践中涉及的资源如下：

表 2-7 资源说明

资源	资源说明
应用客户端（APP Client）	最终用户手机上的APP，负责向应用服务器申请包含预签名的URL，以及访问OBS完成数据上传或下载。
应用服务器（APP Server）	提供该Android/iOS应用的开发者开发的APP后台服务，用于管理凭证信息以及发放预签名URL。
对象存储服务（OBS）	华为云对象存储服务，负责处理移动应用的数据请求。

实施步骤

步骤1 配置应用服务器。

1. 获取SDK开发包。
   请在各语言的**SDK开发指南**中获取。
2. 生成预签名URL的代码。
   预签名URL的计算方法请参考**URL中携带签名**。
   下述示例以在应用服务器中使用Java语言开发进行举例。

   说明

   应用服务器需要根据APP操作类型，识别公共请求消息头与自定义请求消息头，并将其加入到预签名URL生成签名计算中。
   - 公共请求消息头，请参考**构造请求**。
   - 自定义请求消息头，请参考对应操作的API文档。例如PUT上传，参考**PUT上传API**。

```
// 本次请求的桶的endpoint
String endPoint = "http://your-endpoint";

// 认证用的ak和sk硬编码到代码中或者明文存储都有很大的安全风险，建议在配置文件或者环境变量中密文存放，使用时解密，确保安全；本示例以ak和sk保存在环境变量中为例，运行本示例前请先在本地环境中设置环境变量ACCESS_KEY_ID和SECRET_ACCESS_KEY_ID。
// 您可以登录访问管理控制台获取访问密钥AK/SK，获取方式请参见https://support.huaweicloud.com/usermanual-ca/ca_01_0003.html
String ak = System.getenv("ACCESS_KEY_ID");
String sk = System.getenv("SECRET_ACCESS_KEY_ID");
```

```
// 创建ObsClient实例
ObsClient obsClient = new ObsClient(ak, sk, endPoint);
// 替换您的过期时间，单位是秒
long expireSeconds = 3600L;

// 替换成您对应的操作
TemporarySignatureRequest request = new TemporarySignatureRequest(HttpMethodEnum.PUT,
expireSeconds);

// 替换为请求本次操作访问的桶名和对象名
request.setBucketName("bucketname");
request.setObjectKey("objectname");

TemporarySignatureResponse response = obsClient.createTemporarySignature(request);

// 成功返回预签名URL，如下打印URL信息
System.out.println(response.getSignedUrl());
```

更多相关介绍和示例代码，请参见**使用URL进行授权访问**。

步骤2 移动应用客户端使用获取到的预签名URL发送OBS请求。

```
public class Demo extends Activity
{
    private static String bucketName = "my-obs-bucket-demo";
    private static String objectKey = "my-obs-object-key-demo";
    private static OkHttpClient httpClient;
    private static StringBuffer sb;

    @Override
    protected void onCreate(Bundle savedInstanceState)
    {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.activity_main);
        sb = new StringBuffer();
        /*
        * Constructs a client instance with your account for accessing OBS
        */
        httpClient = new OkHttpClient.Builder().followRedirects(false).retryOnConnectionFailure(false)
              .cache(null).build();
        final TextView tv = (TextView)findViewById(R.id.tv);
        tv.setText("Click to start test");
        tv.setOnClickListener(new View.OnClickListener()
        {
            @Override
            public void onClick(View v)
            {
                tv.setClickable(false);
                AsyncTask<Void, Void, String> task = new DownloadTask();
                task.execute();
            }
        });
    }

    class DownloadTask extends AsyncTask<Void, Void, String>
    {
        @Override
        protected String doInBackground(Void... params)
        {
            try
            {
                /*
                 * 这里需要您自己构造上传对象请求到应用服务器来生成到OBS请求的预签名URL
                 * 假如响应结果存放在：response，通过方法获取getSignedUrl()
                 */
                sb.append("Uploading a new object to OBS from a file\n\n");
                Request.Builder builder = new Request.Builder();
                // 使用PUT请求上传对象
                Request httpRequest =
builder.url(response.getSignedUrl()).put(RequestBody.create(MediaType.parse(contentType), "Hello
```

```
OBS".getBytes("UTF-8"))).build();
            Call c = httpClient.newCall(httpRequest);
            Response res = c.execute();
            sb.append("\tStatus:" + res.code());
            if (res.body() != null) {
                sb.append("\tContent:" + res.body().string() + "\n");
            }
            res.close();

            /*
             * 这里需要您自己构造下载对象请求到应用服务器来生成到OBS请求的预签名URL
             * 假如响应结果存放在：response，通过方法获取getSignedUrl()
             */
            sb.append("Downloading an object\n\n");
            Request.Builder builder = new Request.Builder();
            // 使用GET请求下载对象
            Request httpRequest = builder.url(response.getSignedUrl()).get().build();
            OkHttpClient httpClient = new
OkHttpClient.Builder().followRedirects(false).retryOnConnectionFailure(false).cache(null).build();
            Call c = httpClient.newCall(httpRequest);
            Response res = c.execute();
            System.out.println("\tStatus:" + res.code());
            if (res.body() != null) {
                sb.append("\tContent:" + res.body().string() + "\n");
            }
            res.close();

            return sb.toString();
        }
        catch (Exception e)
        {
            sb.append("\n\n");
            sb.append(e.getMessage());
            return sb.toString();
        }
        finally
        {
            if (httpClient != null)
            {
                try
                {
                    /*
                     * Close obs client
                     */
                    httpClient.close();
                }
                catch (IOException e)
                {
                }
            }
        }
    }

    @Override
    protected void onPostExecute(String result)
    {
        TextView tv = (TextView)findViewById(R.id.tv);
        tv.setText(result);
        tv.setOnClickListener(null);
        tv.setMovementMethod(ScrollingMovementMethod.getInstance());
    }
  }
}
```

----结束

相关参考

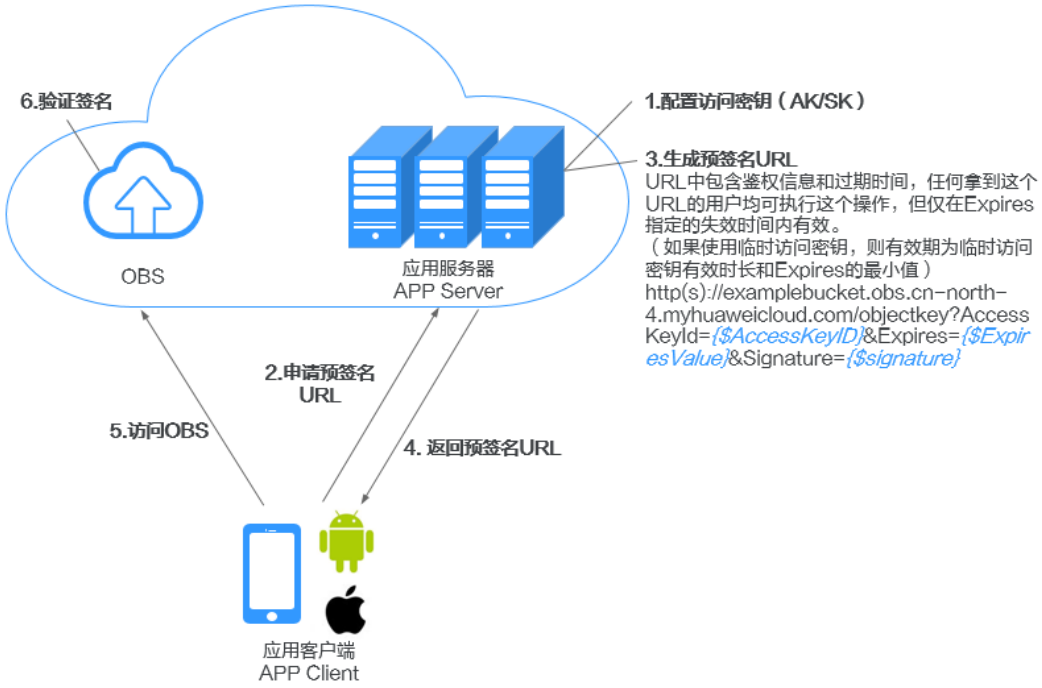
- Java SDK接口参考文档
- Java SDK依赖缺失和依赖冲突的解决方法

2.4.5 使用预签名 URL 直传 OBS（鸿蒙版）

方案架构

应用客户端每个请求都将向应用服务器申请预签名URL，该预签名URL有效期由应用服务器管理。具体流程如图2-13。

图 2-13 移动应用访问 OBS 数据流程



角色分析如下：

- 应用客户端：即最终用户手机上的APP，负责向应用服务器申请包含预签名的URL，以及访问OBS完成数据上传或下载。
- 应用服务器：即提供该Android/iOS/**Harmony**应用的开发者开发的APP后台服务，用于管理凭证信息以及发放预签名URL。
- OBS：即华为云对象存储，负责处理移动应用的数据请求。

实现流程如下：

1. 移动应用客户端向应用服务器申请一个预签名的URL。

   Android/iOS/**Harmony**应用使用OBS服务时，不需要存储访问密钥（AK/SK）。应用在上传前必须向用户的应用服务器申请访问OBS的URL，并携带必须信息，包括请求类型、资源路径和资源名称。比如上传操作需要标识该URL为上传请求，需要包含上传的路径以及上传对象的名称；下载操作需要标识该URL为下载请求，需要包含所下载对象的名称。

2. 应用服务器作为可信设备，在应用服务器上存储访问密钥（AK/SK）。应用服务器在验证客户端身份合法之后，使用应用服务器保存的访问密钥（AK/SK）以及客户端访问的资源、操作类型生成预签名URL。举例：
```
https://examplebucket.obs.cn-north-4.myhuaweicloud.com/objectkey?
AccessKeyId=AccessKeyID&Expires=1532779451&Signature=0Akylf43Bm3mD1bh2rM3dmVp1Bo%3D
```
3. Android/iOS/**Harmony**移动应用获取此URL，直接使用该URL操作数据，比如上传或者下载操作。

   URL中会包含用户的AK、签名、有效期、资源等信息，任何拿到这个URL的人均可执行这个操作。OBS服务收到这个请求并验证签名后，认为该请求就是签发URL的用户自己在执行操作。例如构造一个携带签名信息的下载对象URL，拿到相应URL的人能下载这个对象，但该URL只在Expires指定的失效时间内有效（如果使用临时访问密钥，有效期为临时访问密钥有效时长和Expires的最小值）。URL中携带签名主要用于在不提供给其他人SK的情况下，让其他人能用预签发的URL来进行身份认证，并执行预定义的操作。

资源和成本规划

最佳实践中涉及的资源如下：

表 2-8 资源说明

资源	资源说明
应用客户端（APP Client）	最终用户手机上的APP，负责向应用服务器申请包含预签名的URL，以及访问OBS完成数据上传或下载。
应用服务器（APP Server）	提供该Android/iOS/Harmony应用的开发者开发的APP后台服务，用于管理凭证信息以及发放预签名URL。
对象存储服务（OBS）	华为云对象存储服务，负责处理移动应用的数据请求。

前提条件

- 创建桶。

  在OBS控制台上创建桶。需要将桶权限设置为私有读写或者公共读私有写。

  详细操作步骤请参见**创建桶**和**配置桶策略**。
- 获取访问密钥（AK/SK）。

  预签名URL需要通过访问密钥生成，请参考**访问密钥（AK/SK）**获取。其中访问密钥（AK/SK）对应的用户需设置所需的最小权限，具体权限设置方法参考**向IAM用户授予OBS资源权限**。
- 创建应用服务器。

  此处以ECS为例。请您进入ECS购买页面，根据如下内容进行创建或选择购买ECS实例所需的基础资源。具体操作详情请参见**自定义购买ECS**。

  a. **选择计费模式&区域&可用区**

     i. 根据业务需求，选择合适的计费模式。本文选择操作相对灵活的按需计费模式。

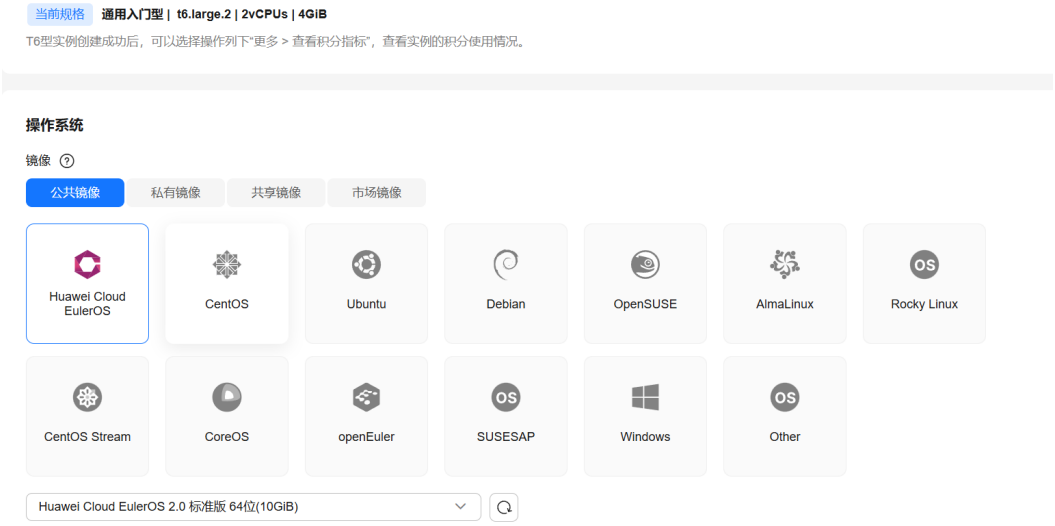
     ii. 区域指ECS的物理数据中心所在的位置，建议您就近选择靠近您业务的区域，可减少网络时延，提高访问速度。本文以选择北京四为例。

iii. 一个区域内有多个可用区，一个可用区发生故障后不会影响同一区域内下的其它可用区。本文以选择随机分配为例。

b. **选择规格&镜像**

i. 实例规格本文选择满足测试需求且价格较为实惠的通用入门型t6，2v4G规格。

ii. 镜像本文选择公共镜像中的Huawei Cloud EulerOS 2.0 标准版 64位(10GiB)。



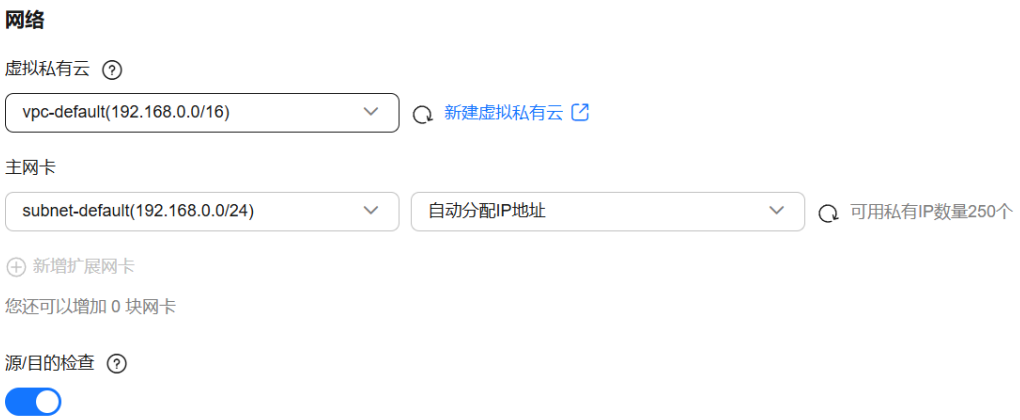
c. **选择存储**

本文实现简单应用服务器搭建，只需要选择系统盘存储操作系统。系统盘本文选择通用型SSD，40GiB大小。

d. **选择网络**

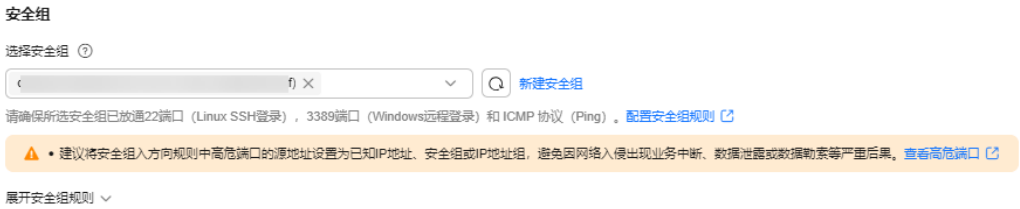
i. 根据业务需求，选择或创建虚拟私有云，本文选择默认的**vpc-default(192.168.0.0/16)**。

ii. 主网卡本文选择default与自动分配IP地址，实际可根据业务需求指定。



e. **创建安全组**

安全组是一种虚拟网络防火墙，能够控制ECS实例的出入流量。创建时，请设置放行SSH（22）、RDP（3389）、HTTP（80）、HTTPS（443）等端口，便于后续访问ECS实例。此处创建的安全组默认设置0.0.0.0/0（表示允许全网段设备访问指定的端口）作为源的规则，后续您可以设置为具体的请求端的IP地址。



f. **绑定公网IP**

本实例需要支持公网访问。本文选择直接购买弹性公网IP。

g. **创建登录凭证**

创建ECS的登录凭证，以供后续连接ECS实例时使用。

h. **创建并查看ECS实例**

确认好配置后，单击右下角立即购买，购买成功后可到弹性云服务器列表查看创建好的ECS。

实施步骤

步骤1 配置应用服务器。

1. 获取SDK开发包。

   请在各语言的**SDK开发指南**中获取。

2. 生成预签名URL的代码。

   预签名URL的计算方法请参考**URL中携带签名**。

   下述示例以在应用服务器中使用Java语言开发进行举例。

说明

应用服务器需要根据APP操作类型，识别公共请求消息头与自定义请求消息头，并将其加入到预签名URL生成签名计算中。

- 公共请求消息头，请参考**构造请求**。
- 自定义请求消息头，请参考对应操作的API文档。例如PUT上传，参考**PUT上传API**。

此处以Java SDK生成预签名URL的代码为示例：

```
// 本次请求的桶的endpoint
String endPoint = "http://your-endpoint";

// 认证用的ak和sk硬编码到代码中或者明文存储都有很大的安全风险，建议在配置文件或者环境变量中密文存放，使用时解密，确保安全；本示例以ak和sk保存在环境变量中为例，运行本示例前请先在本地环境中设置环境变量ACCESS_KEY_ID和SECRET_ACCESS_KEY_ID。
// 您可以登录访问管理控制台获取访问密钥AK/SK，获取方式请参见https://support.huaweicloud.com/usermanual-ca/ca_01_0003.html
String ak = System.getenv("ACCESS_KEY_ID");
String sk = System.getenv("SECRET_ACCESS_KEY_ID");

// 创建ObsClient实例
ObsClient obsClient = new ObsClient(ak, sk, endPoint);
// 替换您的过期时间，单位是秒
long expireSeconds = 3600L;

// 替换成您对应的操作
TemporarySignatureRequest request = new TemporarySignatureRequest(HttpMethodEnum.PUT, expireSeconds);

// 替换为请求本次操作访问的桶名和对象名
request.setBucketName("bucketname");
request.setObjectKey("objectname");

TemporarySignatureResponse response = obsClient.createTemporarySignature(request);

// 成功返回预签名URL，如下打印URL信息
System.out.println(response.getSignedUrl());
```

更多相关介绍和示例代码，请参见**使用URL进行授权访问**。

步骤2 移动应用客户端使用获取到的预签名URL发送OBS请求。

Android应用客户端示例代码：

```
public class Demo extends Activity
{
    private static String bucketName = "my-obs-bucket-demo";
    private static String objectKey = "my-obs-object-key-demo";
    private static OkHttpClient httpClient;
    private static StringBuffer sb;

    @Override
    protected void onCreate(Bundle savedInstanceState)
    {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.activity_main);
        sb = new StringBuffer();
        /*
        * Constructs a client instance with your account for accessing OBS
        */
        httpClient = new OkHttpClient.Builder().followRedirects(false).retryOnConnectionFailure(false)
              .cache(null).build();
        final TextView tv = (TextView)findViewById(R.id.tv);
        tv.setText("Click to start test");
        tv.setOnClickListener(new View.OnClickListener()
        {
            @Override
            public void onClick(View v)
            {
                tv.setClickable(false);
```



```
            AsyncTask<Void, Void, String> task = new DownloadTask();
            task.execute();
        }
    });
}

class DownloadTask extends AsyncTask<Void, Void, String>
{
    @Override
    protected String doInBackground(Void... params)
    {
        try
        {
            /*
             * 这里需要您自己构造上传对象请求到应用服务器来生成到OBS请求的预签名URL
             * 假如响应结果存放在：response，通过方法获取getSignedUrl()
             */
            sb.append("Uploading a new object to OBS from a file\n\n");
            Request.Builder builder = new Request.Builder();
            // 使用PUT请求上传对象
            Request httpRequest =
builder.url(response.getSignedUrl()).put(RequestBody.create(MediaType.parse(contentType), "Hello
OBS".getBytes("UTF-8"))).build();
            Call c = httpClient.newCall(httpRequest);
            Response res = c.execute();
            sb.append("\tStatus:" + res.code());
            if (res.body() != null) {
                sb.append("\tContent:" + res.body().string() + "\n");
            }
            res.close();

            /*
             * 这里需要您自己构造下载对象请求到应用服务器来生成到OBS请求的预签名URL
             * 假如响应结果存放在：response，通过方法获取getSignedUrl()
             */
            sb.append("Downloading an object\n\n");
            Request.Builder builder = new Request.Builder();
            // 使用GET请求下载对象
            Request httpRequest = builder.url(response.getSignedUrl()).get().build();
            OkHttpClient httpClient = new
OkHttpClient.Builder().followRedirects(false).retryOnConnectionFailure(false).cache(null).build();
            Call c = httpClient.newCall(httpRequest);
            Response res = c.execute();
            System.out.println("\tStatus:" + res.code());
            if (res.body() != null) {
                sb.append("\tContent:" + res.body().string() + "\n");
            }
            res.close();

            return sb.toString();
        }
        catch (Exception e)
        {
            sb.append("\n\n");
            sb.append(e.getMessage());
            return sb.toString();
        }
        finally
        {
            if (httpClient != null)
            {
                try
                {
                    /*
                     * Close obs client
                     */
                    httpClient.close();
                }
                catch (IOException e)
```

```
                {
                }
            }
        }
    }

    @Override
    protected void onPostExecute(String result)
    {
        TextView tv = (TextView)findViewById(R.id.tv);
        tv.setText(result);
        tv.setOnClickListener(null);
        tv.setMovementMethod(ScrollingMovementMethod.getInstance());
    }
  }
}
```

Harmony应用客户端示例代码：

```
// 读取文件内容并转为ArrayBuffer格式
const fileInfo = await fs.open(fileUri, fs.OpenMode.READ_ONLY);
const fileStat = await fs.stat(fileInfo.fd);
const data = new ArrayBuffer(fileStat.size);
await fs.read(fileInfo.fd, data);
await fs.close(fileInfo.fd);

try {
  // 这里需要您自己构造上传对象请求到应用服务器来生成到OBS请求的预签名URL
  // 假如响应结果存放在signUrlResult中
  await request(signUrlResult.SignedUrl, {
    method: http.RequestMethod.PUT,
    header: signUrlResult.ActualSignedRequestHeaders,
    extraData: data
  }, 200);
  console.info('putObject success');
} catch (err) {
  console.info('putObject request error: ' + JSON.stringify(err));
  throw err;
}
```

----结束

相关参考

- **Java SDK接口参考文档**
- **Java SDK依赖缺失和依赖冲突的解决方法**
- Harmony项目完整代码可参考：**obs-harmony-demo**

2.5 小程序直传 OBS

背景信息

微信小程序作为当下流行的移动应用，具有广泛的应用场景。如何通过微信小程序上传文件至对象存储服务OBS成为了一个热点问题，本文将通过一个示例程序进行演示。

注意事项

- 客户端计算签名时依赖引用“crypto-js”及“js-base64”两个开源组件，因此需要在微信小程序项目中设置使用NPM模块。
- 在微信小程序中进行编译时，如果在引入“crypto-js”包时出现“Maximum call stack size exceed”报错，请升级微信小程序开发客户端至最新版本。

- 上传过程中返回405时，请检查指定的endpoint是否为对应上传桶的桶域名。

操作步骤

步骤1 设置桶的跨域访问权限。

微信小程序基于BrowserJS进行开发，受同源安全策略的要求，不同域间的网站脚本和内容如需交互，需要配置跨域资源共享（CORS）规范。华为云对象存储服务OBS支持CORS规范，允许跨域访问OBS中的资源，具体配置步骤请参见**配置跨域资源共享**。

CORS规则配置项建议：

表 2-9 CORS 规则

参数	说明	配置建议
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。	全选
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。	*

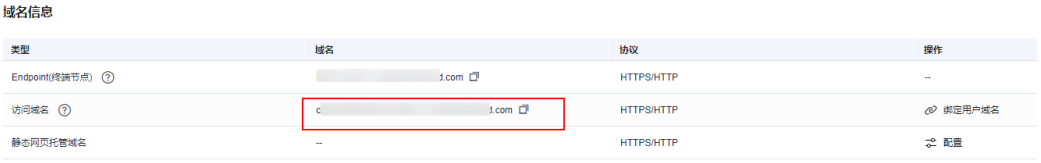
参数	说明	配置建议
补充头域	可选参数，指CORS响应中带的补充头域，给客户端提供额外的信息。 补充头域可设置多个，多个头域之间换行隔开，不支持*、&、:、<、空格以及中文字符。	• ETag • x-obs-request-id • x-obs-api • Content-Type • Content-Length • Cache-Control • Content-Disposition • Content-Encoding • Content-Language • Expires • x-obs-id-2 • x-reserved-indicator • x-obs-version-id • x-obs-copy-source-version-id • x-obs-storage-class • x-obs-delete-marker • x-obs-expiration • x-obs-website-redirect-location • x-obs-restore • x-obs-version • x-obs-object-type • x-obs-next-append-position
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。	根据实际业务设置。

步骤2 配置小程序上传域名白名单。

微信小程序利用白名单机制管理跨域访问，想要实现数据上传，需要在微信小程序平台域名白名单中配置桶的访问域名。

1. 获取桶的访问域名。
   在桶列表单击待操作的桶，进入对象页面后单击“概览”。在“域名信息”下查看桶的访问域名。

图 2-14 桶的访问域名



2. 在微信小程序服务器域名配置中指定桶域名为合法域名。详细配置指导请在**小程序客服**搜索“服务器域名配置”，配置信息如**表2-10**所示。

图 2-15 微信小程序配置服务器信息

表 2-10 微信小程序配置建议

参数	配置建议
request合法域名	桶的访问域名
socket合法域名	根据实际情况填写
uploadFile合法域名	桶的访问域名
downloadFile合法域名	桶的访问域名
udp合法域名	根据实际情况填写
tcp合法域名	根据实际情况填写

步骤3 计算POST上传签名。

POST上传前需要根据上传时自定义使用的policy字段计算相关签名信息，签名计算规则请参见**基于浏览器上传的表单中携带签名**，计算签名相关源代码如下：

对policy进行base64编码（GetPolicy.js）：

```
const Base64 = require('js-base64');

function getPolicyEncode(policy) {
  // 传入表单上传的policy字段，对policy进行Base64编码
  const encodedPolicy = Base64.encode(JSON.stringify(policy));
  return encodedPolicy;
}

module.exports = getPolicyEncode;
```

计算签名的源代码（GetSignature.js）：

```
const Crypto = require('crypto-js');
const Base64 = require('js-base64');

function getSignature(policyEncoded, SecretKey){
  // 利用SK对Base64编码后的policy结果进行HMAC-SHA1签名计算
  const bytes = Crypto.HmacSHA1(policyEncoded, SecretKey);
  // 对计算结果进行Base64编码，得到最终的签名信息
  const signature = Crypto.enc.Base64.stringify(bytes);
  return signature;
}

module.exports = getSignature;
```

步骤4 使用小程序直传数据至对象存储桶中。

基于**步骤3**中得到的编码后的policy字段及signature字段，可以调用小程序中的上传接口，选择本地文件并上传。具体代码示例如下：

配置AK、SK、访问域名等信息的配置文件（Configuration.js）：

- 使用永久访问密钥（AK/SK）

```
// 指定OBS服务相关信息：AK，SK，EndPoint
var Configuration = {
  // 认证用的ak和sk硬编码到代码中或者明文存储都有很大的安全风险，建议在配置文件或者环境变量中密文存放，使用时解密，确保安全；本示例以ak和sk保存在环境变量中为例，运行本示例前请先在本地环境中设置环境变量AccessKeyId和SecretKey。
  // 前端本身没有process对象，可以使用webpack类打包工具定义环境变量，就可以在代码中运行了。
  // 您可以登录访问管理控制台获取访问密钥AK/SK，获取方式请参见https://support.huaweicloud.com/usermanual-ca/ca_01_0003.html
  AccessKeyId: process.env.AccessKeyID,
  SecretKey: process.env.SecretAccessKey,
  EndPoint: 'https://your-test-bucket.obs.myhuaweicloud.com',        //完整的桶访问域名
};


module.exports = Configuration;
```

- 使用临时访问密钥（AK/SK/securitytoken）

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

```
// 指定OBS服务相关信息：AK，SK，SecurityToken，EndPoint
var Configuration = {
  // 认证用的ak和sk硬编码到代码中或者明文存储都有很大的安全风险，建议在配置文件或者环境变量中密文存放，使用时解密，确保安全；本示例以ak和sk保存在环境变量中为例，运行本示例前请先在本地环境中设置环境变量AccessKeyId和SecretKey。
  // 前端本身没有process对象，可以使用webpack类打包工具定义环境变量，就可以在代码中运行了。
  // 您可以登录访问管理控制台获取访问密钥AK/SK，获取方式请参见https://support.huaweicloud.com/usermanual-ca/ca_01_0003.html
  AccessKeyId: process.env.AccessKeyID,
  SecretKey: process.env.SecretAccessKey,
  SecurityToken: process.env.SecurityToken,        //securityToken
  EndPoint: 'https://your-test-bucket.obs.myhuaweicloud.com',        //完整的桶访问域名
};


module.exports = Configuration;
```

说明

配置文件中传入的EndPoint应该为完整的桶访问域名，例如：https://bucketName.obs.myhuaweicloud.com，其中bucketName即小程序上传的目标桶名。

```
// 引入配置文件
const config = require('./Configuration.js');
// 引入policy编码计算方法
const getPolicyEncode = require('./getPolicy.js');
// 引入签名计算方法
const getSignature = require('./GetSignature.js');

const OBSupload = function (filePath){
  if(!filePath){
    wx.showToast({
      title: 'Invalid filePath',
      icon: 'Please re-select path',
    });
  }
  else{
    const fileName = 'testMiniprogram.jpg';  // 指定上传到OBS桶中的对象名

    const OBSPolicy = {                  // 设定policy内容，policy规则定义可参考步骤3中的超链接签名计算规则文档
      "expiration": "2021-12-31T12:00:00.000Z",
      "conditions": [
        { "bucket": "your-test-bucket" },  // 桶名要和配置文件中endpoint中的桶名保持一致
        // { "x-obs-security-token": config.SecurityToken } // 如果是临时访问密钥鉴权，必须设置该值
        { 'key': fileName }
      ]
    }

    const policyEncoded = getPolicyEncode(OBSPolicy);                    // 计算base64编码后的policy
    const signature = getSignature(policyEncoded, config.SecretKey);     // 计算signature

    wx.uploadFile({
      url: config.EndPoint,
      filePath: filePath,
      name: 'file',
      header: {
        'content-type': 'multipart/form-data; boundary=-9431149156168',
      },
      formData: {
        // 从配置文件中获取到的AK信息、计算得到的编码后policy及signature信息
        'AccessKeyID': config.AccessKeyId,
        'policy': policyEncoded,
        'signature': signature,
        'key': fileName,
        // "x-obs-security-token": config.SecurityToken, // 如果是临时访问密钥鉴权，必须设置该值
      },

      success: function(res){
        console.log(res.statusCode);            //打印响应状态码
        if(res.statusCode=='204'){
          console.log('Uploaded successfully', res)
          wx.showToast({
            title: 'Uploaded successfully',
            icon: 'Success'
          });
        }
        else{
          console.log('Uploaded failed', res)
          wx.showToast({
            title: 'Uploaded failed',
            icon: 'Fail'
          });
        }
      },
      fail: function(e){
```

```
      console.log(e);
    }
  })

 }
}

module.exports = OBSupload;
```

----结束

相关操作

上传完成后，要获取对应对象的访问URL，请参见**如何获取对象访问路径**。

3 OBS 数据迁移

3.1 搬迁本地数据至 OBS

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3-1**所示的几种搬迁方案。

表 3-1 搬迁方案

搬迁方式	适用数据量	要求	耗时	费用
OBS工具方式（在线）	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1天左右	数据传输不收取费用，仅OBS收取基本的存储费用
CDM方式（在线）	单次小于8TB的数据量	需要用户单独购买CDM服务	1TB~8TB/天（取决于网络和数据读取源的读写性能）	根据购买CDM实例规格以及使用时长收费，具体参见**CDM价格详情**
DES磁盘方式（离线）	单次小于30TB的数据量	需要用户自己提供磁盘	请参见**从创建DES服务单到数据导入华为云需要多长时间?**	根据磁盘数量以及使用时长收费，具体参见**DES价格详情**
DES Teleport方式（离线）	单次30TB~500TB的数据量	由华为数据中心邮寄Teleport给用户使用	请参见**从创建DES服务单到数据导入华为云需要多长时间?**	根据数据大小以及使用时长收费，具体参见**DES价格详情**
云专线方式（实时）	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**

OBS 工具方式

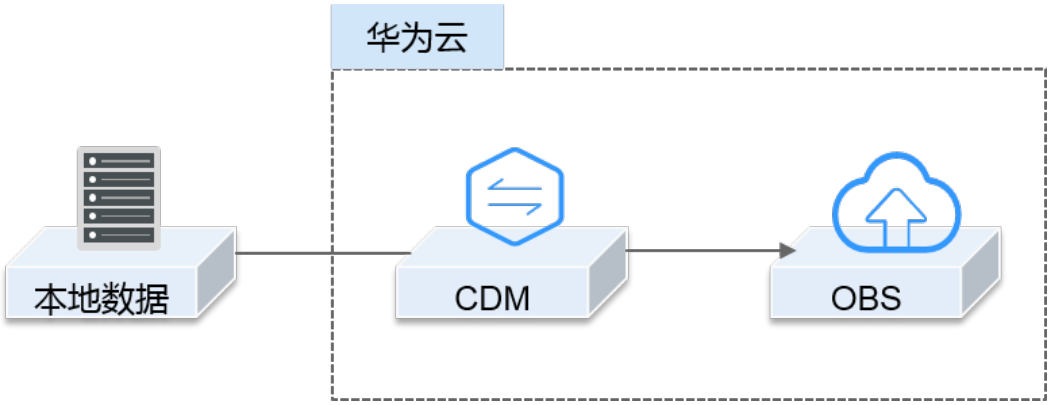
OBS工具方式适用于百GB规模的数据搬迁。OBS提供OBS Browser+、obsutil等多种客户端工具，方便用户在本地直接将数据上传至OBS。由于上传需要占用用户公网带宽，为不影响用户在公网上的主营业务，建议利用公网带宽空闲的时间上传数据。

各工具使用场景及操作指导，请参见**OBS工具指南**。

CDM 方式

云数据迁移（Cloud Data Migration，CDM）提供同构/异构数据源之间批量数据迁移服务。CDM通过创建定时作业，将用户自建存储服务器上的文件系统、数据库、对象存储等数据源与华为云OBS进行连接，从而实现定时、自动地将本地数据搬迁至OBS。

图 3-1 CDM 方式搬迁数据示意图



1. 创建OBS桶

   通过OBS控制台或OBS Browser+创建桶，用于存放原始数据。

2. 购买CDM

   购买CDM服务，即创建CDM集群，用于管理连接与作业。

3. 配置连接与作业

   在创建CDM集群中创建一个源连接和一个目的连接，分别与用户本地数据源和云端OBS连接。然后再创建CDM作业，执行从本地数据搬迁到云端OBS的任务。

4. 启动数据传输

   运行CDM作业，启动数据传输。用户可以通过作业管理界面查看作业进度。

CDM 方式示例：金融大数据咨询业务数据迁移

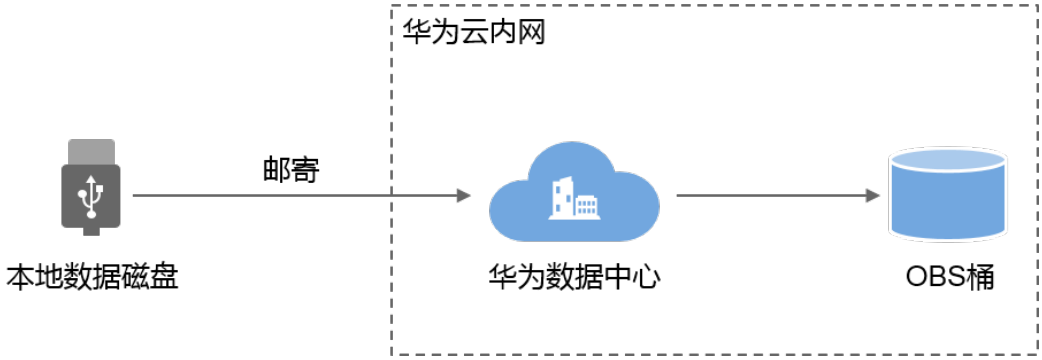
使用CDM将本地贸易统计数据导入到OBS，再使用数据湖探索（Data Lake Insight，DLI）进行贸易统计分析，帮助H咨询公司以极简、极低成本构建其大数据分析平台，使得该公司更好地聚焦业务，持续创新。

详细操作请参见**金融大数据咨询业务数据迁移**。

DES 磁盘方式

DES磁盘方式同样采用离线的方式将用户数据磁盘（USB、eSATA接口的磁盘等）快递至华为云，实现数据高效传输。磁盘方式适用于30TB以下的数据量搬迁。

图 3-2 DES 磁盘方式搬迁数据示意图



1. 创建OBS桶

   通过OBS控制台或OBS Browser+创建桶，用于存放原始数据。

2. 创建DES磁盘方式服务单

   登录DES控制台，创建一个磁盘方式的服务单。然后将DES提供的签名文件导入本地数据磁盘并邮寄给华为云数据中心。

3. 启动数据传输

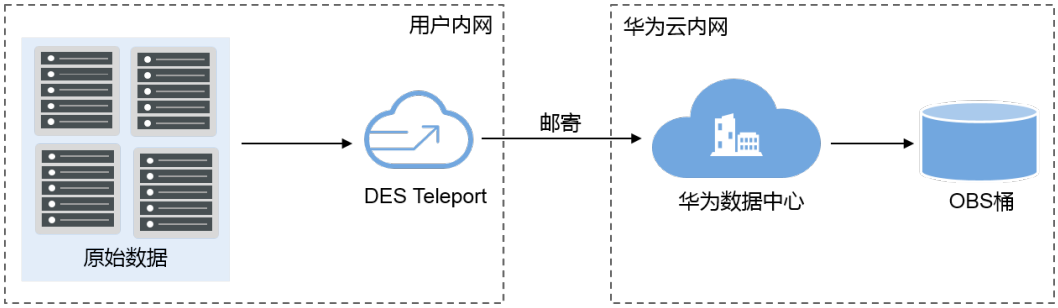
   华为云数据中心收到用户的磁盘并将磁盘挂载到物理服务器后，会短信通知用户填写访问密钥（AK和SK）来启动数据上传。数据传输完成后，用户可以通过DES控制台和OBS控制台两种途径查看传输结果。同时华为云数据中心也会将用户磁盘回寄给用户。

具体操作步骤请参见**磁盘方式详细指导**。

DES Teleport 方式

Teleport是数据快递服务（Data Express Service，DES）专为30TB~500TB范围内数据搬迁至OBS而定制的存储设备，具有防尘防水、抗震抗压以及GPS锁定、传输加密等多重安全防护机制，配合离线传输的方式，能安全、高效的完成大规模数据搬迁。

图 3-3 DES Teleport 方式搬迁数据示意图



1. 创建OBS桶

   通过OBS控制台或OBS Browser+创建桶，用于存放原始数据。

2. 创建DES Teleport服务单

   DES提供Teleport和磁盘两种数据快递方式，在当前场景下选择Teleport方式。

3. 接收并导入数据至Teleport

   成功创建DES服务单后，用户将接收到由华为数据中心邮寄的Teleport设备。接着进行简单配置操作使Teleport与用户客户端连接起来，然后执行数据拷贝并将设备回寄给华为云数据中心。

4. 启动数据传输

   在华为云数据中心收到回寄的Teleport后，用户可以在DES控制台上输入访问密钥启动数据从Teleport到OBS指定桶的传输。数据传输完成后，用户可以通过DES控制台和OBS控制台两种途径查看传输结果。

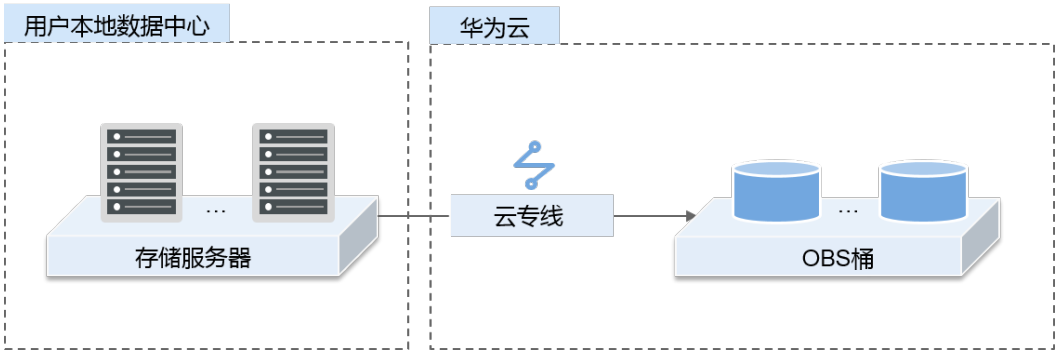
具体操作步骤请参见**Teleport方式详细指导**。

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，更多云专线访问OBS的相关内容请参考**使用云专线访问OBS**。

图 3-4 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. 配置VPC终端节点

   在VPC终端节点中创建DNS终端节点和OBS终端节点，在本地数据中心配置DNS转发规则、DNS路由以及OBS路由。具体操作参见**配置通过内网访问OBS服务的终端节点**。

   说明

   - “拉美-墨西哥城一”、“拉美-圣保罗一”和“拉美-圣地亚哥”区域支持服务类别选择“云服务”购买连接OBS的终端节点，详情参见**购买连接OBS的终端节点**。拉美-墨西哥城一选择com.myhuaweicloud.na-mexico-1.obs；拉美-圣保罗一选择com.myhuaweicloud.sa-brazil-1.obs，“拉美-圣地亚哥”选择com.myhuaweicloud.la-south-2.obs。
   - 其他区域支持服务类别选择“按名称查找服务”购买连接OBS的终端节点，请**提交工单**寻求技术支持获取终端节点服务名称。

4. 启动数据传输

   专线搭建成功并完成VPC终端节点配置后，用户便可以通过控制台、工具、API、SDK等多种方式将本地数据上传至OBS。

迁移专业服务

华为云专业迁移团队提供对象存储数据上云规划设计、上云实施、云上优化全方位服务，帮助您安全、可靠、高效上云。

详情请参见**数据上云设计与实施服务**。

3.2 使用备份软件实现本地数据备份至 OBS

使用场景

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。

Commvault、爱数云备份服务（AnyBackup Cloud）等第三方备份软件，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。

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。

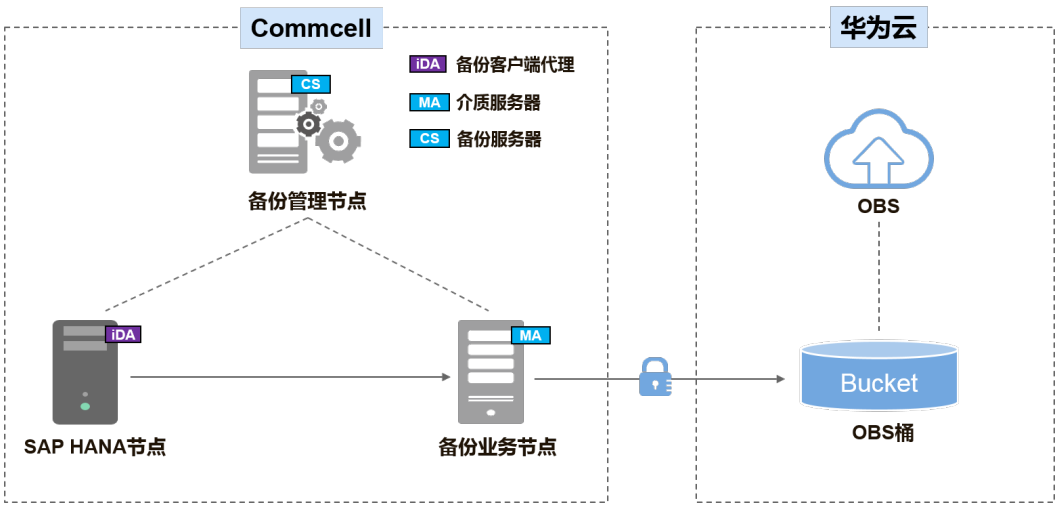
说明

在本场景下推荐使用Commvault V11版本。

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3-5所示。

图 3-5 逻辑架构



逻辑架构中各组件说明如表3-2所示：

表 3-2 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管理控制台，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。

使用 AnyBackup Cloud 备份方案

爱数AnyBackup Cloud结合华为云基础服务，将本地数据备份或迁移到云，提供安全、经济、易管理的数据保护解决方案。

购买方式：

进入**华为云商店**，搜索AnyBackup Cloud，根据场景选择适合自己业务的备份方案。

3.3 迁移第三方云厂商数据至 OBS

有大量数据在第三方云厂商对象存储上的用户，需要先将第三方云厂商上的对象数据下载到本地，再通过OBS控制台、客户端等工具上传到OBS，整个过程耗时又耗力，容易存在漏传、误传等问题。

针对迁移第三方云厂商的对象数据至OBS的场景，华为云提供OMS服务。通过迁移服务，用户只需在控制台配置简单的连接参数以及迁移任务，即可把数据从第三方云厂商轻松、平滑地迁移至OBS。如**表3-3**所示，用户可根据适用场景、迁移速率和费用选择适合的迁移方式。

表 3-3 迁移方案

迁移方式	适用场景	支持的迁移源端	迁移速率	费用
OMS方式	适用于大规模对象数据（500TB以下）全量或增量迁移场景。	请参见**OMS支持迁移的第三方云厂商**	10~20TB/天	收费方法请参见**OMS计费说明**。
MGC方式	适用于大规模对象数据（500TB以上）全量或增量迁移场景。	请参见**迁移其他云平台存储数据至华为云**	大于100TB/天（具体迁移速率与集群/待迁移文件大小有关）	收费方法请参见**迁移中心MGC计费说明**
OBS镜像回源方式（公测中）	适用于无缝迁移数据到OBS场景，即业务数据存储用户自己建立的源站，需要在不中断业务的情况下迁移到OBS上。	用户自己建立的数据源站	不涉及	由第三方云厂商收取数据读取费用，具体以第三方云厂商提供的价格为准。

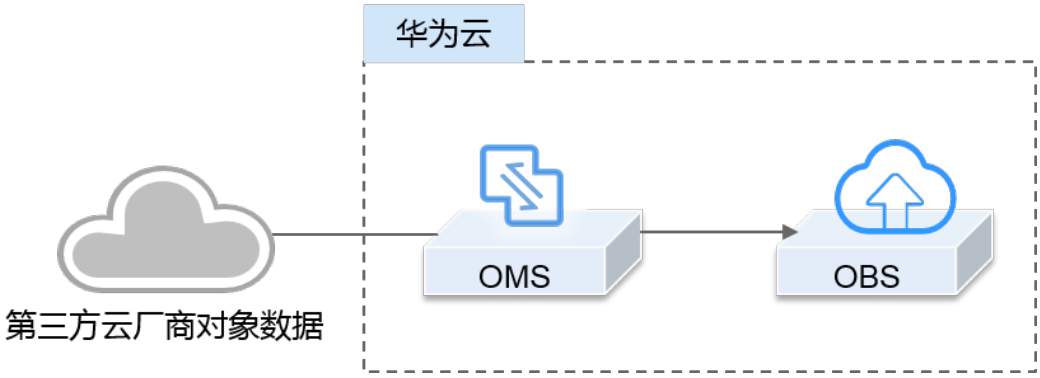
说明

低成本、500TB以上的数据迁移请在华为云上**提交工单**或联系人工客服，根据您的业务模型，为您定制适合超大规模数据迁移的方案。

OMS 方式

OMS是一种云上的对象数据迁移服务，具有安全、高效等优势。数据迁移时，采用HTTPS数据加密通道，确保数据的传输安全。在重复迁移过程中，只迁移有变动或新增的对象，降低成本。

图 3-6 OMS 方式迁移数据示意图



1. 创建OBS桶

   登录OBS**管理控制台**，创建桶用于存放迁移数据。

2. 创建OMS迁移任务

   在OMS控制台创建迁移任务，通过配置访问密钥、桶名等参数将第三方云厂商（源端）与OBS（目的端）关联。

   具体操作步骤请参见**创建对象存储迁移任务**。

3. 开始数据迁移

   执行OMS迁移任务，开始数据迁移。数据迁移过程中，可以在OMS查看任务执行状态以及查看到最终结果。

迁移示例

1. **阿里云OSS迁移至华为云OBS**

   本方案介绍了如何将阿里云对象存储（Object Storage Service，简称OSS）上的数据迁移到华为云对象存储OBS。

   具体方案请参见**操作教程**。

2. **腾讯云COS迁移至华为云OBS**

   本方案介绍了如何将腾讯云对象存储（Cloud Object Storage，简称COS）上的数据迁移到华为云对象存储OBS。

   具体方案请参见**操作教程**。

3. **七牛云迁移至华为云OBS**

   本方案介绍了如何将七牛云对象存储（Kodo）上的数据迁移到华为云对象存储OBS。

   具体方案请参见**操作教程**。

4. **百度云BOS迁移至华为云OBS**

   本方案介绍了如何将百度云对象存储BOS(Baidu Object Storage，简称BOS）上的数据迁移到华为云对象存储OBS。

   具体方案请参见**操作教程**。

5. **优刻得US3迁移至华为云OBS**

   本方案介绍了如何将优刻得对象存储（US3）上的数据迁移到华为云对象存储OBS。

   具体方案请参见**操作教程**。

6. **金山云KS3迁移至华为云OBS**

   本方案介绍了金山云对象存储（Kingsoft Standard Storage Service，简称KS3）上的数据迁移到华为云对象存储OBS。

   具体方案请参见**操作教程**。

7. **HTTP/HTTPS数据源迁移至华为云OBS**

   本方案介绍了如何将网络资源迁移至华为云对象存储OBS。

   具体方案请参见**操作教程**。

业务割接方案

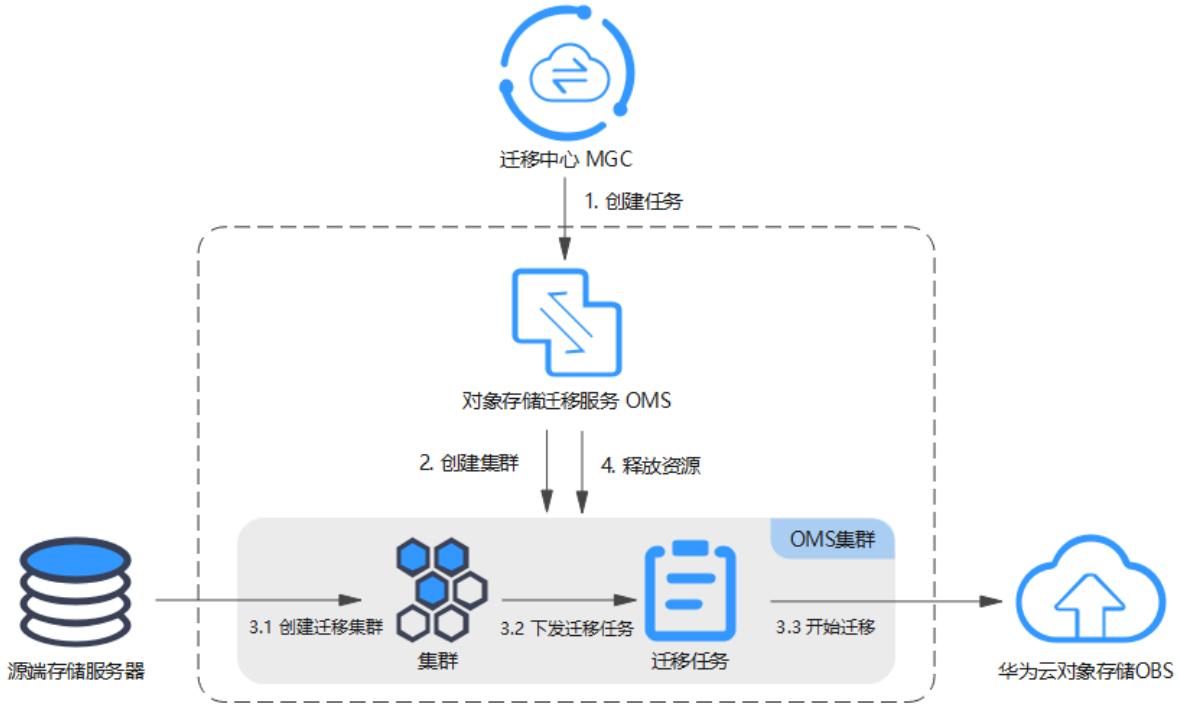
如涉及业务割接，请参考以下方案。

1. **使用“回源配置方案”迁移增量对象数据**
2. **使用“源端/目的端双写方案”方案迁移增量对象数据**
3. **使用"多次同步方案"迁移增量对象数据**

MGC 方式

通过独立专享迁移集群以及配置迁移专线，简单、快捷实现对象存储一站式上云，提升上云效率。

图 3-7 MGC 方式迁移数据示意图



1. 创建目的端。

   在华为云提前创建目的端对象桶。详细操作步骤参见**创建目标端**。

2. 创建集群。

   迁移集群是专为存储工作流提供协作中的核心组件，通过集群可以创建和管理迁移节点、列举节点，部署和升级迁移插件，确保存储工作流顺利运行。详细说明和创建步骤请参见**创建集群**。

3. 创建存储迁移工作流。

   创建迁移工作流，开始进行迁移任务。详细说明和创建步骤请参见**创建存储迁移工作流**。

OBS 镜像回源方式

一般情况下，当客户端访问OBS时，如果OBS中没有被访问的数据，将会返回404错误。OBS提供镜像回源功能，可以在被请求的数据不存在时，通过回源规则从源站获取对应数据。

用户为桶定义镜像回源规则后，如果客户端访问OBS桶中不存在的资源，且该资源符合镜像回源规则，OBS将以镜像回源的方式去数据源站获取资源，将该资源上传到OBS中并返回给客户端。整个过程不中断业务，适用于客户源站无缝迁移数据到OBS，用户可以在无感知的情况下，低成本地迁移业务到OBS上来。镜像回源流程如**图3-8**所示。

图 3-8 镜像回源流程

配置方法请参见**创建镜像回源规则**。

3.4 OBS 之间数据迁移

本教程介绍如何通过对象存储迁移服务OMS实现对象存储服务OBS之间跨账号、跨区域、以及同区域内的数据迁移。

- 跨账号迁移：不同的华为云账号之间桶数据迁移。
- 跨区域迁移：不同区域之间的桶数据迁移。
- 同区域迁移：同区域内的桶数据迁移。

什么是对象存储迁移服务

对象存储迁移服务（Object Storage Migration Service，OMS）是一种线上数据迁移服务，可以帮助您将其他云服务商对象存储服务中的数据在线迁移至华为云的对象存储服务（Object Storage Service，OBS）中，也可以在对象存储服务OBS之间进行灵活的数据迁移。

使用对象存储迁移服务，您只需在控制台填写源端OBS数据信息和目的端OBS数据信息，并创建迁移任务或创建迁移任务组即可，迁移任务与迁移任务组的区别请参见**迁移任务与迁移任务组的适用场景**。

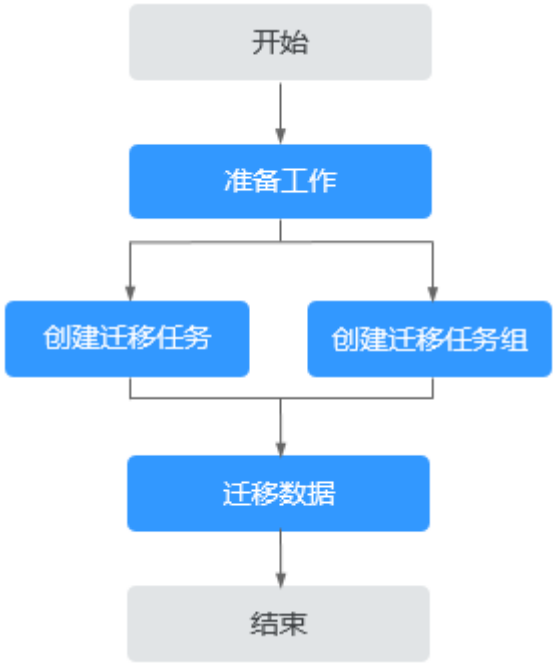
⚠ 注意

- 对象存储迁移服务（OMS）处于免费期，免费期结束后服务将根据您累计使用的迁移流量进行收费，计费方式简单灵活、易于预测。具体费用详情，请参见**产品价格详情**。迁移过程中会调用源端和目的端的对象存储服务的API进行数据的上传、下载，所以会产生一定的API请求及下载流量费用，具体费用说明请参见**计费说明**。
- 跨账号迁移过程除了会产生对象存储迁移服务费用（当前免费）外，还会产生请求费用和流量费用。
  - 请求费用：该项费用在调用OBS API时产生，按请求次数计费，包括PUT/POST/COPY/LIST/GET/HEAD等。
  - 流量费用：源端下载数据时，会产生流量费用，流量由数据的实际大小决定，费用由源端数据所在云服务商收取；数据上传至华为云OBS不收取流量费用。
- 对象存储迁移服务暂不支持迁移多版本的对象存储数据。
- OMS同样适用于OBS桶和并行文件系统桶之间的数据迁移。

迁移流程

迁移流程如**图3-9**所示，具体操作请参见**华为云OBS之间迁移操作指导**。

图 3-9 OBS 之间数据迁移流程



4 OBS 数据访问

4.1 在 ECS 上通过内网访问 OBS

4.1.1 在 ECS 上通过内网访问 OBS 方案概述

应用场景

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。

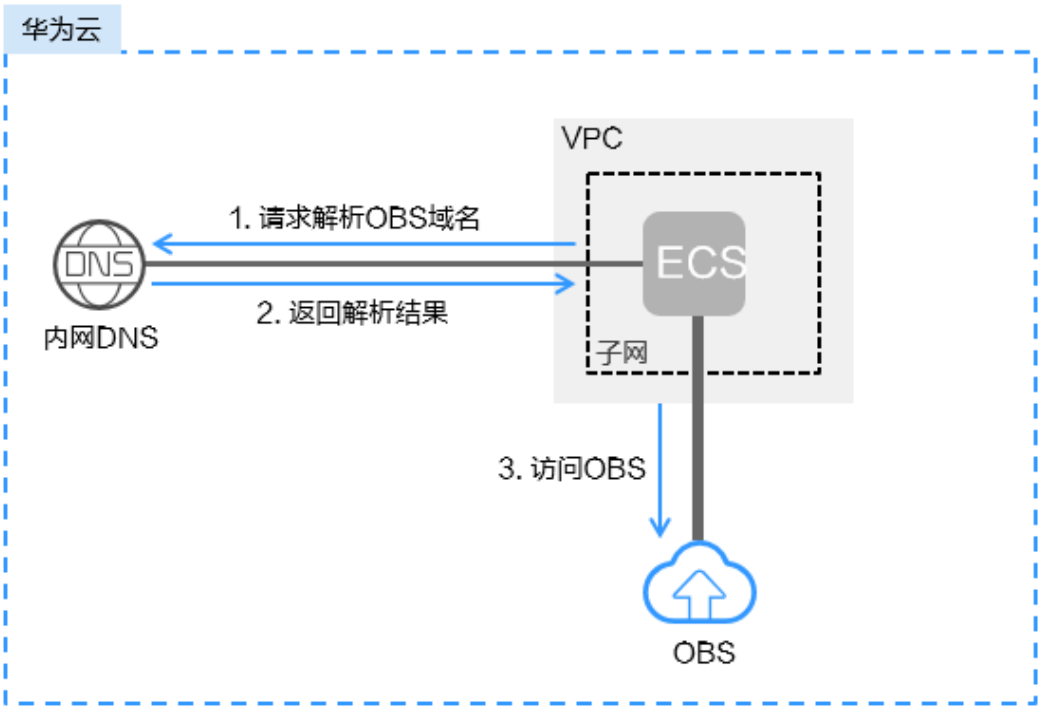
说明

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，例如都在华北-北京四。如果不属于同一个区域，将采用公网访问。

方案架构

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 内网访问 OBS 示意图



- 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。

资源成本及规划

最佳实践中涉及的资源如下：

表 4-1 资源说明

资源	资源说明
弹性云服务器（ECS）	• Windows系统：需安装OBS Browser+ • Linux系统：需安装obsutil
对象存储服务（OBS）	OBS作为数据存储资源池，以减轻服务器负担。 **须知** 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。

资源	资源说明
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。

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

OBS Browser+是一款用于访问和管理对象存储服务的图形化工具，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，下面将介绍具体操作流程和操作步骤。

⚠ 注意

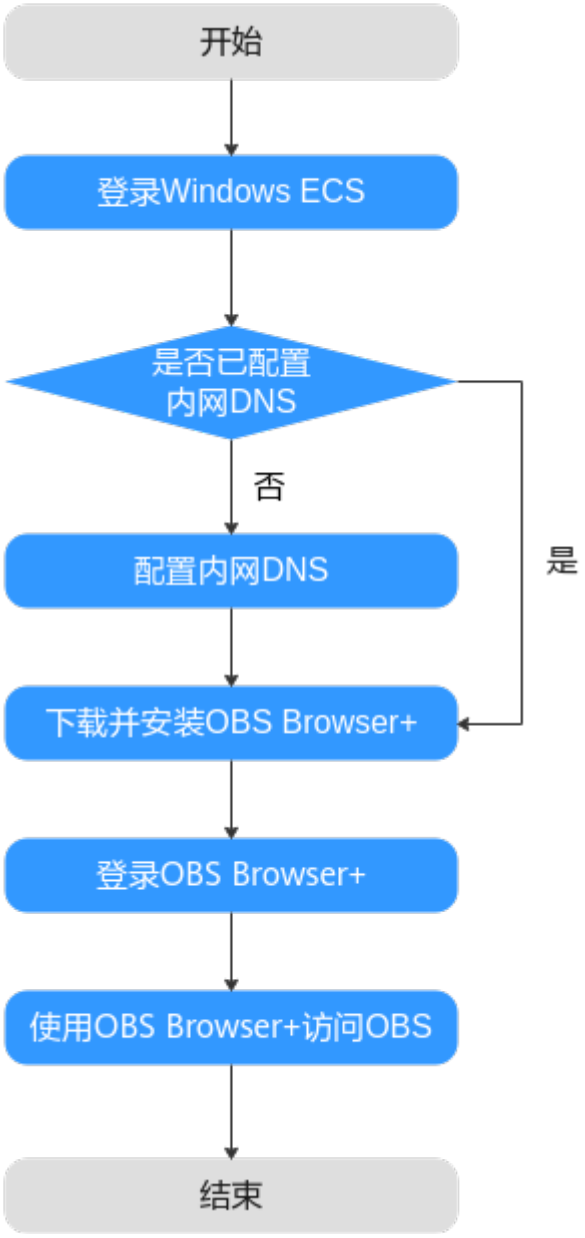
OBS Browser+需通过公网下载，或者从其他可以访问公网的云服务器下载后传到当前云服务器安装。

前提条件

在登录ECS云服务器之前，请确保您已**购买云服务器**。

操作流程

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“控制台”页面。
2. 在服务列表中，选择“计算 > 弹性云服务器 ECS”。
3. 选择待登录的云服务器，登录弹性云服务器。
   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5**。

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**。

- **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，配置备选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。

步骤4 确认已经是内网访问OBS

具体方法请参见**如何判断是否内网访问OBS?**

步骤5 下载并安装OBS Browser+

OBS Browser+下载地址及具体操作请参见**下载OBS Browser+**。

步骤6 登录OBS Browser+

由于OBS Browser+默认使用公网访问OBS，因此在登录OBS Browser+时，“服务提供商”和“服务器地址”需要按照以下要求填写：

- 服务提供商：选择“其他对象存储服务”。
- 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）。

  示例：obs.cn-south-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7 使用OBS Browser+访问OBS

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。

详细使用指南请参见**对象存储服务工具指南（OBS Browser+）**。

----结束

4.1.3 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。

注意

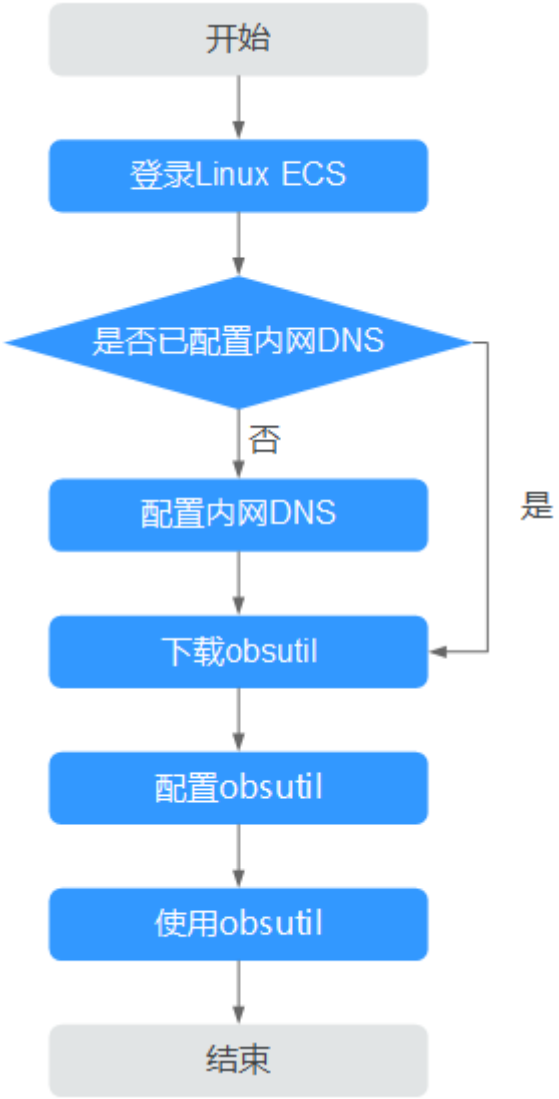
obsutil需通过公网下载，或者从其他可以访问公网的云服务器下载后传到当前云服务器安装。

前提条件

在登录ECS云服务器之前，请确保您已**购买云服务器**。

操作流程

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“控制台”页面。
2. 在服务列表，选择“计算 > 弹性云服务器 ECS”。
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“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5**。

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**。

- **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 确认已经是内网访问OBS

具体方法请参见**如何判断是否内网访问OBS?**

步骤5 下载匹配云服务器架构的obsutil

1. 单击管理控制台左上角的 ，选择区域。
2. 单击“ ”，选择“计算 > 弹性云服务器 ECS”。

系统进入弹性云服务器列表页，您可以在本页面查看您已购买的弹性云服务器，以及弹性云服务器的规格，如果规格有前缀“k”则为ARM架构，此时您应该下载Linux ARM 64位的obsutil安装包，如果没有前缀“k”则为x86架构，此时您应该下载Linux AMD 64位（Linux x86 64位）的obsutil安装包。更多关于云服务器的规格信息请参见**实例类型**。

3. 下载对应版本的obsutil。

   obsutil最新版本和下载链接请参见**下载obsutil**。

步骤6 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7 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

4.2 通过 Nginx 反向代理访问 OBS

应用场景

一般情况下，用户会通过OBS提供的桶访问域名（例如https://*bucketname*.obs.cn-north-4.myhuaweicloud.com）或者绑定的自定义域名来访问OBS。

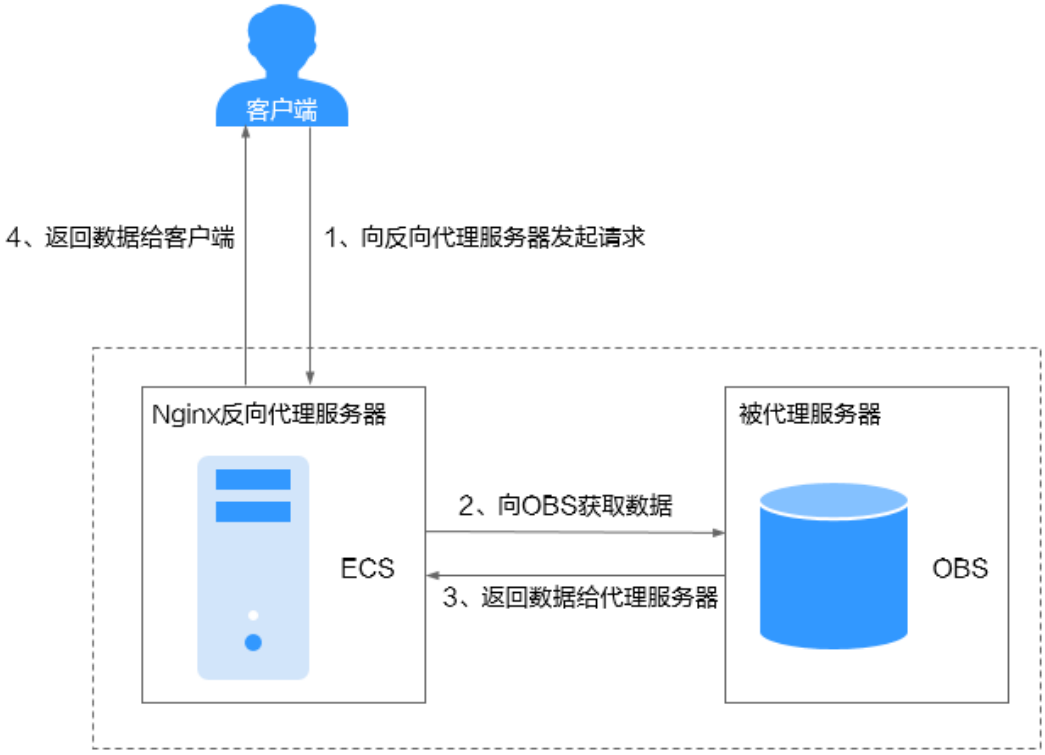
但在某些场景下，用户需要通过固定的IP地址访问OBS，例如：某些企业出于安全考虑，对于可访问的外部地址需要设置黑白名单，而这个时候对于OBS的访问则需要一个固定的IP地址。同样出于安全考虑，华为云OBS桶访问域名通过DNS解析的IP地址是会发生变化的，所以用户无法获取某个桶长期有效的固定IP地址。

此时，可以通过在ECS上搭建Nginx反向代理服务器，来实现通过固定IP地址访问OBS。

方案架构

本实践将Nginx部署在ECS上，搭建Nginx反向代理服务器。用户对代理无感知，只需要将请求发送到反向代理服务器，然后由反向代理服务器向OBS获取数据，再返回给用户。反向代理服务器和OBS对外看做一个整体，仅暴露代理服务器的IP地址，隐藏了OBS真实的域名或IP地址。

图 4-4 通过 Nginx 反向代理访问 OBS 原理



约束与限制

- 已明确OBS桶所在区域和桶的访问域名，如华北-北京四区域的桶：nginx-obs.obs.cn-north-4.myhuaweicloud.com。**查看方法**
- 已在同区域购买Linux操作系统的ECS，本文以CentOS系统为例。**购买ECS方法**
- ECS已绑定EIP，EIP用于从公网下载必要的Nginx安装包。

实施步骤

步骤1 在ECS上安装Nginx

此处以CentOS 7.6版本的操作系统为例。

1. 登录用于搭建Nginx反向代理服务器的ECS。
2. 使用wget命令，下载对应当前操作系统版本的Nginx安装包。
   ```
   wget http://nginx.org/packages/centos/7/noarch/RPMS/nginx-release-centos-7-0.el7.ngx.noarch.rpm
   ```
3. 执行以下命令，建立Nginx的yum仓库。

```
rpm -ivh nginx-release-centos-7-0.el7.ngx.noarch.rpm
```

4. 执行以下命令，安装Nginx。
```
yum -y install nginx
```
5. 执行以下命令，启动Nginx并设置开机启动。
```
systemctl start nginx
systemctl enable nginx
```
6. 在任意终端使用浏览器访问“http://*ECS弹性公网IP地址*”，显示如下图所示，说明Nginx安装成功。

图 4-5 Nginx 安装成功

步骤2 修改Nginx配置文件，反向代理OBS桶

1. 执行以下命令，打开“default.conf”配置文件。
```
vim /etc/nginx/conf.d/default.conf
```
2. 按“i”键进入编辑模式，修改“default.conf”配置文件。
```
server {
    listen       80;
    server_name  **.**.**.**;  #此处填写ECS弹性公网IP地址
    proxy_buffering off;  #关闭代理缓冲区（内存）
    location / {
        proxy_pass  https://nginx-obs.obs.cn-north-4.myhuaweicloud.com;  #此处填写OBS桶访问域名，以http://或https://开头
        index  index.html index.htm；#指定网站初始页。如果包括多个文件，Nginx会根据文件的枚举顺序来检查。
        proxy_set_header Host $proxy_host;
        #当您使用ELB七层监听器时，建议设置X-Forwarded-For参数为空
        #proxy_set_header X-Forwarded-For "";
     }
}
```

表 4-2 配置文件参数说明

参数	说明
server_name	提供反向代理服务的IP地址，即需要暴露给终端用户访问的固定IP地址。 此处填写搭建Nginx反向代理服务的ECS弹性公网IP地址，即当前登录的ECS弹性公网IP地址。

参数	说明
proxy_pass	被代理服务器的地址。 此处填写**前提条件**获取的OBS桶的访问域名，注意需要以http://或https://开头，例如： https://nginx-obs.obs.cn-north-4.myhuaweicloud.com 注意： 当使用API、SDK、obsutil调用时，此处填写区域域名，例如： obs.cn-north-4.myhuaweicloud.com
proxy_buffering	设置是否开启代理缓冲区，取值为on（开启）或者off（关闭）。 如果取值为on，Nginx会把后端返回的内容先放到缓冲区，然后再返回给客户端。 如果取值为off，Nginx会立即把从后端收到的响应内容传送给客户端。 默认值：on 示例：proxy_buffering off

3. 按“Esc”，输入“:wq”保存并退出。
4. 执行以下命令，测试Nginx配置文件状态。
```
nginx -t
```
5. 执行以下命令，重启Nginx服务使配置生效。
```
systemctl stop nginx
systemctl start nginx
```

步骤3 (可选)配置OBS桶策略，允许Nginx代理服务器的IP地址访问OBS

如果您的OBS桶为公共读，或者访问私有桶内对象时在**URL中携带签名**，则可跳过此步骤。

如果您的OBS桶为私有桶，且不希望使用携带签名的URL访问桶内资源，则建议配置以下桶策略：仅允许Nginx代理服务器的IP地址访问OBS桶。

1. 在OBS管理控制台左侧导航栏选择“对象存储”。
2. 在桶列表单击待操作的桶，进入对象页面。
3. 在左侧导航栏，单击“权限控制 > 桶策略”。
4. 单击“创建”。
5. 根据使用习惯，策略配置方式以可视化视图为例。单击“可视化视图”。
6. 配置如下参数。

表 4-3 桶策略参数配置

参数	说明
策略名称	输入自定义的桶策略名称。
效力	选择“允许”。
被授权用户	选择“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：*
授权操作	– 选择“自定义配置” – 选择动作：Get*和List*
授权条件（可选）	– 键：SourceIp – 条件运算符：IpAddress – 值： ■ 如果ECS使用公网DNS，取值为：***ECS的弹性公网IP地址*** ■ 如果ECS使用华为云内网DNS，取值为：**100.64.0.0/10,214.0.0.0/7,*ECS的私有IP地址*** **说明** 取值需要同时配置三个IP地址（IP地址段），请单击“增加”按钮。 其中，100网段和214网段为ECS内网访问OBS的网段。

7. 单击右下角的“创建”，完成桶策略创建。
8. 权限配置信息可以在桶策略列表查看。

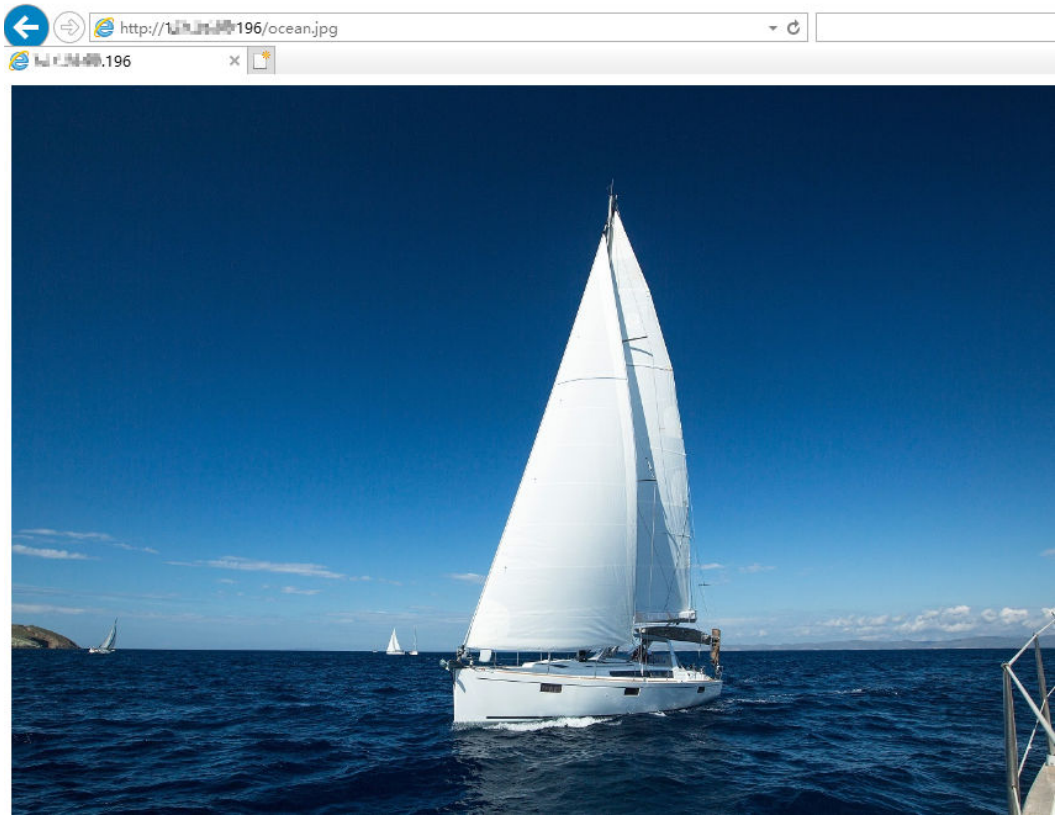
图 4-6 查看桶策略列表权限配置信息

步骤4 验证反向代理配置

在任意终端使用ECS弹性公网IP地址+对象名访问OBS资源，如果能正常访问，则说明配置成功。

例如访问http://*ECS弹性公网IP地址*/ocean.jpg

图 4-7 使用固定 IP 地址访问 OBS 资源



----结束

4.3 通过云连接 CC 实现内网跨区域访问 OBS

应用场景

为了降低访问延迟、满足当地的数据合规性等需求，您的业务数据可能存储在各区域的OBS桶中，与此同时，您可能需要集中访问、处理和分析各区域OBS桶中的数据。例如，您的ECS云服务器部署在华东-上海一，存储数据的OBS桶可能部署在华北-北京四等其他区域，此时ECS云服务器需要跨区域访问OBS桶。在使用**云连接**（Cloud Connect，以下简称CC）前，跨区域访问需要通过**公网**，公网网络延迟高、带宽不稳定，并且会产生较高的公网流量费用。使用云连接CC后，可以打通**跨区域的内网通道，实现内网跨区域访问OBS桶**。基于云连接CC的内网跨区域访问方案具有以下优势：

- **高速传输**：通过华为云优质的内网骨干网，数据传输速度优于公网，延迟更低，稳定性更高。
- **成本优化**：通过内网跨区域访问OBS，不收取流量费用，为您节省成本。
- **数据安全**：数据全程在华为云内网中传输，安全性更高。

本文为您详细介绍通过云连接CC跨区域访问OBS的方案，方案中配套使用了桶的专线域名和专线IP，使用时您只需直接访问OBS桶的专线域名，CC就会自动将访问请求路由到对应区域的OBS桶。

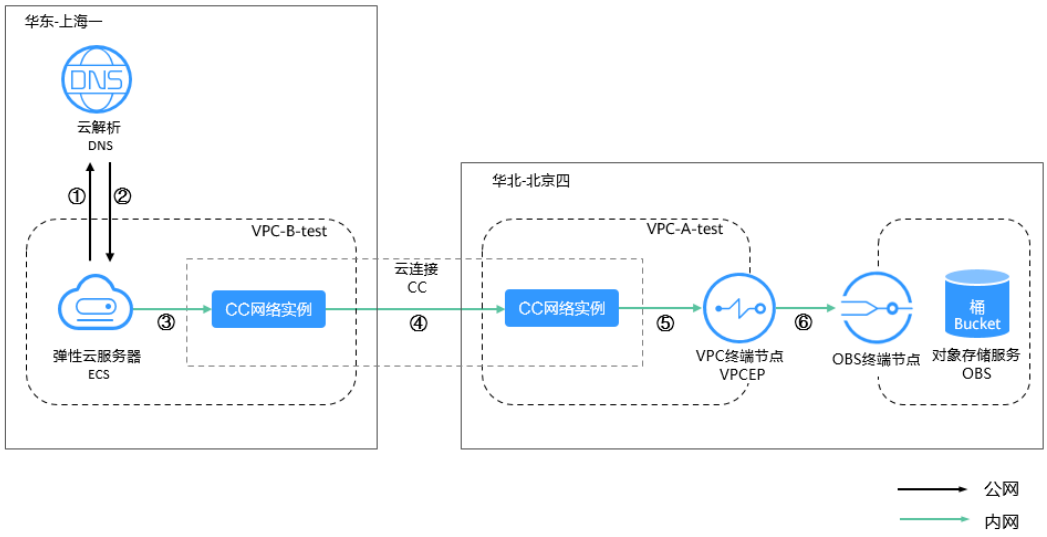
背景介绍

了解使用云连接跨区域访问OBS前，您可能需要了解以下背景知识：

- **云连接：**云连接能够帮助您构建跨区域VPC之间高速、优质、稳定的网络访问，更多关于云连接的内容，请参见**云连接**。
- **OBS桶域名：**桶创建成功后，OBS会根据桶名和桶的区域信息生成一个桶的默认域名“*BucketName*.obs.*RegionID*.myhuaweicloud.com”。例如：华北-北京四名为test-zcy-abc的桶，它的桶域名为test-zcy-abc.obs.cn-north-4.myhuaweicloud.com。
- **OBS桶的内网IP：**OBS桶在华为云内网的访问地址。桶域名通过内网DNS解析得到的就是桶的内网IP，通过公网DNS解析得到的就是桶的公网IP。
- **专线域名**：多云互联场景下，为了解决IDC专线接入OBS时发生的IP冲突问题，OBS为云专线场景提供了专线域名“*BucketName*.obs-private.*RegionID*.myhuaweicloud.com”。例如：华北-北京四名为test-zcy-abc的桶，它的专线域名为test-zcy-abc.obs-private.cn-north-4.myhuaweicloud.com。
- **专线IP：**专线域名通过公网DNS解析后即可得到对应的专线IP。依据IETF和IANA标准，OBS为内网访问保留了100.125.0.0/16网段，此网段多用于IDC数据中心和云厂商内部服务互联。但是对于IDC多云互联场景，由于各云厂商均使用了该网段，导致IDC在配置各云厂商路由时出现IP冲突。为了解决该冲突，OBS为每个华为云Region预留一段专线IP，该专线IP可以通过公网DNS解析专线域名得到，但只能用于内网访问OBS。

方案架构

图 4-8 跨 Region 访问 OBS 方案架构图



通过CC跨Region访问OBS桶的流程如下：

1. 使用ECS访问桶（test-zcy-abc）的专线域名（test-zcy-abc.obs-private.cn-north-4.myhuaweicloud.com）。
2. DNS将专线域名解析的专线IP返回给ECS。华为云内部已完成专线域名到专线IP的映射，因此本实践中您无需配置DNS域名解析。

3. ECS访问专线IP，经过同区域的CC网络实例。
4. 云连接实例将对专线IP的访问路由到桶所在区域的CC网络实例。
5. CC网络实例将访问路由到同VPC的VPC终端节点（OBS网关型终端节点），通过OBS网关型终端节点可以实现大带宽低时延访问OBS桶。
6. 访问经由VPCEP后到达OBS，完成跨区域对OBS桶的访问。

方案优势

- **架构精简：**您无需为了解析OBS域名而购买并配置DNS，OBS预留的专线域名通过公网DNS解析即可得到专线IP，直接访问专线IP即可访问OBS。
- **传输高效：**专用网络进行数据传输，网络性能高，延迟低；使用OBS网关型终端节点可以实现大带宽低时延访问OBS桶。
- **安全可靠：**云连接使用专属私密通道接入华为云VPC，网络隔离，安全性极高。

约束与限制

专线域名当前支持华东-上海一和华北-北京四，其他区域可**提交工单**联系技术支持申请使用。

资源和成本规划

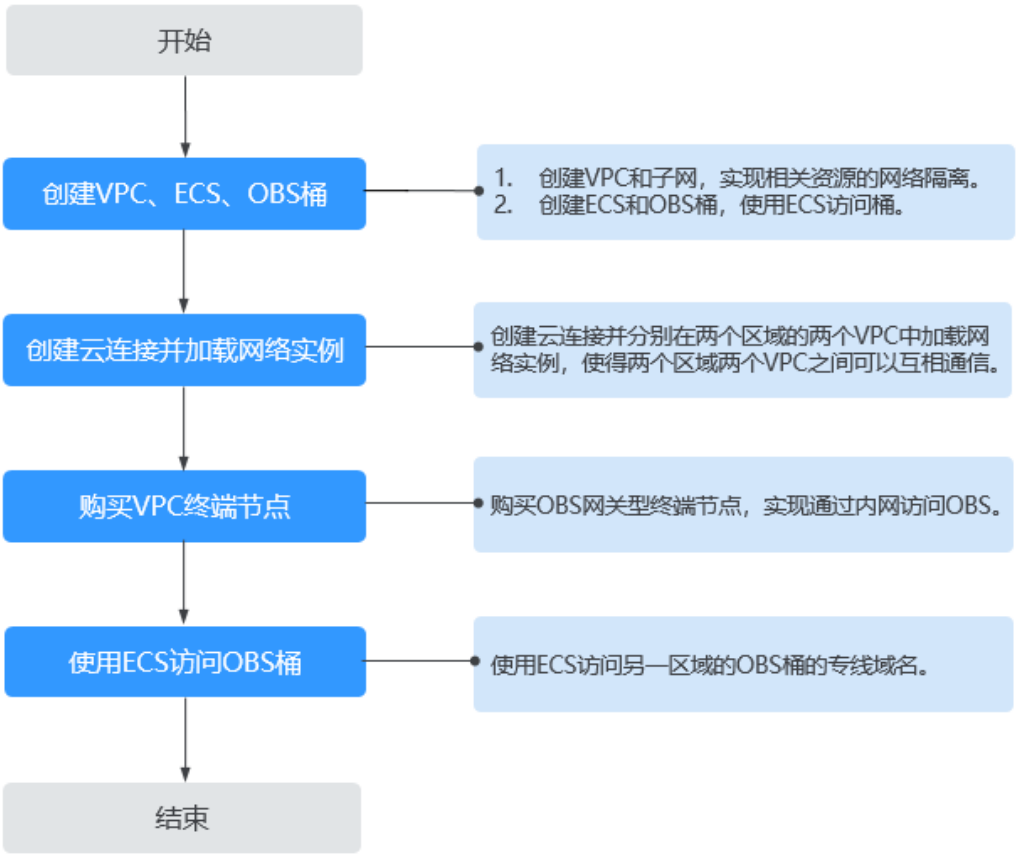
表 4-4 资源规划

区域	资源	资源名称	资源说明	数量	费用
华东-上海一	虚拟私有云VPC	VPC-B-test	VPC网段：172.16.0.0/16 在虚拟私有云控制台创建VPC。	1	免费。
	虚拟私有云子网	subnet-VPC-B	子网网段：172.16.0.0/24 在虚拟私有云控制台创建VPC时，同时配置好子网。	1	免费。
	弹性云服务器ECS	ecs-test	私有IP地址： 在弹性云服务器控制台创建ECS，该ECS属于VPC-B-test，用于访问OBS桶。	1	本实践中，ECS按需计费，计费项包含云服务器、镜像、云硬盘等费用，请参见**ECS按需计费**。
	CC网络实例	-	在云连接控制台的云连接实例中加载华东-上海一的VPC-B-test的网络实例。	1	免费。

区域	资源	资源名称	资源说明	数量	费用
全局资源，无区域限制。	云连接CC	cloudconnect-test	在云连接控制台创建云连接实例。	1	免费。
	云连接带宽包	bandwidthPackge-test	云连接必须搭配带宽包才能正常使用。	1	本实践中，云连接带宽包按需计费，具体请参见**云连接按需计费**。
华北-北京四	CC网络实例	-	在云连接控制台的云连接实例中加载华北-北京四的VPC-A-test的网络实例。	1	免费。
	虚拟私有云VPC	VPC-A-test	VPC网段：192.168.0.0/16 在虚拟私有云控制台创建VPC。	1	免费。
	虚拟私有云子网	subnet-VPC-A	子网网段：192.168.0.0/24 在虚拟私有云控制台创建VPC时，同时配置好子网。	1	免费。
	VPC终端节点	-	在华北-北京四VPCEP控制台，购买OBS桶所在集群终端节点（OBS网关型终端节点）。	1	本实践所使用的终端节点为OBS网关型终端节点，是免费的。
	OBS桶	test-zcy-abc	用于被ECS访问的桶。 在OBS控制台创建桶。	1	根据上传至桶中的对象占用的存储空间收费，具体请参见**存储费用**。

操作流程

图 4-9 通过 CC 跨区域访问 OBS 流程图



实施步骤

步骤一：创建 VPC、ECS、OBS 桶

1. 创建VPC

在华北-北京四和华东-上海一分别创建两个VPC（VPC-A-test、VPC-B-test），用于实现相关资源的网络隔离。

步骤1 进入**创建虚拟私有云页面**。

步骤2 在“创建虚拟私有云”页面，设置以下参数，其他参数保持默认。

更多关于创建VPC的内容，请参见**创建虚拟私有云和子网**。

表 4-5 虚拟私有云参数说明

参数	示例	说明
区域	**华北-北京四**	不同区域的云服务产品之间内网互不相通，请就近选择靠近您业务的区域，可减少网络时延，提高访问速度。
名称	**VPC-A-test**	输入VPC的名称。要求如下： • 长度范围为1~64位。 • 名称由中文、英文字母、数字、下划线（_）、中划线（-）、点（.）组成。

参数	示例	说明
IPv4网段	**192.168.0.0/16**	VPC的地址范围，VPC内的子网地址必须在VPC的地址范围内。 目前支持网段范围： ● 10.0.0.0/8~24 ● 172.16.0.0/12~24 ● 192.168.0.0/16~24 未开启IPv4/IPv6双栈的区域显示参数“网段”，开启IPv4/IPv6双栈的区域显示参数“IPv4网段”。
企业项目	**default**	创建VPC时，可以将VPC加入已启用的企业项目。 企业项目管理提供了一种按企业项目管理云资源的方式，帮助您实现以企业项目为基本单元的资源及人员的统一管理，默认项目为default。 如无特殊的企业项目划分和管理需求，此处可直接选择默认企业项目“default”。 关于创建和管理企业项目的详情，请参见《企业管理用户指南》。
子网名称	**subnet-VPC-A**	输入子网的名称。要求如下： ● 长度范围为1~64位。 ● 名称由中文、英文字母、数字、下划线（_）、中划线（-）、点（.）组成。

步骤3 参数设置完成后，单击“立即创建”。

返回VPC列表，可以查看新创建的VPC。

步骤4 重复步骤1至步骤3，创建第2个VPC，参数要求如下：

- 区域：**华东-上海一**
- 名称：**VPC-B-test**
- IPv4网段：**172.16.0.0/16**
- 企业项目：**default**
- 子网名称：**subnet-VPC-B**

----结束

2. 创建ECS

在华东-上海一的VPC-B-test中创建ECS，用于访问OBS桶。

步骤1 登录控制台，进入购买弹性云服务器页面。选择“自定义购买”。

说明

以下购买ECS过程中的参数设置，仅为本实践所需参数设置，如果您还有其他需求，请根据自定义购买ECS设置ECS购买参数。

步骤2 设置“基础配置”。

表 4-6 “基础配置”参数设置说明

参数	示例	说明
计费模式	**按需计费**	选择ECS的计费模式。 按需计费：为后付费模式，先使用再付费。根据实际使用时长秒级计费，按小时结算。适用于计算资源需求波动的场景，可以随时开通，随时删除。 更多信息，请参见**计费说明**。
区域	**华东-上海一**	选择ECS所属区域。 请就近选择靠近您业务的区域，可减少网络时延，提高访问速度。ECS购买后无法更换区域，请谨慎选择。 更多信息，请参见**区域和可用区**。

步骤3 设置“操作系统”。

表 4-7 “操作系统”参数设置说明

参数	示例	说明
镜像	**CentOS 6.10 64bit (40GiB)**	华为云提供的Linux类型公共镜像。

步骤4 设置“存储与备份”。

表 4-8 “存储与备份”参数设置说明

参数	示例	说明
开启备份（可选）	**不开启**	云备份用于当发生病毒入侵、人为误删除、软硬件故障等事件时，将数据恢复到任意备份点。 本实践中，暂不需要开启备份。您在实际使用过程中，请根据需求开启。 更多信息，请参见**云备份概述**。

步骤5 设置“网络”。

表 4-9 “网络”参数设置说明

参数	示例	说明
虚拟私有云	**VPC-B-test**	选择ECS所在的VPC，用于对ECS实现网络隔离。 更多信息，请参见**虚拟私有云和子网规划建议**。
主网卡	• 主网卡：**subnet-VPC-B** • 私有IP地址分配方式：**自动分配IP地址**	选择VPC子网。

步骤6 设置“公网访问”。

表 4-10 “公网访问”参数设置说明

参数	示例	说明
弹性公网IP	**暂不购买**	如需访问公网，则可以为ECS购买和绑定弹性公网IP。 更多信息，请参见**弹性公网IP概述**。

步骤7 设置“云服务器管理”。

表 4-11 “云服务器管理”参数设置说明

参数	示例	说明
云服务器名称	**ecs-test**	根据命名规则，自定义ECS的名称。
登录凭证	**密码**	选择“登录凭证”方式为“密码”。设置密码并确认密码。

参数	示例	说明
企业项目	**default**	仅当使用企业类型的账号购买ECS时，会显示该参数。 用于按项目统一管理云资源。

步骤8 在页面右侧的“配置概要”中，确认ECS配置详情。

步骤9 阅读协议并勾选同意后，单击“立即购买”。

步骤10 支付订单，完成ECS的购买。

步骤11 单击“返回云服务器列表”，查看已购买的ECS。

----结束

3. 创建OBS桶

在华北-北京四创建OBS桶，用作被ECS访问的桶。

步骤1 在OBS管理控制台左侧导航栏选择“桶列表”。

步骤2 在页面右上角单击“创建桶”。

步骤3 设置以下参数，其他参数保持默认。

更多关于创建OBS桶的内容，请参见创建桶。

表 4-12 创建桶参数说明

参数名称	示例	说明
区域	**华北-北京四**	桶所属的区域。 ● **桶创建成功后，不支持变更区域，请谨慎选择。** ● 请选择靠近您业务的区域创建桶，以降低网络时延，提高访问速度。
桶名称	**test-zcy-abc**	创建桶时，需要设置合适的桶名称。 **桶创建成功后，不支持修改桶名称。** 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或并行文件系统（包含其他用户创建的）名称重复。**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（.），且不能以中划线（-）或英文句号（.）开头及结尾。 ● 禁止两个英文句号（.）相邻，禁止英文句号（.）和中划线（-）相邻。 ● 禁止使用IP地址。

参数名称	示例	说明
企业项目	**default**	将桶加入到企业项目中统一管理。如无特殊的企业项目划分和管理需求，此处可直接选择默认企业项目“default”。 如果您想要了解更多关于如何通过企业项目管理OBS桶，具体请参见**创建桶**中的“企业项目”参数说明。

步骤4 单击右下角的“立即创建”，确认提示信息，并单击“确定”。

步骤5 在“创建成功”弹窗，单击“确定”。在桶列表页可以看到新创建的桶，即表示创建成功。

步骤6 桶创建成功后，需要获取桶对应区域的专线域名和专线IP等信息，以便在后续配置中使用，如**表4-13**所示。其他区域可**提交工单**联系技术支持申请使用。

本实践中，test-zcy-abc桶所在区域的专线域名为“obs-private.cn-north-4.myhuaweicloud.com”，专线IP网段为“120.46.235.0/25”。

表 4-13 对应区域的专线域名和专线 IP 信息

区域名称	区域编码	专线域名	专线IP网段
华北-北京四	cn-north-4	obs-private.cn-north-4.myhuaweicloud.com	120.46.235.0/25
华东-上海一	cn-east-3	obs-private.cn-east-3.myhuaweicloud.com	123.60.199.0/25

----结束

步骤二：创建云连接实例并加载网络实例

创建云连接实例并分别在“华东-上海一”和“华北-北京四”两个区域的两个VPC中加载网络实例，使得两个区域两个VPC之间可以互相通信。

步骤1 创建云连接实例。

1. 进入**云连接实例列表页面**。
2. 单击页面右上方的“创建云连接”。
3. 在弹出的对话框中，设置以下参数，其他参数保持默认。
   更多关于创建云连接的内容，请参见**创建云连接实例**。

表 4-14 云连接实例参数说明

参数	示例	说明
名称	**cloudconnect-test**	云连接实例的名称。
企业项目	**default**	创建云连接实例时，可以将云连接实例加入已启用的企业项目。 企业项目管理提供了一种按企业项目管理云资源的方式，帮助您实现以企业项目为基本单元的资源及人员的统一管理。 如无特殊的企业项目划分和管理需求，此处可直接选择默认企业项目“default”。 关于创建和管理企业项目的详情，请参见《企业管理用户指南》。
使用场景	**虚拟私有云**	云连接实例的使用场景。 选择虚拟私有云场景时，实例类型只能选择虚拟私有云（VPC）和虚拟网关（VGW）。

4. 单击“确定”。

步骤2 加载网络实例。

1. 单击已创建的云连接实例名称，进入云连接实例基本信息页面。
2. 切换至“网络实例”页签，然后单击“加载网络实例”。
3. 在“加载网络实例”弹窗，设置如下参数，其他参数保持默认。
   更多关于加载网络实例的内容，请参见**将网络实例加载至云连接实例**。

表 4-15 加载同账号网络实例参数

参数	示例	说明
区域	**华北-上海一**	需要连接的VPC所在区域。 这里选择ECS所在区域，即华东-上海一。
VPC	**VPC-B-test**	需要加载到云连接实例中实现网络互通的VPC名称。 当实例类型参数选择虚拟私有云时，需要配置此参数。
VPC CIDRs	**subnet-VPC-B**	需要加载到云连接实例中实现网络互通的VPC内的网段路由。 当实例类型参数选择虚拟私有云时，需配置以下两个参数： - **子网：**虚拟私有云的子网，这里选择华东-上海一的VPC的子网“subnet-VPC-B”。 - **其他网段：**置空。

4. 单击“确定”。
5. 重复**步骤2.2**至**步骤2.4**，加载华北-北京四网络实例。参数要求如下：

   - 区域：**华北-北京四**
   - VPC：**VPC-A-test**
   - VPC CIDRs：
     - 选择子网：**subnet-VPC-A**
     - 其他网段：本实践中，此处填写被访问桶（华北-北京四的桶）所在区域的专线域名对应的专线IP网段，**步骤6**已获取。

步骤3 购买带宽包。

1. 切换至云连接实例的“带宽包”页签，单击“购买带宽包”。
2. 在“购买带宽包”页面，设置如下参数，其他参数保持默认。
   更多关于购买带宽包的内容，请参见**购买带宽包**。

表 4-16 购买带宽包参数

参数	示例	说明
计费模式	**按需计费**	带宽包的计费模式。 按需计费：按实际使用时长计费，可以随时开通或删除。 更多信息请参见**云连接按需计费**。

参数	示例	说明
名称	**bandwidthPackage-test**	带宽包的名称。 长度为1~64个字符，支持数字，英文字母，下划线，中划线，点。
企业项目	**default**	将带宽包加入到已启用的企业项目中进行管理。 企业项目是一种云资源管理方式，企业项目管理服务提供统一的云资源按项目管理，以及项目内的资源管理、成员管理。 如无特殊的企业项目划分和管理需求，此处可直接选择默认企业项目“default”。 关于创建和管理企业项目的详情，请参见**《企业管理用户指南》**。
互通类型	**大区内互通**	互通大区的类型。支持： - 大区内互通：指配置域间带宽的区域在同一个大区内。 - 跨大区互通：指配置域间带宽的区域在不同的大区内。 本实践中，华东-上海一和华北-北京四之间通讯属于大区内互通。
互通大区	**中国大陆**	需要实现互通的区域，即配置域间带宽时涉及的区域。
带宽	**5**	带宽是所有基于该带宽包配置的域间带宽总和，请根据网络情况提前做好规划。 单位：Mbit/s
云连接实例	**cloudconnect-test**	选择需要绑定的云连接名称。 本实践中，需要绑定**步骤1**创建的云连接示例“cloudconnect-test”。

3. 单击“立即购买”。
4. 确认购买信息无误后，单击右下角的“提交”。

步骤4 配置域间带宽。

1. 进入**云连接实例列表页面**。
2. 单击**步骤1**创建的云连接实例名称，进入“基本信息”页面。
3. 切换至“域间带宽”页签，单击“配置域间带宽”。
4. 在“配置域间带宽”弹窗，设置如下参数：

表 4-17 配置域间带宽参数

参数	示例	说明
互通区域	华东上海一、华北-北京四	需要实现互通的区域名称。 本实践中，选择华东上海一和华北-北京四互通。
带宽包	**bandwidthPackge-test**	云连接实例绑定的带宽包。 此处选择**步骤3**购买的带宽包。
带宽	5	两个区域实现互通的带宽。 **步骤3**购买带宽包时已设置，此处无需再设置。

5. 单击“确定”。

----结束

步骤三：购买 VPC 终端节点

在“华北-北京四”购买OBS网关型终端节点，使VPC-A-test中的云资源无需弹性公网IP就能够访问OBS。

步骤1 进入**终端节点列表页**。

步骤2 在“终端节点”列表页，单击“购买终端节点”，进入“购买终端节点”页面。

步骤3 “购买终端节点”页面，配置以下参数。其他参数保持默认。

更多关于购买终端节点的内容，请参见**购买终端节点**。

表 4-18 终端节点配置参数

参数	示例	描述
区域	**华北-北京四**	终端节点所在区域。 不同区域的资源之间内网不互通。请选择靠近您的区域，可以降低网络时延、提高访问速度。
服务类别	**按名称查找服务**	当您要连接的终端节点服务为用户私有服务时，需要选择“按名称查找服务”。

参数	示例	描述
服务名称	-	“服务类别”选择“按名称查找服务”，则需要配置该参数。 本实践中，此处填写被访问桶（华北-北京四的桶）所在集群终端节点服务名称，请**提交工单**获取。 输入服务名称，单击“验证”： • 若显示“已找到服务”，继续后续操作。 • 若显示“未找到服务”，请检查“区域”是否和终端节点服务所在区域一致或输入的“服务名称”是否正确。
虚拟私有云	**VPC-A-test**	选择终端节点所属的虚拟私有云。 本实践中，此处选择被访问桶所在区域华北-北京四的虚拟私有云**VPC-A-test**。

步骤4 单击右下角的“立即购买”。

步骤5 在信息确认页面，单击“提交”。

步骤6 返回终端节点列表，可以看到创建的终端节点，即表示创建成功。

----结束

步骤四：结果验证

通过使用ECS访问OBS桶的专线域名来测试域名连通性。

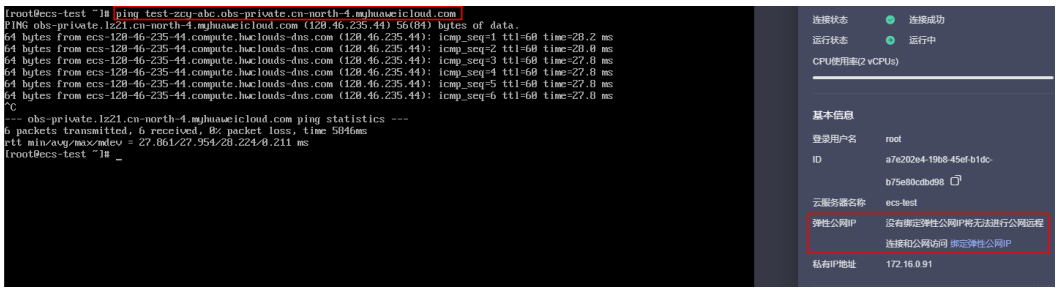
步骤1 在**云服务器列表页**，单击**步骤1**购买的ECS操作列的“远程登录”。

步骤2 在“登录Linux弹性云服务器”弹窗，选择“VNC登录”。

步骤3 输入密码，进入系统后，输入如下命令，检测ECS是否可以跨区域访问OBS桶：

```
ping 桶的专线域名
```

本实践中，命令为：ping test-zcy-abc.obs-private.cn-north-4.myhuaweicloud.com



可以看到，ECS未绑定弹性公网IP也可以跨Region访问OBS桶。

----结束

4.4 使用云专线访问 OBS

4.4.1 使用云专线访问 OBS 概述

应用场景

使用云专线可以建立企业本地数据中心IDC（Internet Data Center，以下简称IDC）与华为云间的高速、低时延、稳定安全的专属连接通道。帮助您在充分利用华为云服务优势的同时，继续使用现有的线下IT设施，实现灵活一体，可伸缩的混合云计算环境，了解更多请参见**云专线**使用云专线访问OBS有以下优势：

- 稳定高效的性能体验：云专线提供高带宽、低延迟且稳定的网络质量。这不仅保障了大数据量、高频次访问OBS时的高速传输效率，更能避免公网拥塞或波动可能引发的传输抖动或中断，为数据备份、容灾、实时数据分析等场景提供可靠的性能保障。
- 安全可靠的数据传输：通过云专线建立的是一条从用户本地数据中心到云上VPC的私有、加密网络通道。该通道与公网物理隔离，有效避免了公网传输潜在的安全风险和干扰，确保了核心业务数据上传/下载至OBS过程中的高度安全性与机密性。

您可以通过OBS桶的内网IP、专线域名、ELB代理三种方式实现云专线访问OBS。

背景介绍

了解如何使用云专线访问OBS前，您可能需要了解以下背景知识：

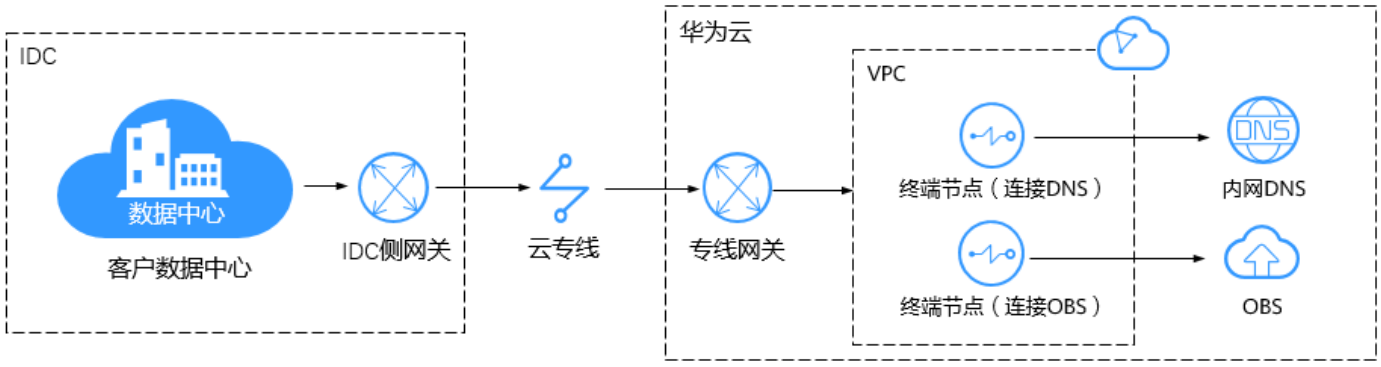
- **OBS桶域名：**桶创建成功后，OBS会根据桶名和桶的区域信息生成一个桶的默认域名“*BucketName*.obs.*RegionID*.myhuaweicloud.com”。例如华北-北京四名为example-bucket的桶，它的桶域名为example-bucket.obs.cn-north-4.myhuaweicloud.com。
- **OBS桶的内网IP：**OBS桶在华为云内网的访问地址。桶域名通过内网DNS解析得到的就是桶的内网IP，通过公网DNS解析得到的就是桶的公网IP。如果您想要通过内网访问OBS，则访问客户端必须与桶处于同一个区域，例如华北-北京四的IDC可以通过内网访问华北-北京四的OBS桶。
- **专线域名**：多云互联场景下，为了解决IDC专线接入OBS时发生的IP冲突问题，OBS为云专线场景提供了专线域名“*BucketName*.obs-private.*RegionID*.myhuaweicloud.com”，例如华北-北京四名为example-bucket的桶，它的专线域名为example-bucket.obs-private.cn-north-4.myhuaweicloud.com。
- **专线IP：**专线域名通过公网DNS解析后即可得到对应的专线IP。依据IETF和IANA标准，OBS为内网访问保留了100.125.0.0/16网段，此网段多用于IDC数据中心和云厂商内部服务互联。但是对于IDC多云互联场景，由于各云厂商均使用了该网段，导致IDC在配置各云厂商路由时出现IP冲突。为了解决该冲突，OBS为每个华为云Region预留一段专线IP，该专线IP可以通过公网DNS解析专线域名得到，但只能用于内网访问OBS。您只需打通专线IP的路由即可实现线下IDC通过云专线访问云上OBS资源。
- **ELB代理：****弹性负载均衡**（Elastic Load Balance，以下简称ELB）是将访问流量根据分配策略分发到后端多台服务器的流量分发控制服务。为OBS桶配置ELB代理后，IDC客户端只需访问ELB负载均衡器在VPC中的内网IP地址即可，ELB负载均衡器会将访问请求转发到OBS桶。

方案介绍

表 4-19 专线访问 OBS

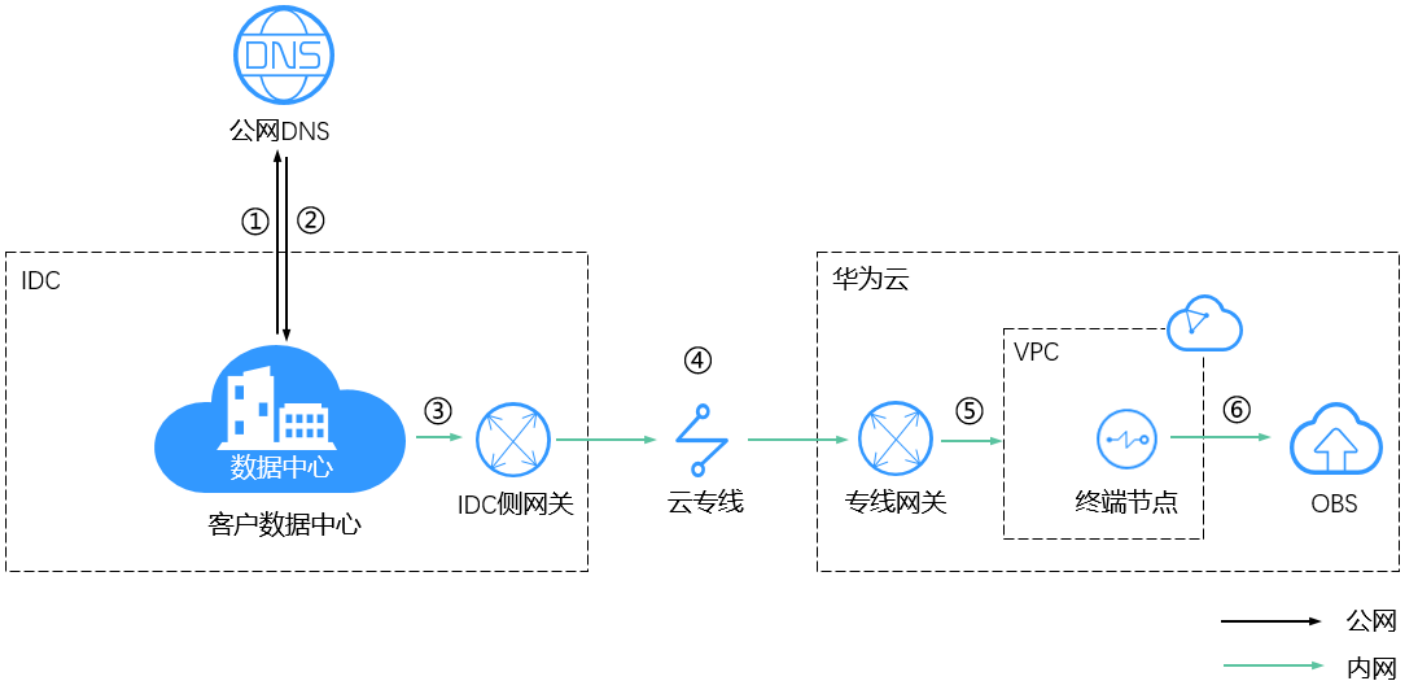
对比维度	通过OBS桶的内网IP访问	通过专线域名访问	通过ELB代理访问
适用场景	通用的云专线访问方案，需要配置内网DNS。	如果在IDC和各云厂商多云互联场景下，各云厂商内网IP网段冲突，可以使用专线域名避免冲突问题，访问OBS专门为IDC场景预留的专线IP网段。	如果IDC机房由于IP规划或其他原因，不能在本地机房配置OBS内网IP、专线IP的路由，可以使用ELB代理，访问VPC私有IP网段。
访问域名	桶域名	专线域名	不涉及
访问地址	OBS桶的内网IP	专线IP	ELB负载均衡器在VPC中的内网IP
DNS配置	内网DNS	公网DNS	不涉及
详细介绍	**通过OBS内网IP专线访问OBS**	**通过专线域名访问OBS**	**通过ELB代理访问OBS**

图 4-10 通过 OBS 内网 IP 专线访问 OBS



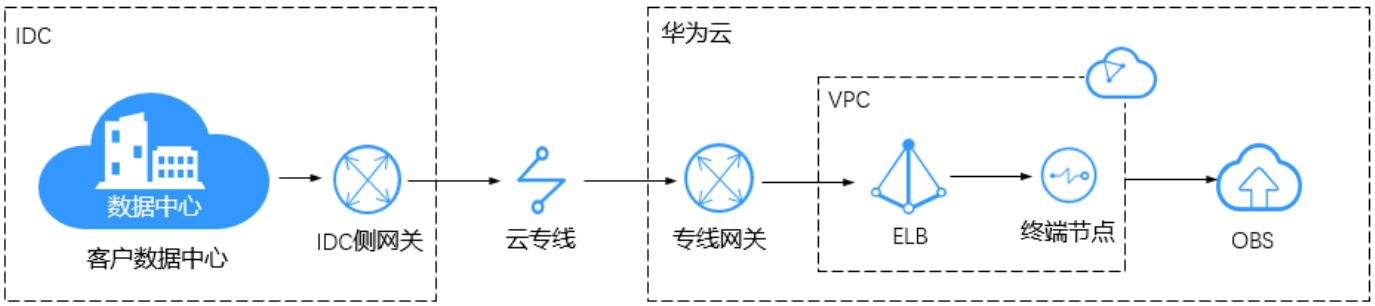
如**图4-10**所示，IDC访问OBS桶域名，内网DNS先对域名进行解析返回OBS桶的内网IP地址，然后再根据内网IP地址通过终端节点访问OBS，详情请见**通过OBS内网IP专线访问OBS**。

图 4-11 通过专线域名访问 OBS



如图4-11所示，IDC访问OBS专线域名，公网DNS先对域名进行解析返回OBS桶的专线IP地址，然后再根据专线IP地址通过终端节点访问OBS，详情请见**通过专线域名访问OBS**。

图 4-12 通过 ELB 代理专线访问 OBS



如图4-12，IDC访问ELB负载均衡器在VPC中的内网IP，ELB将请求进行转发，然后通过终端节点访问OBS，详情请见**通过ELB代理访问OBS**。

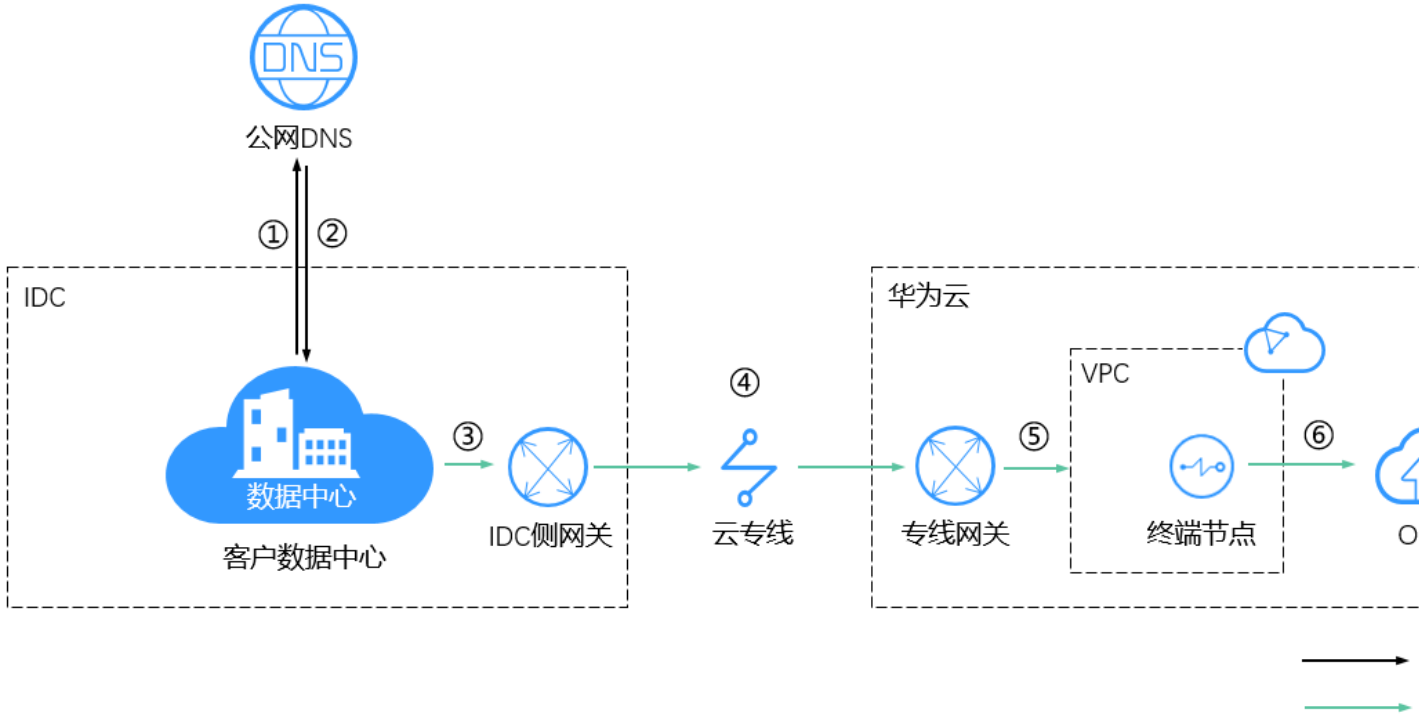
4.4.2 通过专线域名访问 OBS

应用场景

如果在IDC和各云厂商多云互联场景下，各云厂商内网IP网段冲突，可以使用专线域名避免冲突问题，访问OBS专门为IDC场景预留的专线IP网段。

方案架构

图 4-13 通过专线域名访问 OBS



如图4-13所示，IDC数据中心访问OBS的原理如下：

1. IDC数据中心使用**公网**访问OBS提供的**专线域名**（*BucketName*.**obs-private**.*RegionID*.myhuaweicloud.com）。
2. DNS域名解析系统通过**公网**返回专线接入域名对应的**专线IP**。注意，此处的DNS服务商可以是华为云DNS，也可以是其他第三方的云解析服务。
3. IDC侧网关将对**专线IP**的访问路由到云专线，发往华为云专线网关。
4. 数据通过**专线**进行传输，到达华为云的专线网关。数据传输全程在**内网**进行，与公网不发生交互，速度更快安全性更好。
5. 专线网关将对**专线IP**的访问路由到客户的**虚拟私有云VPC**。
6. 访问请求通过VPC关联的**VPCEP终端节点**到达OBS，完成对OBS的访问。

方案优势

- **架构精简：**您无需为了解析OBS域名而购买并配置DNS，OBS预留的专线域名通过公网DNS解析即可得到专线IP，直接访问专线IP即可访问OBS。
- **减少冲突：**使用专线域名访问OBS，没有使用100.64.0.0/10网段，在IDC多云互联场景不会与其他云厂商发生IP冲突。
- **传输高效：**专用网络进行数据传输，网络性能高，延迟低，用户使用体验更佳。
- **安全可靠：**云专线使用专属私密通道接入华为云VPC，网络隔离，安全性极高。

限制与约束

专线域名当前支持华东-上海一和华北-北京四，其他区域可**提交工单**联系技术支持申请使用。

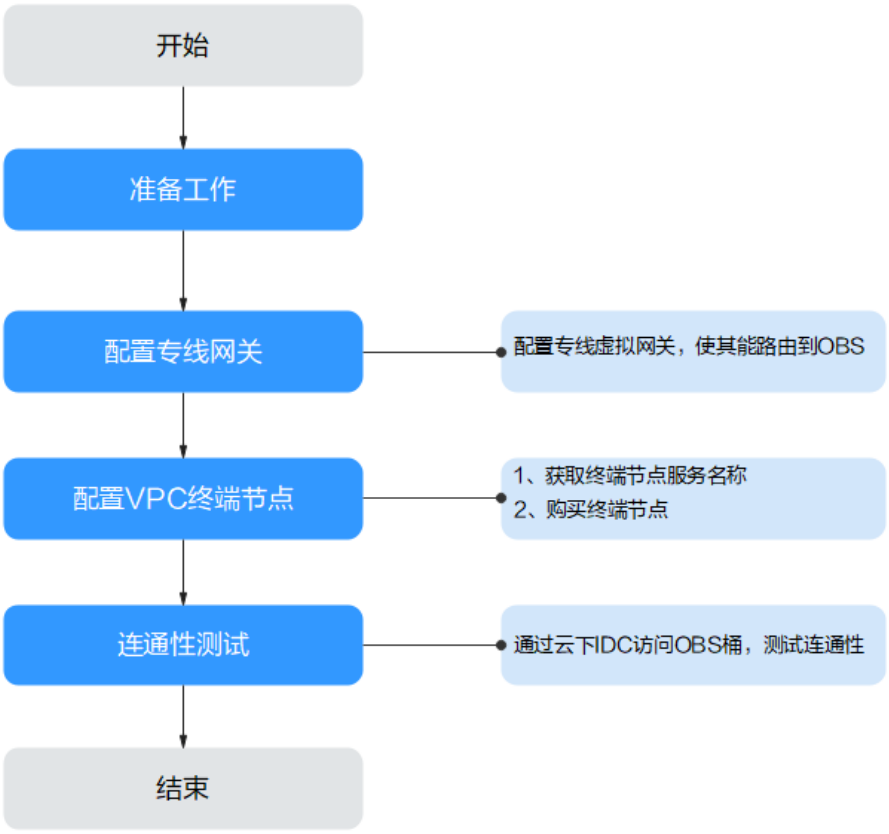
资源和成本规划

表 4-20 资源和成本规划

区域	资源	资源说明	数量	费用
相关资源需处于同一个区域，此处以“华北-北京四”为例	云专线DC	用于连接本地数据中心IDC和华为云虚拟私有云VPC。	1	详情请参见**云专线产品价格详情**。
	虚拟私有云VPC	VPC是您在云上的私有网络，为云服务器、云容器、云数据库等云上资源构建隔离、私密的虚拟网络环境。	1	免费。
	VPC终端节点	在华北-北京四VPCEP控制台，购买OBS桶所在集群终端节点。	1	免费。
	OBS桶	用于被线下IDC访问的桶。	1	详情请参见**OBS计费说明**。

操作流程

图 4-14 使用专线域名访问 OBS 操作流程



准备工作

开始执行操作前，请确保您已完成以下准备工作，注意VPC、云专线和OBS桶需要处于同一个区域中：

- 拥有一个虚拟私有云VPC，如果没有请参考**创建虚拟私有云和子网**创建VPC。
- 已使用云专线完成IDC与华为云VPC之间的通道搭建，详情参见**云专线搭建最佳实践**。
- 拥有一个OBS桶，如果没有请参考**创建桶**创建OBS桶。

步骤一：在云专线控制台配置专线网关

步骤1 进入**云专线虚拟网关列表页**。

步骤2 在页面左上角单击，选择区域和项目。

步骤3 在虚拟网关列表中，单击专线配套的虚拟网关“操作”列的“修改”。

步骤4 在“本端子网”中**添加OBS专线IP网段**，以允许云专线访问OBS专线IP网段。例如“华北-北京四”添加“120.46.235.0/25”。

区域对应的专线域名和网段如下，其他区域可**提交工单**联系技术支持申请使用：

区域名称	区域编码	专线域名	专线IP网段
华北-北京四	cn-north-4	obs-private.cn-north-4.myhuaweicloud.com	120.46.235.0/25
华东-上海一	cn-east-3	obs-private.cn-east-3.myhuaweicloud.com	123.60.199.0/25

步骤5 单击“确定”，完成虚拟网关信息的修改。

----结束

步骤二：在 VPCEP 控制台创建终端节点并配置 VPCEP 策略

步骤1 进入**VPCEP控制台终端节点列表页**。

步骤2 单击右上角“购买终端节点”，进入购买页。

步骤3 在“购买终端节点”页面，根据提示配置参数。此处仅针对本实践中的关键参数进行设置和介绍，其他参数保持默认，更多参数详细信息请参见**购买终端节点**。

参数	示例	说明
区域	**华北-北京四**	终端节点所在区域。要求与VPC、OBS桶所在区域保持一致。
计费方式	**按需计费**	按需计费是后付费模式，按终端节点的实际使用时长计费，可以随时开通/删除终端节点。
服务类别	**按名称查找服务**	选择“按名称查找服务”。
服务名称	-	在终端节点服务列表的“名称”列，输入待访问终端节点服务的名称，单击“验证”。 **提交工单**获取服务名称，提交工单时同步提供OBS桶名给技术支持人员。将从工单中获得的服务名称填写到“服务名称”中，单击“验证”。
虚拟私有云	-	选择**与云专线对接的VPC**。
策略	-	设置终端节点策略。您可以根据业务需求配置访问策略，详情参见**双端固定**。

步骤4 单击右下角的“立即购买”。

步骤5 确认终端节点配置，单击“提交”。

----结束

步骤三：连通性测试

在本地IDC客户端，访问“*BucketName*.obs-private.*RegionID*.myhuaweicloud.com”。例如华北-北京四名为example-bucket的

桶，它的桶域名为example-bucket.obs.cn-north-4.myhuaweicloud.com。如能正常访问则表示IDC已连通OBS。

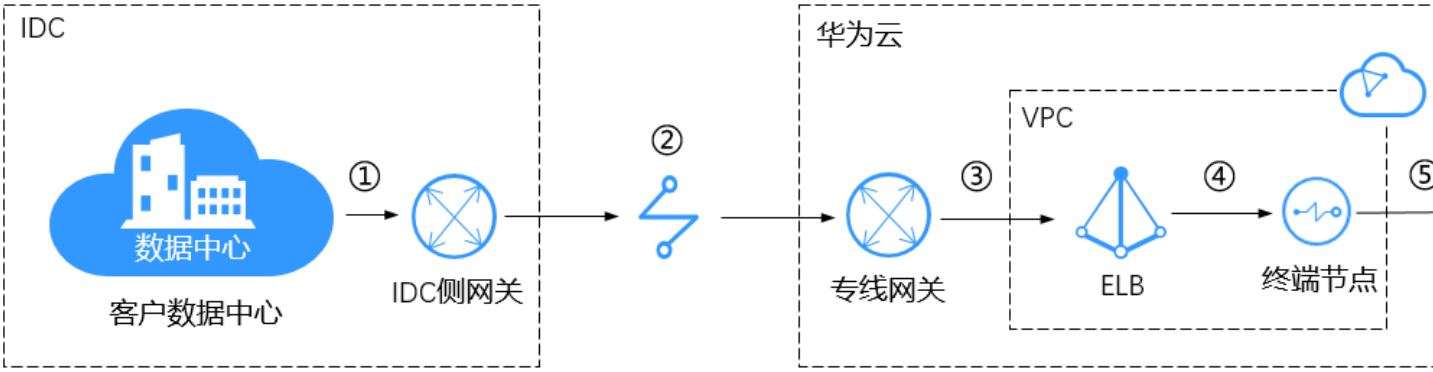
4.4.3 通过 ELB 代理访问 OBS

应用场景

如果您的IDC机房由于IP规划或其他原因，不能在本地机房配置OBS内网IP、专线IP网段的路由，只能使用虚拟私用云VPC的私有IP网段，可以参考本方案使用ELB代理实现IDC通过VPC私网IP访问云上OBS资源。

方案架构

图 4-15 使用 ELB 代理 IDC 访问 OBS



如图4-15所示，使用ELB代理实现IDC通过云专线访问OBS的原理如下：

1. IDC数据中心访问VPC私有IP。
2. IDC侧网关将对VPC私有IP的访问路由到云专线，发往华为云专线网关。数据通过**专线**进行传输，到达华为云的专线网关。数据传输全程在**内网**进行，与公网不发生交互，速度更快安全性更好。
3. 专线网关将对VPC私有IP的访问路由到客户虚拟私有云VPC中的弹性负载均衡ELB。
4. ELB将访问请求分发到与OBS桶绑定的**VPCEP**终端节点。
5. 通过VPC关联的**VPCEP终端节点**到达OBS，完成对OBS的访问。

资源和成本规划

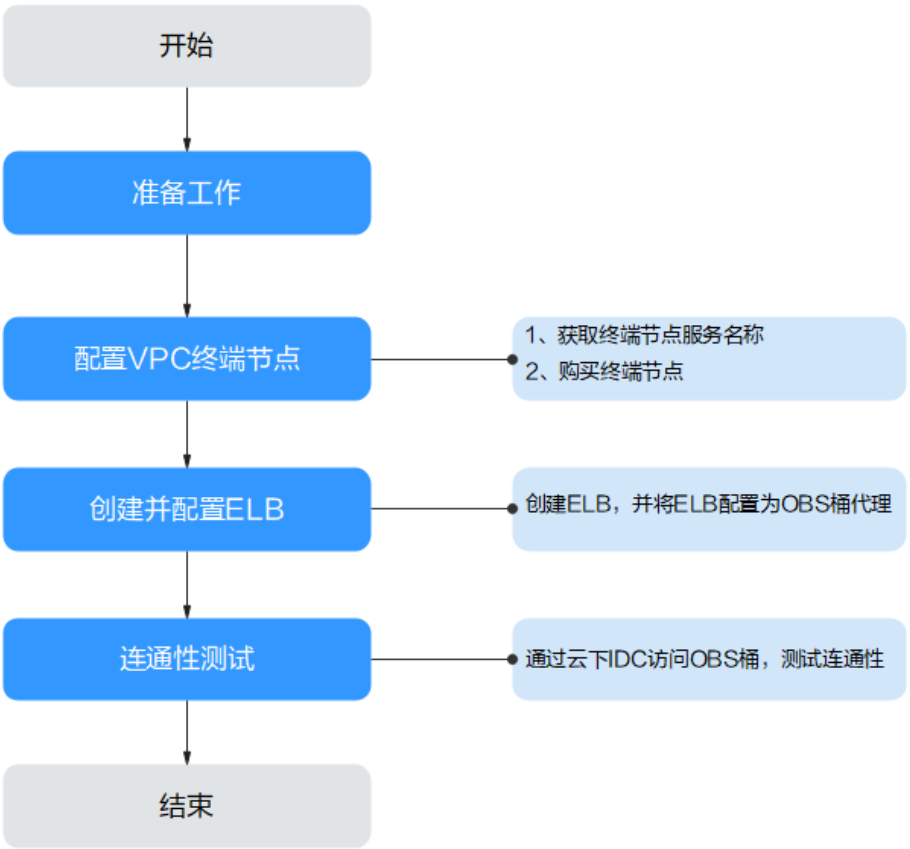
以下资源需要**部署在同一个区域**中，本文以“华北-北京四”为例。

表 4-21 资源和成本规划

资源	资源名称	资源说明	数量	费用
云专线DC	example-dc	用于连接线下数据中心IDC和虚拟私有云VPC的私有专属通道。	1	详情请参见**云专线产品价格详情**。

资源	资源名称	资源说明	数量	费用
虚拟私有云 VPC	example-vpc	VPC是您在云上的私有网络，为云上资源构建隔离、私密的虚拟网络环境，**该VPC需要与云专线相连接**。	1	免费。
ELB 负载均衡器	example-elb	作为OBS的代理，将对VPC私网IP的访问分发到OBS桶。该ELB需要部署在专线对接的VPC中。	1	详情请参见**弹性负载均衡产品价格详情**。
VPC 终端节点	example-ep	用于连接VPC与OBS桶。该VPC终端节点需要绑定与专线对接的VPC，并且与要连接的OBS桶处于同一个集群。	1	免费。
OBS 桶	example-bucket-a	被线下数据中心IDC访问的桶。	1	详情请参见**OBS计费说明**

操作流程



准备工作

开始执行操作前，请确保您已完成以下准备工作：

- 拥有一个虚拟私有云VPC，该如果没有请参考**创建虚拟私有云和子网**创建VPC。本文假设VPC部署在“华北-北京四”，名为“example-vpc”。
- 已使用云专线完成线下数据中心IDC与华为云VPC之间的通道搭建，详情参见**云专线搭建最佳实践**。本文假设云专线部署在“华北-北京四”，名为“example-dc”。
- 拥有一个OBS桶，如果没有请参考**创建桶**创建OBS桶。本文假设OBS桶部署在“华北-北京四”，名为“example-bucket-a”。

步骤一：在 VPCEP 控制台创建终端节点并配置 VPCEP 策略

步骤1 进入**VPCEP控制台终端节点列表页**。

步骤2 单击右上角“购买终端节点”，进入购买页。

步骤3 在“购买终端节点”页面，根据提示配置参数。此处仅针对本实践中的关键参数进行设置和介绍，其他参数保持默认，更多参数详细信息请参见**购买终端节点**。

参数	示例	说明
区域	**华北-北京四**	终端节点所在区域。要求与VPC、OBS桶所在区域保持一致。
计费方式	**按需计费**	按需计费是后付费模式，按终端节点的实际使用时长计费，可以随时开通/删除终端节点。
服务类别	**按名称查找服务**	选择“按名称查找服务”。
服务名称	-	在终端节点服务列表的“名称”列，输入待访问终端节点服务的名称，单击“验证”。 **提交工单**获取服务名称，提交工单时同步提供OBS桶名给技术支持人员。将从工单中获得的服务名称填写到“服务名称”中，单击“验证”。
虚拟私有云	**example-vpc**	选择**与云专线对接的VPC**。此处以部署在“华北-北京四”，名为“example-vpc”的VPC为例，该VPC与“example-dc”云专线对接。
策略	-	设置终端节点策略。您可以根据业务需求配置访问策略，详情参见**双端固定**。

步骤4 单击右下角的“立即购买”。

步骤5 确认终端节点配置，单击“提交”。

----结束

步骤二：在 ELB 控制台创建独享型 ELB 并添加监听器

创建独享型ELB

步骤1 进入**购买弹性负载均衡页面**。

步骤2 根据界面提示选择负载均衡器的基础配置，配置参数如**表4-22**所示。此处仅针对本实践中的关键参数进行设置和介绍，其他参数保持默认，更多参数详细信息请参见**购买独享型负载均衡器**。

表 4-22 负载均衡器的基础配置

参数	示例	说明
实例类型	**独享型**	选择独享型。 独享型实例适用于大流量高并发的业务场景，如大型网站、云原生应用、车联网、多可用区容灾应用。实例类型的区别详见**独享型负载均衡与共享型弹性负载均衡的区别**。
计费模式	**按需计费**	选择计费模式。 • 包年/包月：预付费模式，即先付费再使用，按照订单的购买周期进行结算。 • 按需计费：后付费模式，即先使用再付费，按照弹性负载均衡实际使用时长计费，秒级计费，按小时结算。
区域	**华北-北京四**	选择VPC和OBS所在的region，此处以“华北-北京四”为例。

参数	示例	说明
可用区	**可用区1** **可用区2**	可用区是指在同一区域下，电力、网络隔离的物理区域，可用区之间内网互通，不同可用区之间物理隔离。 建议选择多个可用区，提高服务的可用性。更多可用区规划请参考**实例可用区**。 **警告** 实例创建后，修改可用区配置可能会导致该实例的业务闪断数秒，请在购买时做好规划。
名称	**example-elb**	待创建负载均衡器的名称。 • 长度范围为1~64位。 • 名称由中文、英文字母、数组、下划线（_）、中划线（-）和点组成。
企业项目	**default**	创建负载均衡器时，可以将其加入已启用的企业项目。 企业项目是一种云资源管理方式，企业项目管理服务提供统一的云资源按项目管理，以及项目内的资源管理、成员管理。关于创建和管理企业项目的详情，请参见**《企业管理用户指南》**

步骤3 选定独享型负载均衡实例的基础配置后，您需选择弹性负载均衡的实例规格，实例规格配置参数如**表4-23**所示。

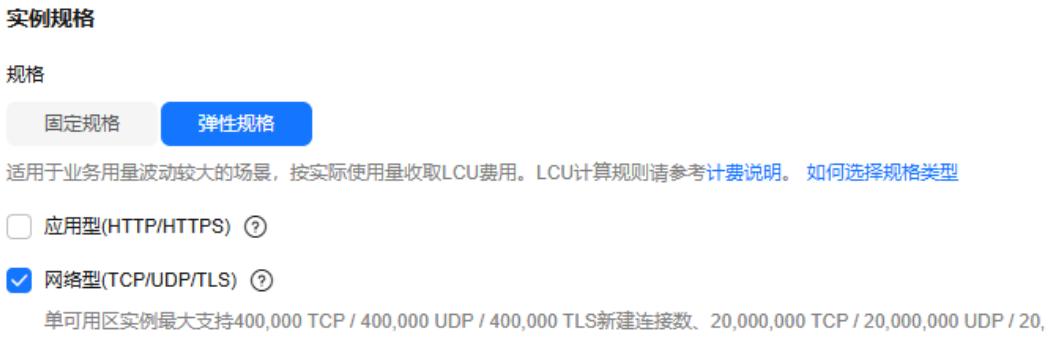


表 4-23 负载均衡器的规格说明

参数	示例	说明
规格	**弹性规格**	选择规格。 • **弹性规格**：适用于业务用量较大的场景，按实例使用量收取LCU费用。 • **固定规格**：适用于业务用量较为稳定的场景，按固定规格折算收取LCU费用。 如何选择规格详见**独享型负载均衡的实例规格**。
	网络型	只勾选网络型。**网络型**支持TCP、UDP和TLS协议，适用于四层大流量高并发业务，如文件传输、即时通信、在线视频等业务。

步骤4 请根据界面提示选择负载均衡器的网络配置，配置参数如表4-24所示。

表 4-24 负载均衡器的网络配置

参数	示例	说明
网络类型	**IPv4私网**	选择IPv4私网。负载均衡器通过IPv4私网IP对外提供服务，将来自同一个VPC的客户端请求按照指定的负载均衡策略分发到后端服务器进行处理。如果您有IPv4公网业务需求，请为负载均衡实例绑定弹性公网IP。
所属VPC	**example-vpc**	选择**专线对接的VPC**。 负载均衡器所属虚拟私有云，**独享型ELB创建完成后不支持切换**，请做好相关网络规划。
前端子网	-	前端子网为独享型负载均衡提供私网IP地址，用于与内网中的资源进行通信。请根据您的网络规划自行选择，本方案对该参数无特殊要求。
IPv4地址	**自动分配IP地址**	选择自动分配IP地址，由系统自动为负载均衡器分配IPv4地址。

参数	示例	说明
后端子网	**与前端子网保持一致**	选择与前端子网保持一致。 后端子网为独享型负载均衡提供私网IP地址，用于与后端服务器进行通信和健康检查。 通过合理规划子网，可以避免因ELB实例占用IP地址数量超过预期而影响业务扩展的情况，详情请参考**独享型ELB子网规划的推荐方案**。
IP类型后端	**开启**	开启IP类型后端。 开启后，支持用户按照IP地址为负载均衡器添加后端服务器。支持添加与ELB实例不同VPC的服务器IP地址，详情请参见**配置不同VPC的服务器作为后端服务器（IP类型后端）**。 开启IP类型后端，ELB需要占用后端子网中的IP地址与后端服务器进行通信，请确保预留足够的IP地址。

步骤5 您可以为弹性负载均衡配置弹性公网IP满足IPv4公网业务诉求，配置详情见**表4-25**。

表 4-25 为负载均衡器配置弹性公网 IP

参数	示例	说明
弹性公网IP	**暂不购买**	支持您为负载均衡器配置对应的弹性公网IP以处理IPv4公网业务流量。 • **暂不购买**：您可在弹性负载均衡创建完成后根据实际需求进行弹性公网IP的绑定。 • **现在购买**：系统为弹性负载均衡实例新创建一个弹性公网IP。 • **使用已有**：为弹性负载均衡实例选择一个已有的弹性公网IP地址。

步骤6 选择弹性负载均衡实例的购买数量，此处填写“1”。

步骤7 单击“立即购买”，完成创建。

----结束

创建监听器

您需要创建**80、443端口**共2个监听器，以下步骤以创建80端口监听器为例，执行完成后请按照相同步骤创建443端口监听器。

步骤1 进入**弹性负载均衡列表页**。

步骤2 单击上面步骤创建的负载均衡名称，此处以单击“example-elb”为例。

步骤3 切换到“监听器”页签，单击“添加监听器”，配置监听器。参见**表4-26**配置监听器参数。此处仅针对本实践中的关键参数进行设置和介绍，其他参数保持默认，更多参数详细信息请参见**添加监听器**。

表 4-26 独享型负载均衡配置 TCP 监听器参数说明

参数	示例	说明
前端协议	**TCP**	协议选择TCP。客户端与负载均衡监听器建立流量分发连接的协议。
监听端口	**单端口监听**	负载均衡器对外提供服务时接收请求的端口。选择**单端口监听**，即仅对设置的一个监听端口进行监听。
	80	端口号，是负载均衡器对外提供服务时接收请求的端口。
名称（可选）	**example-listener**	监听器名称。
访问控制	**允许所有IP访问**	您可以使用ELB监听器的**访问控制**功能来**控制访问ELB监听器的IP地址**，更多信息请参见**访问控制策略**。

步骤4 单击“下一步：配置后端分配策略”。

步骤5 选择“新创建”后端服务器组，配置后端服务器组参数请参见**表4-27**。

表 4-27 配置后端分配策略参数说明

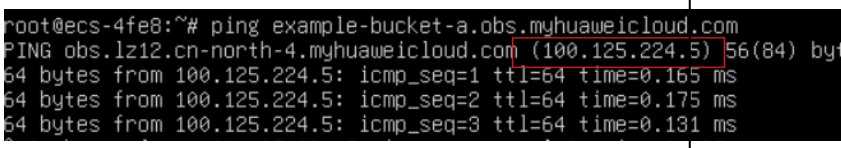
参数	示例	说明
名称	**example-server-group**	待创建的后端服务器组的名称。

参数	示例	说明
服务器组类型	**混合类型**	指定后端服务器组的类型。 混合类型既支持按照弹性云服务器和辅助弹性网卡实例添加后端服务器，也支持开启IP类型后端功能后按照IP地址添加后端服务器。 混合类型一定需要指定虚拟私有云，且后端服务器组绑定的是该虚拟私有云下的负载均衡。
转发模式	**负载均衡**	负载均衡流量转发模式，选择“负载均衡”类型。负载均衡属于普通后端服务器组，里面可以添加多个后端服务器，扩展业务的服务能力。
后端协议	**TCP**	后端云服务器自身提供的网络服务的协议，选择TCP。
IP版本	**IPv4**	后端服务器组支持添加后端服务器的IP地址版本，选择IPv4。
分配策略类型	**加权轮询算法**	负载均衡采用的算法。加权轮询算法根据后端服务器的权重，按顺序依次将请求分发给不同的服务器，权重大的后端服务器被分配的概率高。 更多关于分配策略的信息，请参见**配置流量分配策略分发流量**。

步骤6 单击“下一步：添加后端服务器”，添加后端服务器。

步骤7 选择“IP类型后端”页签，单击“添加IP类型后端”。参照**表4-28**配置IP类型后端参数。

表 4-28 添加 IP 类型后端

参数	示例	说明
IP类型后端IP	100.125.224.5	OBS桶在内网的IP地址。您可以选择以下任一种方式获取： • 提交工单获取，提交工单时同步提供OBS桶名给技术支持人员。 • 登录与OBS桶在相同region的ECS云服务器，此处以登录“华北-北京四”的ECS云服务为例，执行以下命令： **ping *BucketName*.obs.myhuaweicloud.com** 例如，执行“ping example-bucket-a.obs.myhuaweicloud.com”，系统将回显OBS桶的内网IP地址： 
业务端口	80	后端服务器处理访问请求的端口。
权重	-	后端服务器的转发权重。权重越高的后端服务器将被分配到越多的访问请求。每台后端服务器的权重取值范围为[0,100]，新的请求不会转发到权重为0的后端服务器上，请按需配置且不要配置为0。

步骤8 单击“确定”。

步骤9 单击“下一步：确认配置”。

步骤10 确认配置无误后，单击“提交”。

----结束

步骤三：连通性测试

步骤1 进入弹性负载均衡列表页。

步骤2 获取负载均衡器的服务地址，访问该服务地址即可访问OBS。

----结束

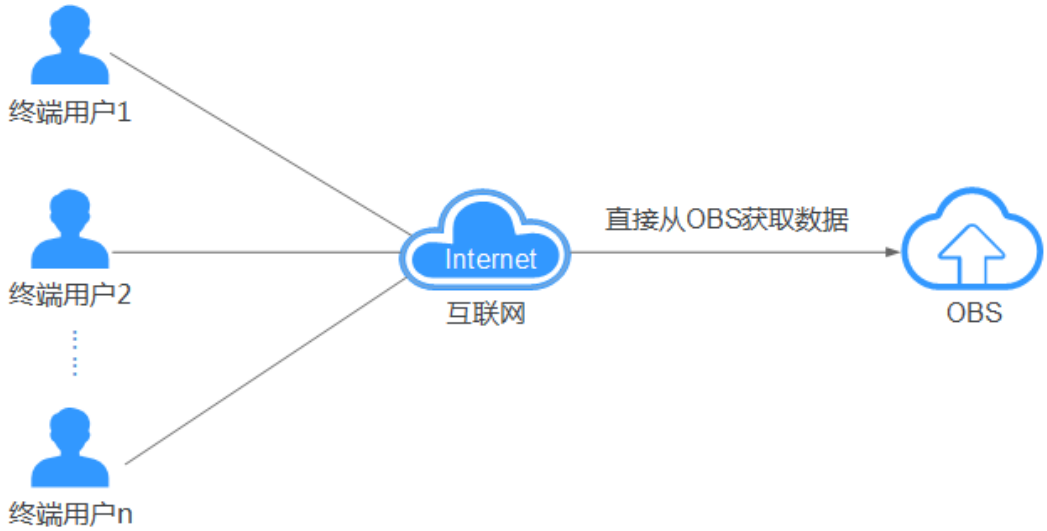
5 OBS 域名管理

5.1 通过 CDN 加速访问 OBS

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能够很好地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

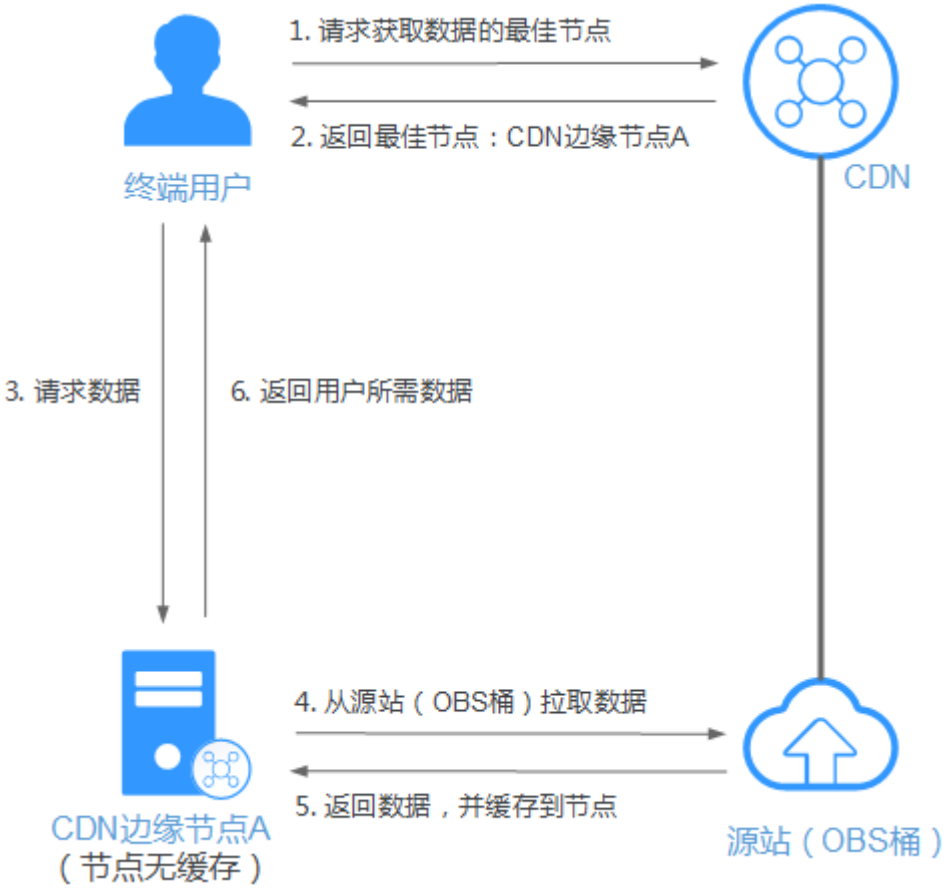


方案说明

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。

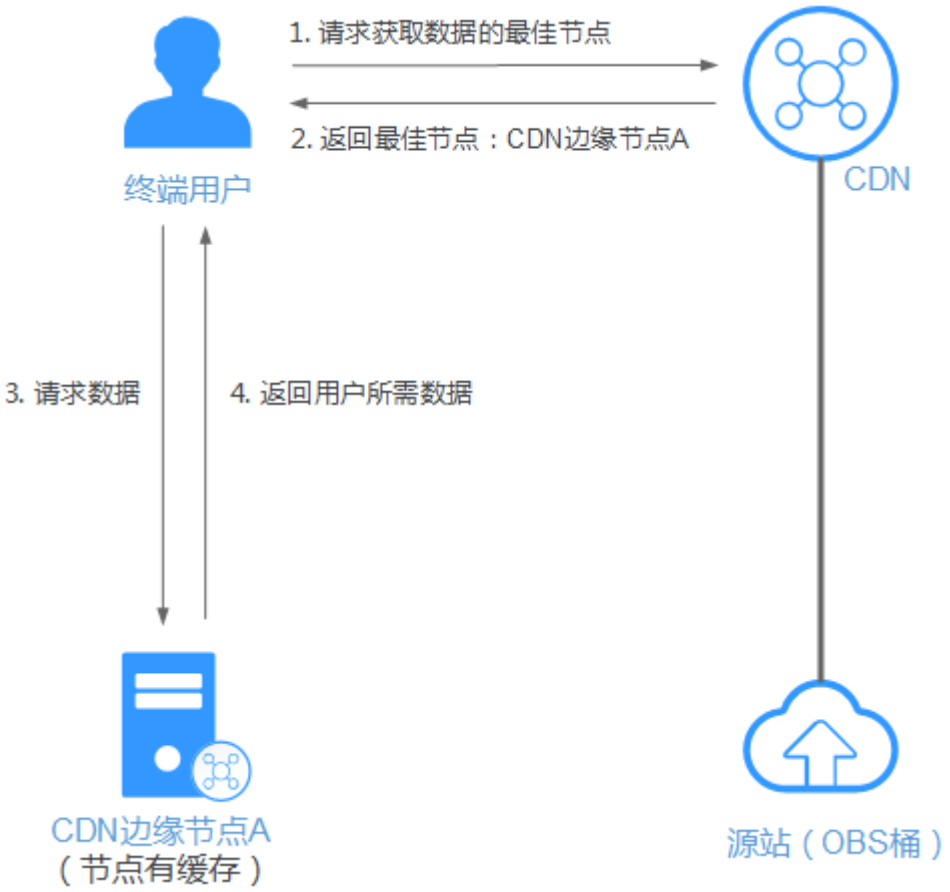
在CDN节点没有缓存用户请求的数据或缓存到期的情况下，CDN加速访问OBS的示意图如图5-2所示。

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**：OBS提供CDN回源流量包折扣方式，使CDN从OBS获取数据时流量费用更低。当数据缓存至CDN节点时，后续请求都将通过CDN回源流量计费，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更优的边缘节点，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，进入桶对象页面后单击“概览”，在“基本信息”中查看。

配置方法

- 手动配置：以点播加速为例，操作步骤请参见**通过CDN加速OBS视频点播方案介绍**。

- 一键部署：当前部分区域支持一键部署，详见**一键部署CDN下载加速**。

通过 CDN 加速 OBS 视频点播方案介绍

下面将为您介绍通过CDN加速OBS视频点播方案，包含方案的应用场景、架构和优势、约束限制，详细的资源规划和操作步骤。

应用场景

传统的点播服务会加大服务器的负载，并消耗巨大的带宽资源，同时又无法保证终端用户访问时需要的高速体验。

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。

本方案适用于提供音视频点播服务的客户。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。

方案架构

图 5-4 视频点播加速架构图

1. 客户在CDN控制台配置加速域名。
2. 终端用户A通过浏览器或APP发出请求数据，经DNS解析转向CDN节点。
3. CDN节点从OBS桶中拉取数据，OBS返回数据。
4. 数据返回至终端用户A。
5. 终端用户B访问同一数据，通过浏览器或APP发出请求数据，经DNS解析转向CDN节点。
6. 经过终端用户A的访问，CDN节点有缓存数据，直接返回所需数据至终端用户B。

方案优势

- OBS安全、高可靠且低成本，可以节省存储费用。
- 通过分布在各个区域的CDN节点，将音视频内容扩展到距离终端用户较近的地方，用户可以享受更加流畅的点播体验。
- 华为云CDN与华为云OBS通过内网连接，节省带宽费用。

综上，客户可以通过更低的费用，为终端用户提供更加优质的视频点播服务。

视频点播方案约束与限制

- 支持CDN加速的区域：华北-北京一、华北-北京四、华东-上海一、华南-广州、华南-广州-友好用户环境、西南-贵阳一。
- 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。

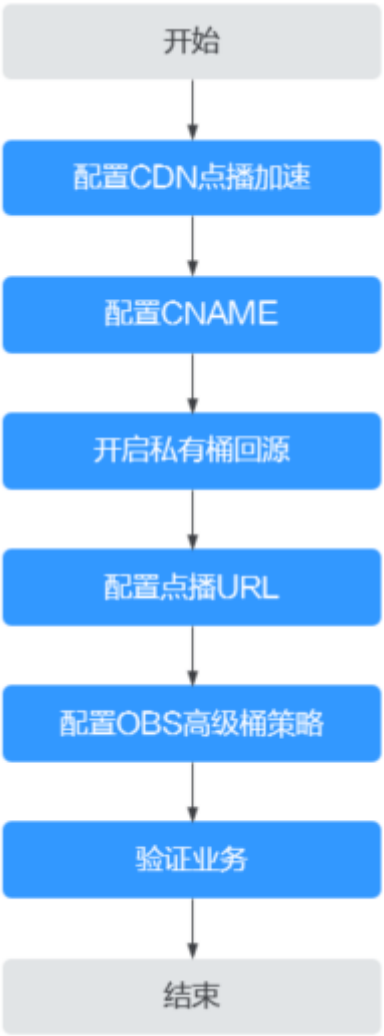
资源与成本规划

本节介绍最佳实践中资源规划情况，包含以下内容：

表 5-1 资源和成本规划内容说明

维度	说明
资源规划	**必选** ● OBS：存放图片、软件包等静态资源的桶，存储类别为“标准存储”或“低频访问存储”（归档与深度归档存储不支持直接配置CDN加速），桶策略为“私有”。 ● CDN：提供点播加速。 ● DNS：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。 ● 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。
成本规划	**必选** ● OBS费用：详见**OBS计费说明**。 ● CDN费用：详见**CDN计费说明**。 **可选** 回源流量包：当回源获取数据时，CDN访问OBS会产生回源流量。OBS提供回源流量包，可以减少回源流量产生的流量费用。 **须知** 本文提供的成本预估费用仅供参考，资源的实际费用以华为云管理控制台显示为准。

操作流程



实施步骤

步骤1 （可选）购买CDN回源流量包

当回源获取数据时，CDN访问OBS会产生回源流量。OBS提供回源流量包，可以减少回源流量产生的流量费用。如果未购买回源流量包，将按需走公网流出流量扣费。

1. 进入**购买资源包页面**。
2. 根据实际业务需求配置以下参数。
   - 区域：选择待配置CDN加速的桶所在区域。
   - 资源包类型：选择“回源流量包”。
   - 每月流量：根据每月实际流量使用情况选择合适的规格。
   - 购买数量：输入购买回源流量包的数量。与每月流量结合，以组成不同规格的回源流量包。例如购买2个每月1TB的回源流量包，则实得流量为2TB。
   - 购买时长：选择需要购买的回源流量包时长。
   - 生效时间：根据实际情况选择“支付完成后立即生效”或“指定生效时间”。

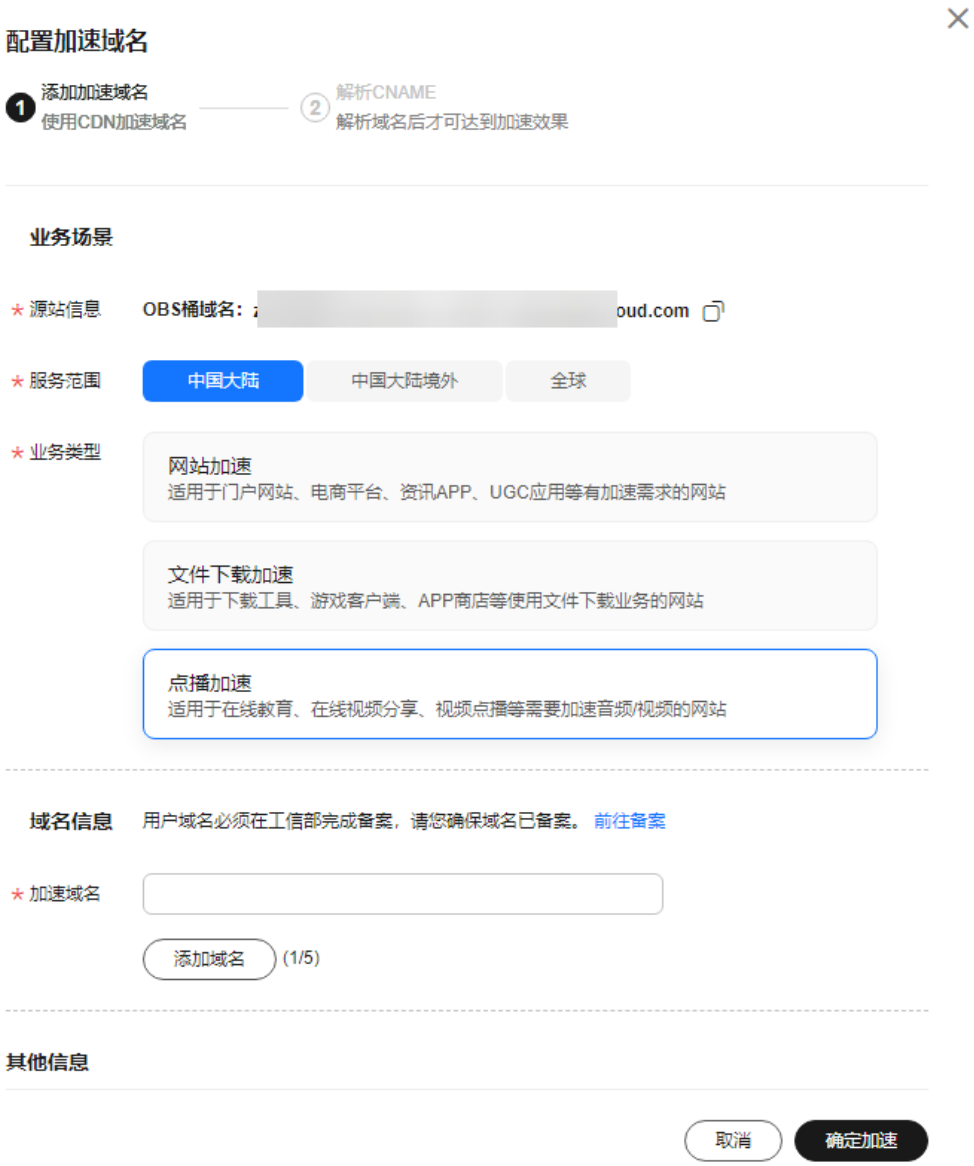
3. 单击“加入清单”。
4. 在右侧资源包清单中确认资源包信息，单击“立即购买”。

步骤2 配置CDN点播加速

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，并可以在绑定时配置CDN加速。

1. 登录OBS管理控制台。
2. 单击存放软件包的桶名称，此处以“my-video”为例。
3. 在左侧导航栏选择“域名管理”，单击“配置加速域名”。
4. 在“配置加速域名”弹框中配置CDN加速信息，如图5-5所示。
   - 服务范围：根据需要选择。
   - 业务类型：选择“点播加速”。
   - 加速域名：输入视频网站域名，此处以“click.my-video.com”为例。

图 5-5 配置加速域名



5. 单击“确定加速”。

步骤3 配置CNAME

在OBS绑定用户域名并配置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。本示例中自动生成的CNAME域名为“click.my-video.com.c.cdnhwc1.com”。

不同DNS服务商的CNAME配置方式不同，此处以华为云云解析服务为例。其他DNS服务商的CNAME配置方法可参考**配置CNAME域名解析**。

1. 登录DNS**管理控制台**。
2. 在左侧菜单栏中，选择“公网解析”，进入公网域名列表页面。
3. 在待添加记录集的域名所在行，单击“域名”列的域名名称。本实践中对应的域名为“my-video.com.”。
4. 单击“添加记录集”，进入“添加记录集”页面。
5. 根据界面提示填写参数配置，参数信息如**表5-2**所示。下表中未提到的参数可保持默认值。

表 5-2 参数说明

参数	参数说明	取值样例
主机记录	主机记录指域名前缀。	click
类型	记录集的类型，此处为CNAME类型。	CNAME-将域名指向另外一个域名
别名	用于是否将此记录集关联至云服务资源实例。	否
线路类型	用于DNS服务器在解析域名时，根据访问者的来源，返回对应的服务器IP地址。 添加解析线路类型时，切记先添加默认线路类型，以保证网站可访问。	全网默认
TTL(秒)	TTL指解析记录在本地DNS服务器的有效缓存时间。如果您的服务地址经常更换，建议TTL值设置相对小些，反之，建议设置相对大些。	默认为“5分钟”，即300s
值	需指向的域名。 如果没有开启CDN加速，该值为桶访问域名；如果开启CDN加速后，该值为CDN分配的CNAME域名。	click.my-video.com.c.cdnhwc1.com

6. 单击“确定”，完成添加。
7. 验证CNAME配置是否生效。

   打开Windows操作系统中的cmd程序，输入如下指令：


```
nslookup -qt=cname 桶绑定的自定义域名
```

本实践中桶绑定的自定义域名为“click.my-video.com”。如果回显CDN分配的CNAME域名，则表示CNAME配置已经生效。

步骤4 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。

1. 登录CDN**管理控制台**。
2. 在左侧菜单栏中，选择“域名管理”。
3. 在域名列表中，单击需要修改的域名或域名所在行的“设置”，进入域名配置页面。本实践中对应的域名为“download.game-apk.com”。
4. 选择“基本配置”页签。
5. 在源站配置模块，单击编辑。
6. 选择源站类型为OBS桶域名，桶类型选择“私有桶”，其余选项配置请参见**CDN源站配置**。
7. 单击“保存”按钮，完成源站添加。
8. 如果您账号下的此域名是初次配置OBS私有桶回源，您还需要先对CDN进行云资源委托授权，授权成功后CDN将有权限访问您账号下的OBS私有桶，授权操作请参见**OBS委托授权**。

   说明

   请勿删除CDN针对OBS的委托关系，否则会导致CDN无法在回源时从OBS私有桶获取相应资源。

步骤5 配置点播URL

将代码中需要点播加速的文件URL地址配置为：视频网站域名+文件在OBS桶中的存储路径+文件名称。

以**步骤2**配置的视频网站域名**click.my-video.com**以及存储在my-video桶中的**video/3.2.1/**文件夹下的**introduction.mp4**文件为例，文件点播URL的配置如下：

```
https://click.my-video.com/video/3.2.1/introduction.mp4
```

步骤6 配置OBS高级桶策略，避免私有桶内对象被匿名用户列举

开启私有桶回源后，任何匿名用户访问桶的自定义域名（CDN加速域名），均可列举桶根目录中的对象，导致对象列表暴露在公网。如果不希望匿名用户（未经身份认证和鉴权的用户）都能列举桶内对象，还需对列表权限进行配置，配置方法有多种，详情可参见**为什么OBS桶接入CDN后，访问域名会列出所有文件列表?**

您可根据自身业务选择配置方法，此处以其中一种配置桶策略的方法为例，配置两条高级桶策略，仅允许指定用户列举桶内对象：

1. 登录OBS**管理控制台**。
2. 单击存放软件包的桶名称（即开启了私有桶回源的OBS桶），本例中为“my-video”。
3. 在左侧导航栏选择“权限控制 > 桶策略”。
4. 单击“创建”，创建第一条桶策略。
5. 根据使用习惯，策略配置方式以可视化视图为例。单击“可视化视图”。
6. 配置如下参数。

本条策略的含义：**除了指定的用户外，其他任何人都没有桶的列举权限（List*）**。

表 5-3 桶策略参数配置说明

参数		说明
策略名称		输入自定义的桶策略名称
策略内容	效力	拒绝
	被授权用户	- 被授权用户：当前账号 - 子账号：选择允许列举桶内对象的用户。可根据实际业务需要，选择与账号同名的IAM用户或其他IAM用户
	授权资源	- 资源范围：当前桶
	授权操作	- 动作范围：自定义配置 - 选择动作：List*
	高级设置-排除策略（可选）	- 勾选：排除以上被授权用户

7. 单击右下角的“创建”，完成第一条桶策略创建。
8. 再次单击“创建”，创建第二条桶策略。
9. 根据使用习惯，策略配置方式以可视化视图为例。单击“可视化视图”。
10. 配置如下参数。

    本条策略的含义：允许指定的用户拥有桶的列举权限（List*）。此处指定的用户需要和上一条策略保持一致。

    说明

    Q：为什么还要配置第二条允许列举的桶策略?

    A：由于在控制台普通模式下创建桶策略，被授权用户无法指定到当前账号本身。所以在第一条桶策略中，被授权用户无论选择与账号同名的IAM用户或其他IAM用户，实际都把当前账号本身排除在外了。这些IAM用户之前有私有桶的列举权限，是因为账号在IAM中进行了授权。但在第一条桶策略配置完成后，账号本身不再有列举权限，导致无法给这些IAM用户授予列举权限，所以当前这些IAM用户的列举权限为默认Deny。基于显示Deny > Allow > 默认Deny的原则，还需要配置一条允许列举的桶策略，才能让这些IAM用户实现正常列举。

表 5-4 桶策略参数配置说明

参数		说明
策略名称		输入自定义的桶策略名称
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：选择允许列举桶内对象的用户。需要和第一条桶策略保持一致

参数		说明
	授权资源	- 资源范围：当前桶
	授权操作	- 动作范围：自定义配置 - 选择动作：List*

11. 单击右下角的“创建”，完成第二条桶策略创建。
12. 登录CDN控制台，在“预热刷新 > 缓存刷新”中，刷新CDN缓存，使桶策略在CDN加速域名生效。

    刷新缓存时选择“URL”类型，输入的URL为**配置文件点播URL**中添加的文件点播URL，本例中为：

    ```
    https://click.my-video.com/video/3.2.1/introduction.mp4
    ```

步骤7 验证业务

待视频网站重新部署后，登录视频网站，点播视频文件。

如果视频可以成功点播，则表示加速配置成功。

----结束

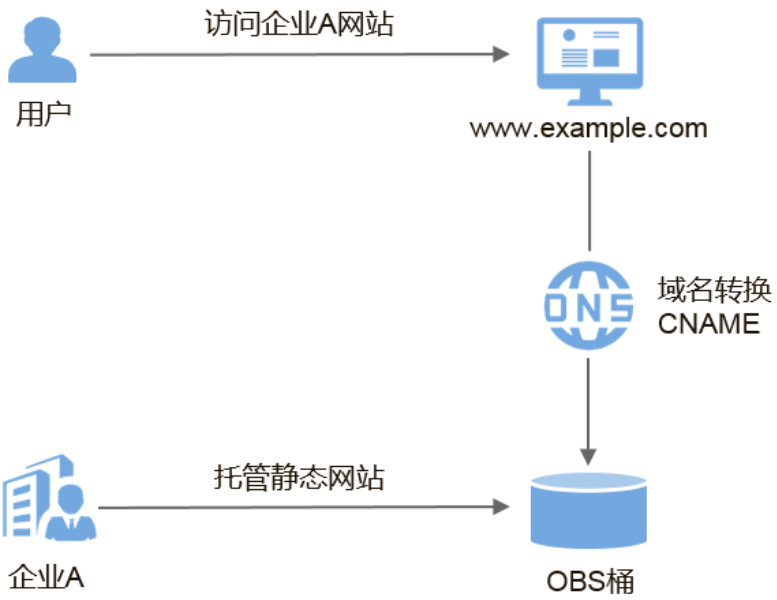
5.2 使用自定义域名托管静态网站

应用场景

当企业有大量静态网站需要提供给用户访问，却不想搭建网站服务器时，可以将静态网站托管在OBS桶中，用户可以直接通过OBS桶绑定的自定义域名访问托管的静态网站。

方案架构

图 5-6 使用自定义域名访问静态网站示意图



1. 企业将静态网站托管至OBS桶中，并为OBS桶绑定对外的自定义域名。
2. 用户访问自定义域名时，即可直接访问到存储在OBS桶中的静态网站。

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**。

方案优势

- 快速构建基于静态内容的网站，简化建站流程，降低运营成本。
- 无需搭建服务器，静态网站轻松上线。

资源和成本规划

本节介绍最佳实践中资源规划情况，包含以下内容：

表 5-5 资源和成本规划说明

资源	资源说明	成本说明
OBS	需要创建一个OBS桶用于存放静态网站文件，同时在OBS桶上完成静态网站托管配置和自定义域名绑定。	OBS的使用涉及以下几项费用： • 存储费用：静态网站文件存储在OBS中产生的**存储费用**。 • 请求费用：用户访问OBS中存储的静态网站文件时产生的**请求费用**。 • 流量费用：用户使用自定义域名通过公网访问OBS时产生的**流量费用**。 实际产生的费用与存储的文件大小、用户访问所产生的请求次数和流量大小有关，请根据自己的业务进行预估。
静态网站文件	• 静态网站首页： 访问静态网站时返回的索引页面，即首页。 示例：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。 示例：error.html	免费

资源	资源说明	成本说明
自定义域名	用户自己的域名地址，需要绑定在OBS桶上。 按照工信部要求，您绑定自定义域名的桶如果在以下区域，需要提前完成**ICP备案**。 包括：华北-北京一、华北-北京四、华北-乌兰察布一、华东-上海一、华东-上海二、华南-广州、西南-贵阳一 示例：www.example.com	准备自定义域名涉及域名注册费用，由域名注册商收取，具体费用以实际为准。
CDN	可选。可以为OBS桶绑定的自定义域名开启CDN加速，以实现更快的资源访问速度。	使用CDN加速会产生相应的流量费用，具体请参见**CDN加速OBS计费规则**。 实际产生的费用与用户访问所产生的流量大小有关，请根据自己的业务进行预估。
DNS	OBS桶绑定的自定义域名需要在DNS上配置CNAME记录。	免费

本例中，静态网站文件的示例如下：

- index.html的内容为：

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

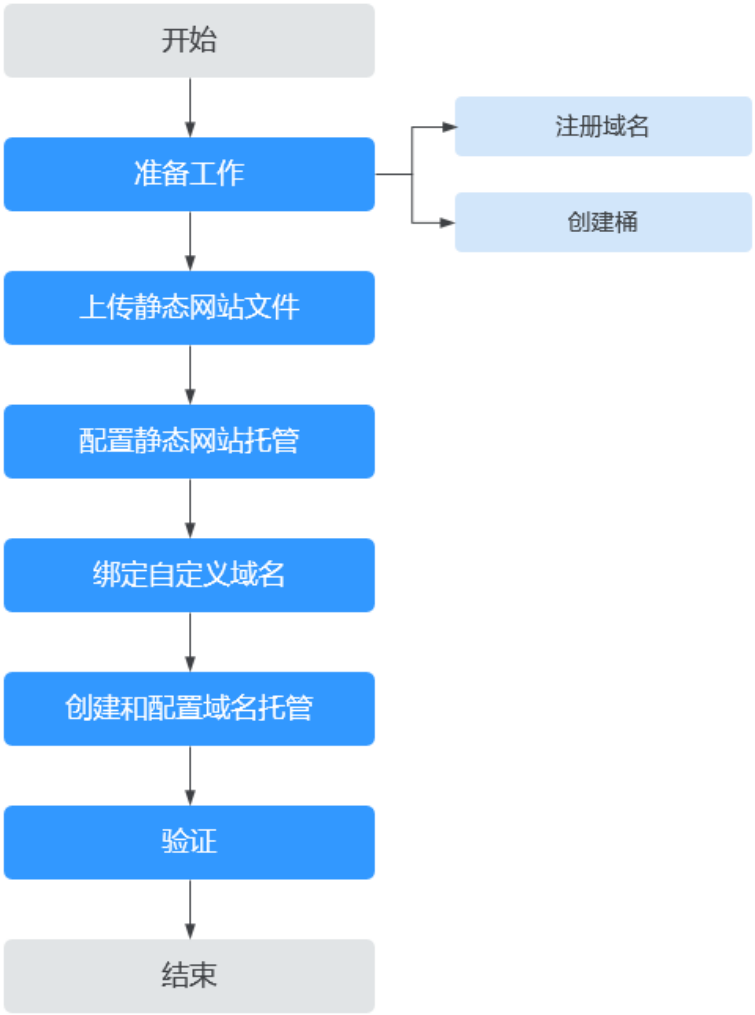
- error.html的内容为：

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

操作流程

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：

图 5-7 使用自定义域名托管静态网站流程图



准备工作

包含以下准备工作：

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。

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：

步骤1 打开**OBS管理控制台**，根据页面提示进行登录。

步骤2 在页面右上角单击“创建桶”。

步骤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。
- **默认存储类别**：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”。存储类别详细介绍请参见**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。
- **服务端加密**：选择“不开启加密”。
- **企业项目**：请先**创建企业项目**，默认为default企业项目，然后在创建桶时选择对应企业项目。仅企业账号能够配置企业项目。

步骤4 单击“立即创建”，完成桶创建。

----结束

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**准备工作**创建的桶中。

说明

在支持批量上传的区域，OBS控制台每次最多支持100个文件同时上传，总大小不超过5GB，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**。

步骤1 单击待操作的桶名称，进入桶对象页面。

步骤2 单击“上传对象”，系统将弹出如下所示对话框。

图 5-8 上传对象

步骤3 添加待上传的文件。

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。

步骤4 单击“上传”完成文件上传。

----结束

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**。

步骤1 单击桶名称，进入桶对象页面后单击“数据管理 > 静态网站托管”。

步骤2 单击“配置静态网站托管”按钮。

步骤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，如下所示。

图 5-9 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**。

步骤4 单击“确定”。

----结束

配置自定义域名

步骤1 单击桶名称进入“对象”页面，在左侧导航栏选择“域名管理”。

步骤2 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”输入“www.example.com”，如下所示。

图 5-10 配置自定义域名

步骤3 单击“确定”。

步骤4 根据页面提示，支持单击“一键解析”，或手动完成解析CNAME，单击右下角的“我已了解”，如图5-11所示。

说明

华为云域名支持一键解析添加CNAME记录；非华为云域名不支持一键解析，请用户自行配置解析规则。

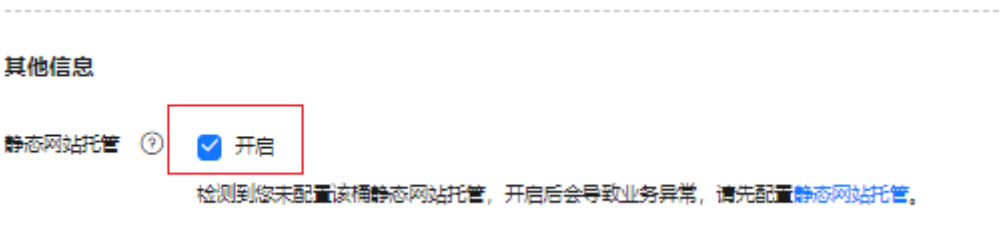
图 5-11 解析 CNAME

步骤5 （可选）配置CDN加速。

说明

CDN加速需收费，具体请参见**CDN价格说明**。

1. 在已绑定的自定义域名操作列，单击“开启加速”。
2. 根据您的业务情况选取对应的“服务范围”和“业务类型”。
3. 在“其他信息”栏目，勾选开启静态网站托管。



4. 单击“确定加速”。

步骤6 （可选）如果开启了CDN加速，需要按照以下步骤配置CDN加速。

1. 在已绑定的自定义域名操作列，单击“管理CDN加速”。
2. 在打开的CDN控制台页面，单击域名，然后再单击“高级配置”，进入域名高级配置页面。

3. 在“高级配置”中的“HTTP header配置”中，添加“Content-Disposition”响应头，取值为“inline”。

----结束

配置加速域名

步骤1 单击桶名称进入“对象”页面，在左侧导航栏选择“域名管理”。

步骤2 单击页面上方的“配置加速域名”，弹出“配置加速域名”页面，如图5-12所示。

图 5-12 配置加速域名

步骤3 选择“服务范围”，选择“业务类型”，设置“加速域名”，单击“确定加速”。

步骤4 根据页面提示，支持单击“一键解析”，或手动完成解析CNAME，单击右下角的“我已了解”，如图5-13所示。

说明

华为云域名支持一键解析添加CNAME记录；非华为云域名不支持一键解析，请用户自行配置解析规则。

图 5-13 解析 CNAME

步骤5 支持使用“自动刷新缓存”功能，如图5-14所示，在域名管理列表，找到需要创建自动刷新缓存的域名卡片，在“自动刷新缓存”的右侧单击“配置”，单击开启“自动刷新缓存”开关，出现配置页面。

图 5-14 配置自动刷新缓存

步骤6 配置自动刷新策略参数，完成后单击“确定配置”。

表 5-6 事件触发器参数说明

参数	说明
事件	自动刷新策略生效的事件类型。目前，OBS支持以下事件类型： • **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**：Put上传对象事件。 • **Post**：Post上传对象事件。 • **Copy**：使用Copy方法复制对象事件。 • **CompleteMultipartUpload**：表示合并分段任务。 • **ObjectRemoved**：表示删除对象的操作。 • **Delete**：删除对象事件。
前缀	自动刷新策略生效对象的前缀。 **说明** 当前不支持目录刷新，前缀不能以“/”结尾。
后缀	自动刷新策略生效对象的后缀。 **说明** 当前不支持目录刷新，后缀不能以“/”结尾。
IAM委托	在使用OBS的部分特性时，需要使用IAM委托功能给OBS授予相关的权限，以委托OBS处理您的数据。

步骤7 如果开启了CDN加速，需要按照以下步骤配置CDN源站信息。

1. 在已绑定的自定义域名操作列，单击“管理CDN加速”。
2. 在打开的CDN控制台页面，单击域名，进入域名基本配置页面。
3. 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，勾选“静态网站托管”。
4. 单击“确定”。
5. 在“高级配置”中添加“Content-Disposition”响应头，取值为“inline”。

说明

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**。

----结束

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

您也可以直接在域名注册商域名解析中，根据是否开启CDN加速来添加一条别名记录。

- 如果绑定自定义域名时开启了CDN加速，则添加的别名记录需指向CDN提供的加速域名。例如：域名“www.example.com”开启CDN加速后的加速域名为“www.example.com.c.cdnhwc1.com”，则需要在域名注册商添加一条值为“www.example.com CNAME www.example.com.c.cdnhwc1.com”的记录。
- 如果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“example”所处区域“华北-北京一”，则需要在域名注册商添加一条值为“www.example.com CNAME example.obs.cn-north-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：

步骤1 创建公网域名。

在云解析服务中创建公网域名，使用**准备工作**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**配置网站解析**章节中的“添加域名”部分内容。

步骤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”。
- **记录类型**：选择“CNAME – 将域名指向另外一个域名”。
- **线路类型**：选择“全网默认”。
- **TTL(秒)**：保持默认。
- **记录值**：需指向的域名。如果绑定自定义域名时没有开启CDN加速，此处填写OBS的桶的静态网站托管域名；如果开启了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**添加公网域名解析记录**。

步骤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**配置网站解析**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。

----结束

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5-15所示。

  图 5-15 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5-16所示。

  图 5-16 404 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。

（后续操作）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。

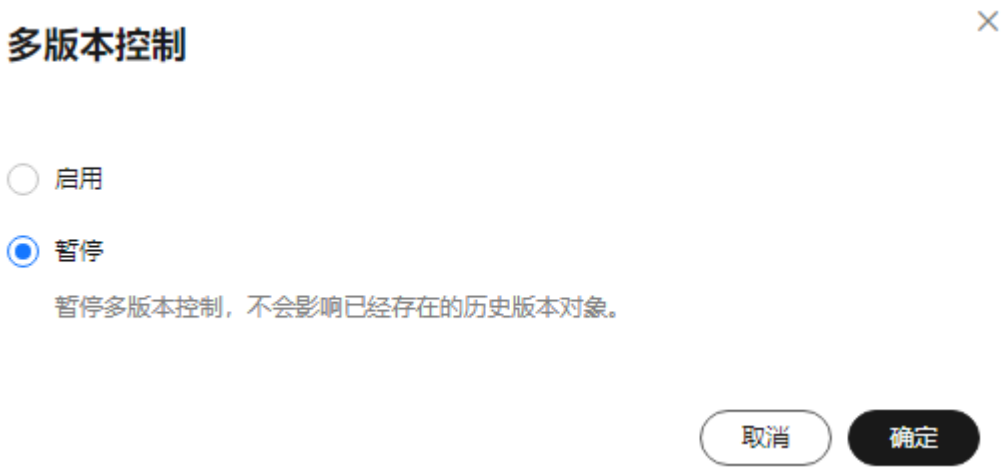
启用多版本控制

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，进入桶对象页面后在左侧导航栏单击“概览”。

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

图 5-17 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，进入对象页面。

步骤3 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”。

图 5-18 上传对象

步骤4 添加待上传文件。

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5 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

6 OBS 数据一致性校验

应用场景

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。

方案架构

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。默认情况下，OBS不会进行一致性校验，您可以通过以下方式在上传下载时主动启用校验。

说明

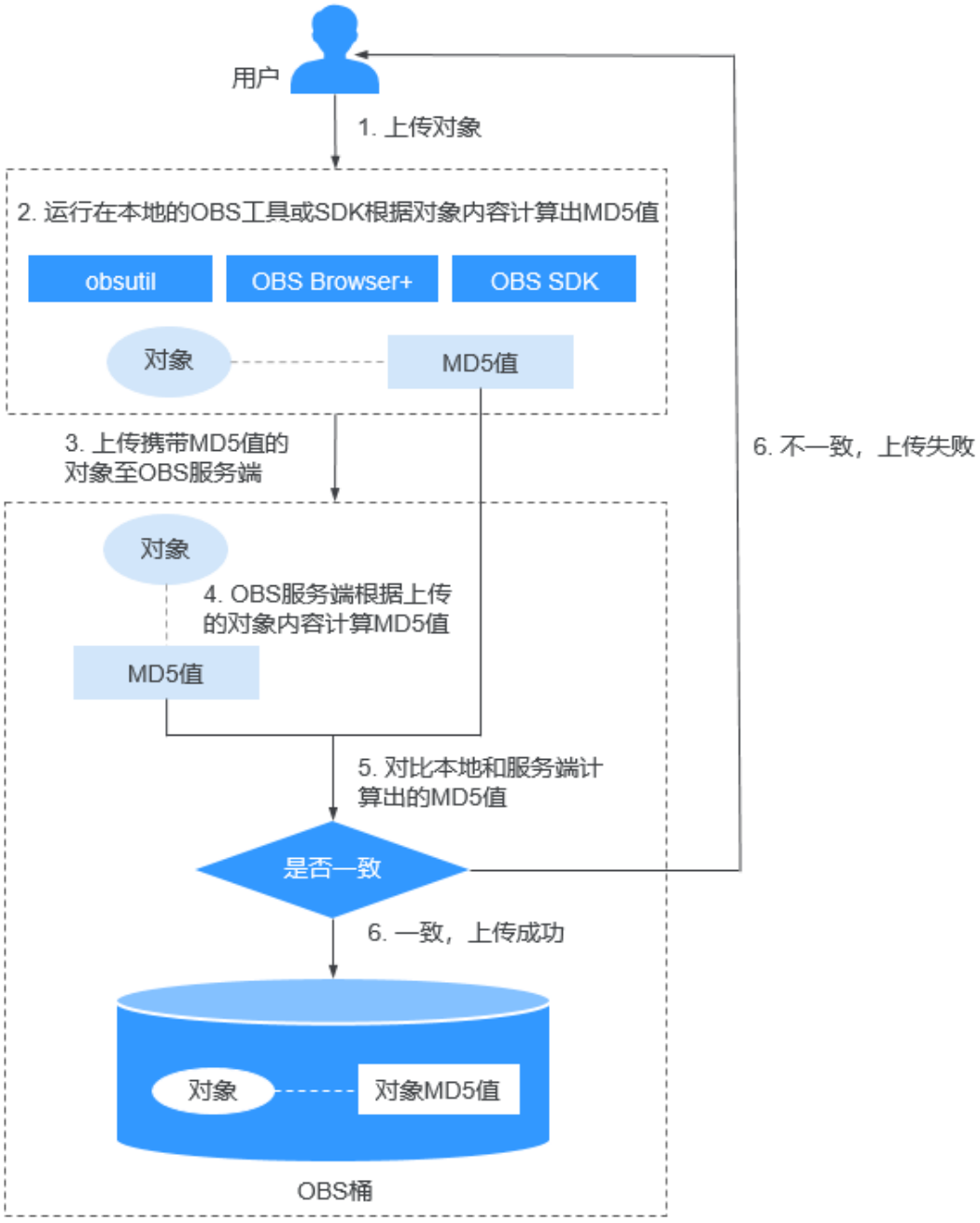
- 各种方式的一致性校验结果互通，即无论您使用以下何种方式在上传时通过了一致性校验，都可以使用其他方式在下载时校验一致性。
- 下载对象时，只有当待下载对象具有MD5值时，MD5校验才会生效。
- 启用MD5进行数据一致性校验会影响上传下载性能。

表 6-1 校验数据一致性的方式

方式	说明	操作指导
obsutil	命令行工具，可以通过简单的一行命令实现上传下载，并且在命令中选择是否采用MD5校验。	使用obsutil校验上传对象的一致性
		使用obsutil校验下载对象的一致性
OBS Browser+	图形化界面工具，可以一键开启或关闭MD5校验，同时提供任务管理，方便查看校验状态。	使用OBS Browser+校验上传对象的一致性
		使用OBS Browser+校验下载对象的一致性
OBS SDK	开发者可以通过OBS SDK进行二次开发，自行判断MD5校验结果，并根据实际业务进行结果处理。	使用OBS SDK校验上传对象的一致性
		使用OBS SDK校验下载对象的一致性

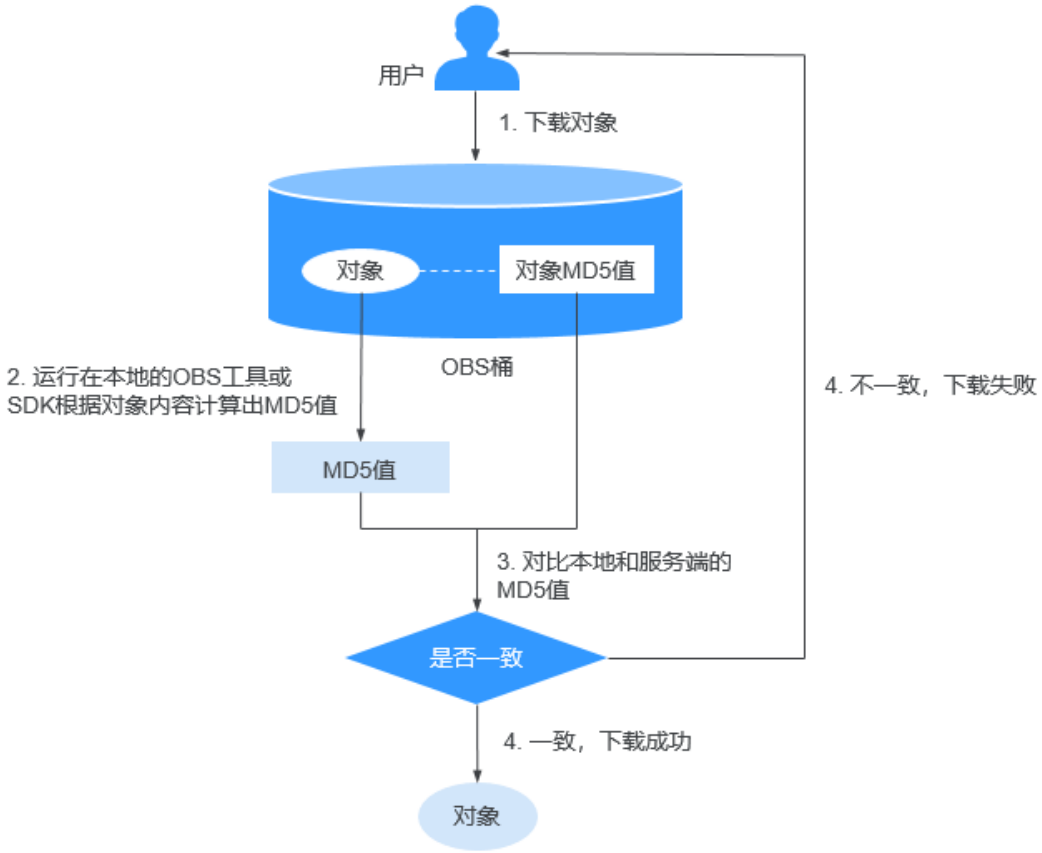
上传对象时，OBS会先在客户端计算出对象的MD5值然后携带上传至OBS，OBS服务端再根据上传的对象内容计算出MD5值，最终与携带上传的MD5值进行对比，如果对比结果一致，对象上传成功，否则上传失败。使用MD5值对上传数据进行一致性校验的示意图如图6-1所示。

图 6-1 校验上传对象的一致性



下载对象时，OBS会将对象已有的MD5值与根据下载的对象内容计算出来的MD5值进行对比，如果对比结果一致，对象下载成功，否则下载失败。使用MD5值对下载数据进行一致性校验的示意图如图6-2所示。

图 6-2 校验下载对象的一致性



校验上传对象的一致性

obsutil、OBS Browser+以及OBS SDK都支持在上传对象时进行一致性校验，您可以根据自己的业务选择任意一种方式进行校验。本文分别介绍了几种方式在上传对象时进行一致性校验的操作指导。

方式一：使用 obsutil 校验上传对象的一致性

obsutil支持在上传对象时通过附加参数（vmd5）来校验数据的一致性。

以在Windows操作系统上传本地一个位于D盘的test.txt文件至mytestbucket桶为例，开启一致性校验的命令示例如下：

```
obsutil cp D:\test.txt obs://mytestbucket/test.txt -vmd5
```

校验通过后，对象上传成功，系统显示Upload successfully的回显信息。

```
D:\obsutil>obsutil cp D:\test.txt obs://mytestbucket/text.txt -vmd5
Start at 2019-06-11 01:43:07.5075864 +0000 UTC

Parallel:       5                       Jobs:           5
Threshold:      50.00MB                 PartSize:       5.00MB
VerifyLength:   false                   VerifyMd5:      true
Exclude:
Include:
CheckpointDir: C:\Users\[redacted]\.obsutil_checkpoint

[-------------------------------------------------] 100.00% ?/s 291B/291B 50ms

Upload successfully, 291B, 2b0ec156a68e0035ea18d85c1b3ce619, D:\test.txt --> obs
://mytestbucket/text.txt, cost [108], status [200], request id [0000016B44342DC6
860CCDE792CFFC25]
```

方式二：使用 OBS Browser+校验上传对象的一致性

OBS Browser+默认关闭MD5校验，在OBS Browser+上启用MD5校验一致性并上传对象的步骤如下：

步骤1 登录OBS Browser+。

步骤2 单击客户端右上方的 

，并选择“高级设置”。

步骤3 勾选“MD5校验”，如图6-3所示。

图 6-3 配置 MD5 校验

步骤4 单击“确定”。

步骤5 选择待上传文件的桶，上传文件。

- 如果MD5校验成功，则文件上传成功。
- 如果MD5校验失败，则文件上传失败，且在任务管理中提示失败原因：校验文件MD5失败。

----结束

方式三：使用 OBS SDK 校验上传对象的一致性

OBS提供Java、Python等多种语言的SDK，各SDK通过在上传对象时设置对象的Content-MD5值以开启一致性校验。如何计算并设置对象MD5值请前往**OBS SDK**参见各自开发指南的setObjectMetadata接口。

此处以使用OBS Java SDK上传Windows本地D盘一个名为text.txt的文本文件至mytestbucket为例，上传过程使用MD5值校验数据一致性的示例代码如下：

```
String endPoint = "https://your-endpoint";
// 认证用的ak和sk硬编码到代码中或者明文存储都有很大的安全风险，建议在配置文件或者环境变量中密文存放，使用时解密，确保安全；本示例以ak和sk保存在环境变量中为例，运行本示例前请先在本地环境中设置环境变量ACCESS_KEY_ID和SECRET_ACCESS_KEY_ID。
// 您可以登录访问管理控制台获取访问密钥AK/SK，获取方式请参见https://support.huaweicloud.com/usermanual-ca/ca_01_0003.html
String ak = System.getenv("ACCESS_KEY_ID");
String sk = System.getenv("SECRET_ACCESS_KEY_ID");
// 创建ObsClient实例
ObsClient obsClient = new ObsClient(ak, sk, endPoint);
// 计算并设置MD5值
ObjectMetadata metadata = new ObjectMetadata();
File file = new File("D:\\text.txt");
FileInputStream fis = new FileInputStream(file);
InputStream is = (InputStream)fis;
String contentMd5 = obsClient.base64Md5(is);
metadata.setContentMd5(contentMd5);
// 带MD5值上传文件
obsClient.putObject("mytestbucket", "text.txt", file, metadata);
```

说明

- 对象数据的MD5值必须经过Base64编码。
- OBS服务端会将该MD5值与对象数据计算出的MD5值进行对比，如果不匹配则上传失败，返回HTTP 400错误。如果匹配，对象上传成功，返回HTTP 200状态码。

校验下载对象的一致性

OBS Browser+、obsutil以及OBS SDK都支持在下载对象时进行一致性校验，您可以根据自己的业务选择任意一种方式进行校验，本文就几种方式如何使用一致性校验进行了详细说明。

前提条件

待下载对象已有MD5值，如果没有MD5值，将不会进行一致性校验。对象的MD5值需要在上传的时候计算并设置，详细操作请参见**校验上传对象的一致性**。

方式一：使用 obsutil 校验下载对象的一致性

obsutil支持在下载对象时通过附加参数（vmd5）来校验下载数据的一致性。

以在Windows操作系统下载mytestbucket桶中的test.txt文件至本地为例，开启数据一致性校验的步骤如下：

步骤1 执行以下命令，检查待下载对象是否具有MD5信息。

```
obsutil stat obs://test-bucket/test.txt
```

- 返回的对象基本信息中，包含MD5信息，如下图所示，执行**步骤2**。


```
D:\obsutil_windows_amd64>obsutil stat obs://mytestbucket/text.txt
Start at 2019-06-10 09:07:00.9978182 +0000 UTC

Key:
  obs://mytestbucket/text.txt
LastModified:
  2019-06-10T09:04:26Z
Size:
  291
StorageClass:
  standard
MD5:
  2b0ec156a68e0035ea18d85c1b3ce619
ETag:
  2b0ec156a68e0035ea18d85c1b3ce619
ContentType:
  text/plain
```

- 不包含MD5信息，下载对象时无法进行一致性校验。

步骤2 执行以下命令，下载对象。

```
obsutil cp obs://mytestbucket/test.txt D:\test.txt -vmd5
```

- 对象下载成功且通过一致性校验，回显信息如下：

```
Download successfully, 317B, a6d2a254f93af83c6efe59232bdbb4e0, obs://mytestbucke
t/test.txt --> D:\test.txt, cost [50], status [200], request id [0000016B4466E8C
3860BFF29740B5669]
```

- 如果桶中对象没有MD5值，对象能够下载成功，但不会校验一致性，回显信息如下：

```
Download successfully, 317B, n/a, obs://mytestbucket/text.txt --> D:\text.txt, c
ost [100], status [200], request id [0000016B445FA2CB860DCF05B537DF8E]
Warn: Cannot get the valid md5 value of key [text.txt] in bucket [mytestbucket]
to check
```

----结束

方式二：使用 OBS Browser+校验下载对象的一致性

OBS Browser+默认关闭MD5校验，在OBS Browser+上启用MD5校验一致性并下载对象的步骤如下：

步骤1 登录OBS Browser+。

步骤2 单击客户端右上方的 

，并选择“高级设置”。

步骤3 勾选“MD5校验”，如图6-4所示。

图 6-4 配置 MD5 校验

步骤4 单击“确定”。

步骤5 选择待下载文件的桶，下载文件。

- 如果MD5校验成功，则文件下载成功。
- 如果MD5校验失败，则文件下载失败，且在任务管理中提示失败原因：校验文件MD5失败。

----结束

方式三：使用 OBS SDK 校验下载对象的一致性

OBS SDK对待下载对象的自定义元数据中的MD5值和下载到本地的对象的MD5值进行对比，通过对比结果判断下载对象的一致性。

⚠ 注意

1. 该功能的前提是对象自定义元数据中必须有MD5值字段，并且该字段表示的意思是原始对象的MD5值。
2. 上传过程中设置MD5值到自定义元数据中的示例代码请参考**方式三：使用OBS SDK校验上传对象的一致性**。

此处以使用OBS Java SDK下载mytestbucket桶中一个名为test.txt的文本文件为例，下载过程使用MD5值校验数据一致性的示例代码如下：

```
String endPoint = "https://your-endpoint";
// 认证用的ak和sk硬编码到代码中或者明文存储都有很大的安全风险，建议在配置文件或者环境变量中密文存放，使用时解密，确保安全；本示例以ak和sk保存在环境变量中为例，运行本示例前请先在本地环境中设置环境变量ACCESS_KEY_ID和SECRET_ACCESS_KEY_ID。
// 您可以登录访问管理控制台获取访问密钥AK/SK，获取方式请参见https://support.huaweicloud.com/usermanual-ca/ca_01_0003.html
String ak = System.getenv("ACCESS_KEY_ID");
String sk = System.getenv("SECRET_ACCESS_KEY_ID");
// 创建ObsClient实例
final ObsClient obsClient = new ObsClient(ak, sk, endPoint);
// 获取对象的MD5值
```

```
ObjectMetadata metadata = obsClient.getObjectMetadata("mytestbucket", "test.txt");
String md5Origin = metadata.getUserMetadata("contentMd5");
// 计算下载后对象的MD5值
ObsObject obsobject = obsClient.getObject("mytestbucket", "test.txt");
String md5Download = obsClient.base64Md5(obsobject.getObjectContent());
// 对比MD5值
if(md5Origin.contentEquals(md5Download))
    System.out.println("Object MD5 validation passes!\n");
else
    System.out.println("Object MD5 validation failed!\n");
```

7 OBS 数据安全

7.1 OBS 安全配置建议

安全性是华为云与您的共同责任。华为云负责云服务自身的安全，提供安全的云；作为租户，您需要合理使用云服务提供的安全能力对数据进行保护，安全地使用云。详情请参见**责任共担**。

本文提供了OBS使用过程中的安全最佳实践，旨在为提高整体安全能力提供可操作的规范性指导。根据该指导文档您可以持续评估OBS资源的安全状态，更好的组合使用OBS提供的多种安全能力，提高对OBS资源的整体安全防御能力，保护存储在OBS桶内的数据不泄露、不被篡改，以及数据传输过程中不泄露、不被篡改，确保您在OBS上的资源无合规风险。

本文从以下几个维度给出建议，您可以评估OBS使用情况，并根据业务需要在本指导的基础上进行安全配置。

- **建议妥善管理认证凭证，减小因凭证泄漏导致的数据泄露风险**
- **正确的使用OBS提供的访问控制能力保护数据不泄露、不被篡改**
- **加密存储数据**
- **构建数据的恢复、容灾能力避免数据被异常破坏**
- **确保您的数据在传输到OBS过程中不被窃取和篡改**
- **利用OBS提供的操作日志审计是否存在异常数据访问操作**
- **使用最新版本的SDK获得更好的操作体验和更强的安全能力**
- **确保您在OBS上的资源无合规风险**
- **使用其他云服务进一步增强对数据的安全防护**

建议妥善管理认证凭证，减小因凭证泄露导致的数据泄露风险

1. **建议使用临时AK/SK进行业务处理，减小因凭证泄露导致的数据安全风险**

   当部署在ECS上的应用程序或者其他华为云服务需要访问OBS资源时，必须对访问OBS的请求进行签名，因此应用程序或服务需要持有一个可以访问OBS桶的凭证。建议您为应用程序或服务配置IAM委托或临时AK/SK，通过IAM委托可以获取一组临时AK/SK，临时AK/SK到期自动过期失效，可以有效降低凭证泄露造成的数据泄露风险。详情请参见**通过临时访问密钥访问OBS**和**通过委托获取临时AK/SK**。

2. **定期轮转永久AK/SK减小凭证泄漏导致您数据泄露的风险**

   如您必须使用永久AK/SK，建议对永久AK/SK进行定期凭证轮转，同时加密存储，避免凭证长期使用过程中预置的明文凭证泄露导致数据泄露。详情请参见**通过永久访问密钥访问OBS**。

正确的使用 OBS 提供的访问控制能力保护数据不泄露、不被篡改

正确的使用OBS提供的访问控制能力，可以有效预防您的数据被异常窃取或者破坏。

1. **建议对不同角色的IAM用户仅设置最小权限，避免权限过大导致数据泄露或被误操作**

   为了更好的进行权限隔离和管理，建议您配置独立的IAM管理员，授予IAM管理员IAM策略的管理权限。IAM管理员可以根据您业务的实际诉求创建不同的用户组，用户组对应不同的数据访问场景，通过将用户添加到用户组并将IAM策略绑定到对应用户组，IAM管理员可以为不同职能部门的员工按照最小权限原则授予不同的数据访问权限，详情请参见**部门公共数据权限管理**和**策略语法**。

2. **利用桶策略保护您的数据不被异常读取和操作**

   仅在资源上配置实际业务处理中所需权限，避免权限配置过大导致数据被错误分享给他人。详情请参见**OBS权限控制概述**。

   OBS的桶策略支持多种Condition条件灵活设置，每一个Condition都是一个新的安全控制维度，建议您通过配置Condition进一步限定数据访问的上下文，如通过拒绝非指定源IP或非指定VPC对桶的访问，限制数据只能被指定客户端访问，避免数据被窃取。详情请参见**限制指定IP地址对桶的访问权限**、**配置双端固定**和**桶策略参数说明**。

3. **建议使用双端固定，即同时设置VPC终端节点策略与桶策略，对OBS的资源进行权限控制**

   设置VPC终端节点策略可以限制VPC中的服务器（ECS/CCE/BMS）访问OBS中的特定资源；同时，设置桶策略可以限定OBS中的桶被特定VPC中的服务器访问，从而在请求来源和被访问资源两个角度保证OBS数据的安全性。详情请参见**配置双端固定**。

4. **建议将需要公开访问的对象和私有的对象使用不同的桶进行存储，从而简化您的访问控制策略**

   推荐将需要公开访问的对象和私有的对象使用不同的桶进行存储。公开桶内请勿存放敏感数据，同时请避免私有桶误配置授权公开访问的桶策略导致私有对象泄露，建议存储私有对象的桶通过Condition进一步限制可以访问数据的源端确保数据不被外部攻击者窃取。详情请参见**限制指定IP地址对桶的访问权限**。

5. **建议使用OBS的数据临时分享功能来快速分享指定数据，无需进行复杂的桶策略编写**

   当需要将存放在OBS中对象（文件或文件夹）分享给其他用户时，建议使用OBS的数据临时分享功能，分享的URL可指定有效期，过期自动失效，避免数据长期暴露给其他用户导致泄露。详情请参见**通过临时URL访问OBS**。

6. **开启敏感操作多因子认证保护您的数据不被误删**

   OBS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，对数据的高危操作进行控制。详情请参见**敏感操作**。

确保您在 OBS 上的资源无合规风险

1. **关闭公开写的桶保护您的资源不被黑灰产客户利用**

当桶被配置为公开写，意味着匿名用户或模糊匹配的批量用户均可修改桶内对象，数据存在被篡改的风险。同时，公开写一旦被非法用户利用，向桶中上传违反《网络安全法》和《反电信网络诈骗法》等法规的违规内容，可能会面临云资源被监管机构封禁、桶拥有者承担法律责任的风险。您可以采取以下措施避免相关风险：

- **设置桶为私有**：遵循最小权限原则，将桶配置为仅指定用户可以访问，避免开启公共读、公共写或公共读写，防止非法用户上传违规内容，您可以使用**桶策略**或**桶ACL**进行配置。
- **开启防盗链**：配置请求标头Referer的白名单或黑名单，防止其他网站恶意引用您的文件，详情参见**防盗链**。
- **设置内容检测：**如果您的桶中存在公开内容，建议使用**Moderation（内容审核服务）**对桶内文件进行内容审核。

2. **加强对私有桶上传内容审核，避免由于不可控输入，导致合规风险**

   如果由于您的业务场景需要外部用户上传内容，存在较大合规风险，建议使用**Moderation（内容审核服务）**对桶内文件进行内容审核。

3. **使用自定义域名，保护您的业务不受其他合规管控活动的干扰**

   当华为云基础域名（myhuaweicloud.com）因合规管控等原因被相关机构接管时，使用自定义域名可以避免您的业务访问因此而受到影响。

   使用自定义域名访问OBS桶时，建议在配置域名DNS解析的过程中，将CNAME记录配置为*bucketName*.obs.*regionID*.myhuaweicloud-custom.com，其中*bucketName*为桶名，*regionID*为区域名，详情请参见**通过自定义域名访问桶**。

加密存储数据

OBS支持SSE-KMS服务端加密方案，为桶配置SSE-KMS服务端加密能力后，对于上传到桶中的每个对象，OBS都会访问KMS服务获取您指定的KMS密钥进行数据加密，避免数据明文存储。当下载对象时，OBS同样会访问KMS获取对应密钥进行数据解密，整个加解密过程中OBS都不会存储对应密钥。详情请参见**配置桶默认加密**。

OBS支持SSE-OBS服务端加密方案，为桶配置SSE-OBS服务端加密能力后，对于上传到桶中的每个对象，OBS都会进行数据加密，避免数据明文存储。当下载对象时，OBS会自动帮助用户进行数据解密。详情请参见**配置桶默认加密**。

除了SSE-KMS和SSE-OBS方案，OBS还支持SSE-C服务端加密方案，您可以在对象上传和下载的请求中携带密钥和加解密算法，OBS使用您提供的密钥和算法对对象数据进行加解密，避免数据明文存储。OBS不存储您提供的加密密钥，如果您丢失加解密密钥，则会无法获取该对象明文数据。详情请参见**服务端加密SSE-C方式**。

构建数据的恢复、容灾能力避免数据被异常破坏

预先构建数据的容灾和恢复能力，可以有效避免异常数据处理场景下数据误删、破坏的问题。

1. **建议启用多版本获得异常场景数据快速恢复能力**

   利用多版本控制，您可以在一个桶中保留一个对象的多个版本，在意外操作或应用程序故障时通过历史版本对象快速恢复数据。详情请参见**多版本控制**。

2. **建议使用跨区域复制构建异地数据容灾能力**

   有些数据需要异地备份存储，跨区域复制为您提供跨区域数据容灾的能力，满足您将数据复制到异地进行备份的需求。详情请参见**跨区域复制**。

确保您的数据在传输到 OBS 过程中不被窃取和篡改

1. **建议使用HTTPS协议访问OBS，确保数据传输过程中不被窃取和破坏**

   HTTPS（超文本传输安全协议）是一种互联网通信协议，可保护客户端与服务端之间传输的数据的完整性和机密性。建议您使用HTTPS协议进行数据访问。

2. **建议使用桶策略限制对OBS桶的访问必须使用HTTPS协议**

   为避免客户端误使用HTTP协议进行OBS业务操作，建议通过桶策略中的SecureTransport条件进行限制，限制是否必须使用HTTPS协议发起请求对该桶进行操作。SecureTransport配置为True时，发起的请求必须使用SSL加密。如何配置桶策略中Condition以及SecureTransport条件，详情请参见**桶策略参数说明**。

利用 OBS 提供的操作日志审计是否存在异常数据访问操作

1. **开启云审计服务记录OBS的所有访问操作便于事后审查**

   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。

   您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。详情请参见**审计**。

2. **开启桶Logging记录桶的所有访问请求**

   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。详情请参见**日志记录**。

3. **使用云监控服务对安全事件进行实时监控、告警**

   您在使用OBS的过程中会也可能会遇到服务端返回的错误响应，为使您更好地掌握OBS桶的状态，华为云提供了云监控服务（Cloud Eye）。您可使用该服务监控自己的OBS桶，执行自动实时监控、告警和通知操作，帮助您实时掌握桶中所产生的请求、流量和错误响应等信息。

   云监控服务不需要开通，会在用户创建资源（如OBS桶）后自动启动。

   关于云监控服务的更多介绍，请参见**云监控服务产品介绍**。

使用最新版本的 SDK 获得更好的操作体验和更强的安全能力

建议客户升级SDK并使用最新版本，可以在您使用OBS的过程中对您的数据提供更好的保护。最新版本SDK在各语言对应界面下载，请参见**OBS SDK**。

使用其他云服务进一步增强对数据的安全防护

1. **启用WAF进行静态网站防护**

   如果您需要使用OBS静态网站托管功能，为进一步提升您网站的安全性，建议您使用华为云的WAF服务对您的域名进行保护，降低网站被网络攻击的风险。详情请参见**管理防护域名**。

2. **启用安全云脑SecMaster保障OBS资源安全**

   安全云脑通过“安全上云合规检查1.0”、“等保2.0三级要求”、“护网检查”三种基线规则，检测OBS桶关键配置项，告警提示存在安全隐患的配置，并提供相应配置加固建议和帮助指导。您可以通过安全云脑的资源管理功能，快速了解到OBS桶所属区域、安全状况等信息，帮助您定位安全风险问题。详情请参见**资源管理**。

3. **隐私保护**

   随着组织管理越来越多的数据，大规模地识别和保护它们的敏感数据会变得越来越复杂、昂贵和耗时。建议您通过DSC服务对OBS桶内数据进行敏感数据识别和管理，降低隐私数据识别和保护的成本以及复杂度。详情请参见**创建敏感数据识别任务**。

7.2 减少因误操作导致的数据丢失风险

华为云无法恢复您主动删除、覆盖、配置规则自动删除或服务协议到期自动删除的OBS数据。为了避免误删操作导致业务无法正常运行，本文提供了几种规避方式，您可结合自身业务选择合适的方案。

说明

以下建议并不等同完整的安全解决方案，可能不适合您的环境或不满足您的环境要求，仅作为参考。请务必在日常使用中提高数据安全意识并时刻做好内容安全防范措施。

可能导致数据被删除或覆盖的场景

- 通过控制台、API、SDK、OBS Browser+、obsutil、obsfs方式删除对象。详情请参见**删除对象**。
- 通过控制台、API、SDK、OBS Browser+、obsutil、obsfs方式上传同名文件到OBS，会导致OBS内已有文件被覆盖。
- 如果您在生命周期规则中配置了定期删除文件的规则，OBS会根据生命周期的配置定期删除符合条件的文件。详情请参见**生命周期管理**。
- 如果您配置了跨区域复制规则，且选择的是增/删/改同步，则对源存储空间（桶）进行文件修改或删除操作时，操作会同步到目的Bucket。详情请参见**跨区域复制**。
- 没有正确的配置桶的访问权限，导致文件被他人恶意删除或覆盖。访问权限相关说明请参见**权限管理**。
- 如果账号欠费，会根据“客户等级”定义不同的保留期时长。进入保留期后您在OBS中存储的数据会予以保留，账号会处于受限状态。保留期满仍未缴清欠款，存储在OBS中的数据将被删除且无法恢复。详情请参见**欠费和续费**。

开启桶的多版本控制

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，详情请参见**多版本控制**。

跨区域复制到异地备份

您可以使用跨区域复制功能将数据复制到异地进行备份，详情请参见**跨区域复制**。

WORM 保护对象，保护期内禁止删除

您可以通过WORM功能保护对象，在保护期内阻止删除或覆盖对象，详情请参见**WORM**。

7.3 降低因恶意访问导致资金或资源包损失的风险

⚠ 注意

由于场景和业务存在差异性，以下建议可能无法完全适配您的实际环境或满足特定要求，并不等同完整的安全解决方案，仅作为参考。

如果您的OBS桶或并行文件系统遭受恶意攻击或流量盗刷，会引发信息泄露和流量激增，造成资源包耗尽、高额账单等较大的资金损失，且一旦账户余额耗尽进入欠费状态可能会影响业务正常运行：

- 账单风险

  一旦桶遭受恶意攻击或流量被盗刷，会引发流量激增，由于OBS基于实际使用的流量进行计费，因此这些恶意行为产生的所有流量费用均需由您自行承担，最终形成远高于正常使用水平的高额账单。

- 欠费风险

  受计费周期及账单处理延迟等因素制约，无法在账户余额耗尽的瞬间立即暂停服务，这就导致当恶意攻击引发高额费用时，可能出现账户欠费。账户欠费可能会影响业务正常运行 ，造成更大范围的损失。

您可以参考本文给出的一系列防护建议，有效规避此类风险，提升存储安全防护能力。

阻止桶公共访问

公共访问是指请求者无需拥有特定权限或身份验证即可访问桶和桶内数据，存在数据泄露和恶意访问导致大量外网流量的风险。为了避免这些风险，OBS支持为桶配置阻止公共访问功能（Block Public Access，以下简称BPA），以确保数据的安全性。借助BPA，桶拥有者可以集中轻松限制资源的公共访问。启用该功能后，已有的公共访问权限会被忽略，并禁止创建新的公共访问权限配置，以保障数据的安全性。

了解具体详情和操作步骤，可参考**阻止桶公共访问**。

配置双端固定实现 VPC 粒度的访问控制

使用“双端固定”特性，即同时设置VPC终端节点策略与桶策略，可以对OBS的资源提供VPC粒度的权限控制。一方面，设置VPC终端节点策略可以限制VPC中的服务器（ECS/CCE/BMS）访问OBS中的特定资源；另一方面，设置桶策略可以限定OBS中的桶被特定VPC中的服务器访问，从而在请求来源和被访问资源两个角度保障了安全性。使用双端固定，不仅能够提升数据的安全性，还能降低因恶意访问流量而导致资金损失的概率。

了解具体详情和操作步骤，可参考**双端固定**。

修改 ACL 为私有访问权限

除非您有明确需求，允许包括匿名访问者在内的所有人员对您的OBS资源进行读写操作，否则尽量避免将桶或对象的ACL设置为 “公共读写（public-read-write）” 或 “公共读（public-read）”。以下是对这两种公共权限的说明：

- 公共读写：任何人（包括匿名访问者），都有权对该桶内的对象进行读写操作。任意用户都能访问桶内对象，并可向桶中写入数据，这不仅可能导致数据泄露，还会因为大量写入操作使费用急剧增加。更严重的是，若恶意写入违法信息，还会损害您的合法权益。因此，除特殊场景外，不推荐配置公共读写权限。
- 公共读：只有桶所有者能写桶内数据，但任何人（包括匿名访问者）都能进行读操作。由于互联网上的任何用户都能访问桶内数据，同样存在数据泄露和费用激增的风险，操作时务必谨慎。

考虑到“公共读写”或“公共读”带来的数据安全隐患，强烈建议您将桶或对象的读写权限设置为 “私有（private）”，即只有桶或对象所有者才能够读写桶和桶内数据，其他人员均无法访问。但在将ACL修改为私有前，请务必确认您的业务不会受到影响。了解具体详情和操作步骤，可参考**ACL**的相关内容。

通过桶日志监控恶意访问 IP

开启桶日志，监控桶日志中的“Remote IP”字段，该字段用于记录发起访问请求的IP地址，您可以灵活使用该字段实现桶的安全防护：

- 识别陌生或可疑IP地址的访问：分析Remote IP字段可识别来自陌生或可疑IP地址的访问尝试，进而发现潜在的恶意攻击，如暴力破解、数据窃取等。如果发现某个IP地址频繁发起异常访问请求，就可以采取相应的安全措施，如限制该IP的访问权限。
- 对存储桶的访问流量进行分析和管理：监测Remote IP字段来观察不同IP地址或IP地址段的流量使用情况，发现异常的流量高峰时及时采取措施应对可能的网络拥塞或DDoS攻击。
- 历史记录审查：定期回顾桶日志中的Remote IP字段历史记录，查找长期存在但未被发现的异常访问模式或潜在的安全威胁迹象。例如，发现某个IP地址在过去一段时间有异常行为，通过历史记录审查可以及时发现并采取措施。

了解具体详情和操作步骤，可参考**桶日志**。

配置防盗链

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。防盗链就是通过配置基于请求标头Referer的访问规则，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，从而防止其他网站盗用您的文件，并避免由此引起的不必要的流量费用增加。

例如，某个桶配置了白名单Referer为https://11.11.11.11。

- 用户A在https://11.11.11.11嵌入test.jpg图片，当浏览器请求访问此图片时会带上https://11.11.11.11的Referer，此场景下OBS将允许该请求的访问。
- 用户B盗用了test.jpg的图片链接并将其嵌入https://22.22.22.22，当浏览器请求访问此图片时会带上https://22.22.22.22的Referer，此场景下OBS将拒绝该请求的访问。

了解具体详情和操作步骤，可参考**防盗链**。

设置跨域资源共享

跨域资源共享（Cross Origin Resource Sharing，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支持根据您的业务场景灵活配置CORS规则，实现允许或者拒绝相应的跨域请求，确保跨域数据传输的安全性。

了解具体详情和操作步骤，可参考**配置CORS实现跨域访问OBS**。

避免使用顺序前缀的方式命名文件

如果您在上传对象时采用容易被总结规律的方式进行对象命名，比如按照时间戳、字母顺序排列、日期或数字ID等，攻击者一旦发现命名规律，即可根据规律批量获取文件，导致数据泄露。为了避免这种情况，建议使用更安全的命名方法，例如在文件名前加上十六进制哈希值，这种随机生成的字符序列很难被预测，能降低文件名被恶意遍历的风险，进而降低恶意访问的风险。

7.4 降低因账号密码泄露带来的未授权访问风险

在云服务环境中，账号和密码作为最基本的认证机制，是保护用户资源的第一道防线。一旦这些凭证遭到泄露，攻击者可能获得未经授权的访问权限，进而对存储在云端的对象（如文件、数据库等）执行非法操作，包括但不限于读取、修改或删除数据。这种行为不仅会直接导致数据丢失或损坏，还可能造成财务损失、声誉损害以及法律纠纷。

为了确保资源的安全性，建议您不要将所有资源集中放置在一个账号下。考虑到不同资源的内容及其访问场景存在差异，建议根据这些差异将资源分配至不同的账号中，以实现账号级的隔离。

与此同时OBS也提供了一些降低未授权访问风险的方法：

- 通过权限控制方式来确保数据安全，包括IAM权限和桶策略配置。
- 通过多因素认证方式来降低未授权访问的风险。
- 通过临时访问密钥方式来降低未授权访问的风险。

创建 IAM 用户并授权使用 OBS

华为云账号默认拥有所有API的访问权限，这意味着如果账号凭证不慎泄露，可能会导致严重的安全风险。为了降低这种风险，您可以使用**IAM权限**进行精细的权限管理。

您可以通过IAM为不同的用户或应用分配具有特定权限的角色，从而限制他们只能访问被授权的资源和服务。确保团队成员或应用程序仅能访问执行其工作所需的最小权限集。例如您的员工中有负责软件开发的人员，您希望他们拥有创建桶的使用权限，但是不希望他们拥有删除桶等高危操作的权限，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创建桶，但是不允许删除桶资源的权限，控制他们对OBS资源的使用范围。

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。自定义策略中可以添加的授权项（Action）请参考**桶相关授权项**和**对象相关授权项**。

桶策略设置

桶策略允许您为特定的用户或账号设置对OBS桶及其内部对象的访问权限。通过合理配置桶策略，可以有效地降低数据风险：

- 细粒度访问控制：通过桶策略，您可以灵活定义“谁”（用户、账号、IP等）在“什么条件下”（时间、来源IP等）对“哪些资源”（桶或对象）执行“哪些操作”（读、写、删除等）。这样可以确保只有授权用户才能访问敏感数据。
- IP白名单/黑名单：您可以设置桶策略来限制只能从特定的IP地址范围访问OBS桶，从而防止来自未知或不受信任位置的访问尝试。

桶策略通用配置方法如下：

- **使用模板创建桶策略**
- **自定义创建桶策略（可视化视图）**
- **自定义创建桶策略（JSON视图）**

配置桶策略，请注意以下几点：

- 定期审查和更新策略，及时清理无效规则。
- 仅授予必要权限，避免使用"Action": "obs:*"。
- 桶策略与IAM策略共同作用时，最终权限同账号内取并集，跨账号取交集。了解详情参见**访问控制机制冲突时，如何工作?**
- 启用HTTPS访问，HTTPS可以对数据进行加密和防止中间人攻击，确保敏感信息不被窃取。
- 请谨慎设置匿名访问。允许匿名访问机制将导致OBS暴露于未授权访问风险中，互联网中的任意用户均可访问桶。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）。攻击者仅需通过公开信息获取Endpoint（如obs.cn-north-4.myhuaweicloud.com）及目标桶名称，即可直接访问数据资源。

使用多因素认证

多因素认证是一种非常简单的安全实践方法，它能够在用户名称和密码之外再额外增加一层保护。启用多因素认证后，用户进行操作时，除了需要提供用户名和密码外（第一次身份验证），还需要提供验证码（第二次身份验证），因此您的账号和资源将有更高的安全保护。开启多因素认证详情参见**虚拟MFA**。

通过临时访问密钥访问 OBS

OBS可以通过IAM获取临时访问密钥（临时AK，SK和securitytoken）进行临时授权访问。通过使用临时AK，SK和securitytoken，您可以为第三方应用或IAM用户颁发一个自定义时效和权限的访问凭证。

临时访问密钥相比IAM用户的永久访问密钥的优势主要有两点：

- 临时访问密钥的有效时间为15min至24h，不必暴露出IAM用户的永久密钥，降低了账号泄露带来的安全风险。
- 在获取临时访问密钥时，通过传入policy参数设置临时权限来进一步约束使用者的权限范围，方便IAM用户对使用者的权限进一步管理。

操作详情请参见**临时授权访问OBS**。

⚠ 注意

在使用IAM权限之前需明确用户所需要的权限集合，避免权限过大造成的安全风险。

7.5 强制桶加密

应用场景

如果您的业务场景对安全性、合规性要求较高，可使用Organizations云服务提供的SCP策略，强制要求绑定策略的成员账号在创建桶时必须开启服务端加密，且现有桶不允许执行关闭桶加密操作。

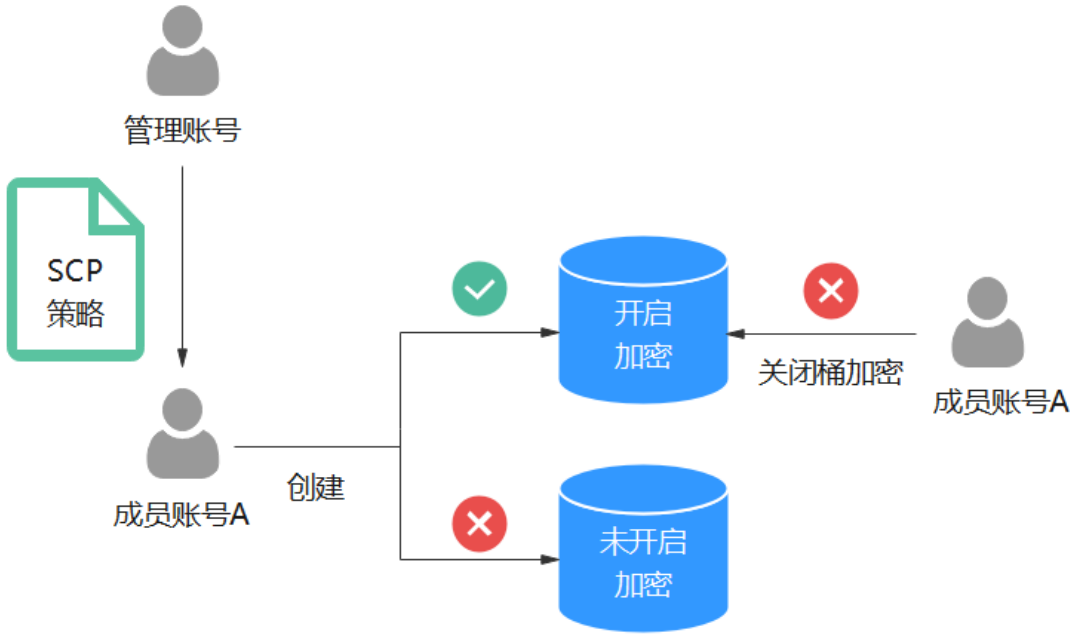
背景介绍

在使用华为云的过程中，您可能不仅仅只拥有一个华为账号，而是同时拥有多个华为账号，例如企业A有下属子公司B、C、D，企业A总部有账号a，下属子公司分别有账号b、c、d。为了帮助您更高效地管理多个账号，华为云提供了**Organizations云服务**，使用Organizations您可以创建一个组织，然后将多个账号都加入到组织中进行统一管理。

- **组织：**组织是为管理多账号关系而创建的实体，一个组织由一个管理账号和若干个成员账号组成，详情请参见**组织概述**。
- **管理账号**：管理账号是创建组织的账号，管理账号可通过策略（例如服务控制策略）对成员账号进行权限和资源的管理，详情请参见**组织相关账号概述**。
- **成员账号**：除管理账号外，组织中的剩余账号都为成员账号，详情请参见**组织相关账号概述**。
- **组织单元：**组织单元是成员账号的容器或分组单元，一个组织单元下可以关联多个子组织单元或者成员账号，详情请参见**组织单元**。
- **服务控制策略**(Service Control Policy，以下简称SCP)：Organizations提供的一种基于组织的访问控制策略，管理账号可以使用SCP指定成员账号的权限边界，限制成员账号的操作，详情参见**SCP策略概述**。

方案架构

图 7-1 使用 SCP 策略实现强制桶加密



本文将展示如何使用SCP策略实现强制桶加密，如图7-1所示，管理账号创建了一个组织，账号A是组织中的成员账号且受到管理账号的管理。管理账号通过SCP策略的方式，限制了成员账号A的创建桶行为，强制成员账号A只能创建加密桶，非加密桶的创建会被拒绝。同样，可以使用SCP策略规定现有桶不允许执行关闭桶加密操作。

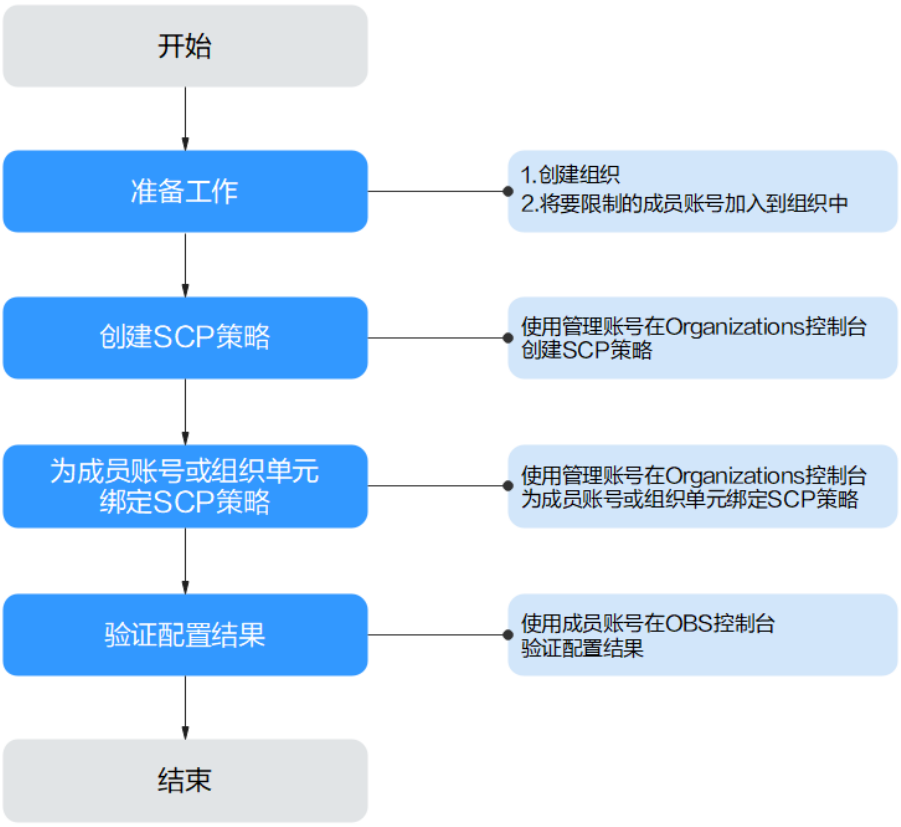
约束与限制

成员账号绑定SCP策略后，策略将在30分钟内生效。

操作流程

配置强制桶加密的流程如下：

图 7-2 强制桶加密操作流程



步骤一：在 Organizations 控制台完成准备工作

配置强制桶加密前，请确保您已完成了以下准备工作：

步骤1 创建组织，如何创建组织请参考**创建组织**。创建完成后，创建组织的账号会自动成为组织的管理账号。

步骤2 使用管理账号将需要限制行为的成员账号加入到组织中，如何邀请账号加入组织请参考**邀请账号加入组织**。

步骤3 【可选】为了方便您后续对账号的管理，建议您将需要管理的账号移动到组织单元中，如何新建组织单元请参见**新建组织单元**，如何移动账号到组织单元请参见**移动账号**。这样后续绑定SCP策略时，只需要绑定组织单元，策略就会对组织单元下的所有成员账号生效，提升您的管理效率。

----结束

步骤二：在 Organizations 控制台创建 SCP 策略

步骤1 使用**管理账号**登录**Organizations控制台**，单击左侧树中的“策略管理”，进入策略管理页。

步骤2 单击“服务控制策略”，进入SCP管理页。

步骤3 单击“创建”，进入SCP创建页。

步骤4 输入策略名称。注意，创建的策略名称不能与已有策略名称重复。

步骤5 （可选）输入策略描述。

步骤6 编辑SCP策略。以下为两个SCP策略示例供您参考：

示例一：创建桶必须开启服务端加密，对加密方式不做限制，也不限制加密配置是否能关闭。

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "obs:bucket:createBucket"
      ],
      "Condition": {
        "Bool": {
          "obs:BucketEncrypted": [
            "false"
          ]
        }
      }
    }
  ]
}
```

示例二：创建桶必须开启服务端加密并使用SSE-KMS加密方式，且现有桶不允许执行关闭桶加密操作。

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "obs:bucket:createBucket"
      ],
      "Condition": {
        "StringNotEquals": {
          "obs:x-obs-server-side-encryption": [
            "kms"
          ]
        }
      },
      "Resource": [
        "*"
      ]
    },
    {
      "Effect": "Deny",
      "Action": [
        "obs:bucket:putEncryptionConfiguration"
      ],
      "Condition": {
        "Bool": {
          "obs:BucketEncrypted": [
            "false"
          ]
        }
      }
    }
  ]
}
```

步骤7 单击右下角“保存”后，系统会自动校验语法，如跳转到策略列表，则SCP创建成功。如提示“策略内容格式不正确”，请按照**SCP语法规范**进行修改。

----结束

步骤三：在 Organizations 控制台为成员账号或组织单元或绑定 SCP 策略

步骤1 使用**管理账号**登录**Organizations控制台**，单击左侧树中的“策略管理”，进入策略管理页。

步骤2 单击“服务控制策略”，进入SCP策略列表页。

步骤3 单击**步骤二**中创建的SCP策略右侧的“绑定”，在弹窗中选中要绑定SCP策略的成员账号或组织单元。

步骤4 在弹窗中输入“确认”，单击右下角“确定”，完成策略绑定。

----结束

步骤四：在 OBS 控制台验证配置结果

验证示例一：

步骤1 使用**成员账号**在OBS**管理控制台**左侧导航栏选择“桶列表”。

步骤2 在页面右上角单击“创建桶”。

步骤3 参照**如何创建桶**配置桶参数，不开启服务端加密。

步骤4 配置完成后单击“立即创建”，如果创桶失败，则说明配置生效。

----结束

验证示例二：

步骤1 使用**成员账号**在OBS**管理控制台**左侧导航栏选择“桶列表”。

步骤2 在页面右上角单击“创建桶”。

步骤3 参照**如何创建桶**配置桶参数，不要选择SSE-KMS加密方式。

步骤4 配置完成后单击“立即创建”，如果创桶失败，则说明强制使用SSE-KMS的策略生效。

步骤5 接下来验证禁止关闭桶加密的策略。打开服务端加密并选择SSE-KMS加密方式，创建一个开启SSE-KMS加密的桶。

步骤6 创桶成功后在桶列表中，单击新建的桶，进入“对象”页。

步骤7 在左侧导航栏，单击“概览”，进入“概览”页。

步骤8 在概览页的“基础配置”区域下，单击“服务端加密”卡片，系统弹出“服务端加密”对话框。

步骤9 关闭服务端加密，单击“确认”。如果关闭失败，则说明“禁止关闭桶加密”的策略生效。

----结束

8 OBS 性能优化建议

OBS按照对象名的UTF-8编码范围来进行分区管理，对系统进行水平扩展与动态负载均衡。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。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。

示例：

比如典型的日志归档场景，可能上传的对象名都是如下形式：

```
yourbucket/obslog/20190610-01.log.tar.gz
yourbucket/obslog/20190610-02.log.tar.gz
yourbucket/obslog/20190610-03.log.tar.gz
yourbucket/obslog/20190610-04.log.tar.gz
...
yourbucket/obslog/20190611-01.log.tar.gz
yourbucket/obslog/20190611-02.log.tar.gz
yourbucket/obslog/20190611-03.log.tar.gz
yourbucket/obslog/20190611-04.log.tar.gz
```

建议为对象名添加3位以上16进制哈希前缀：

```
yourbucket/6ac-obslog/20140610-01.log.tar.gz
yourbucket/b42-obslog/20140610-02.log.tar.gz
yourbucket/17f-obslog/20140610-03.log.tar.gz
yourbucket/ac9-obslog/20140610-04.log.tar.gz
...
yourbucket/95d-obslog/20140611-01.log.tar.gz
yourbucket/4a5-obslog/20140611-02.log.tar.gz
yourbucket/ea2-obslog/20140611-03.log.tar.gz
yourbucket/ba3-obslog/20140611-04.log.tar.gz
```


9 大数据场景下使用 OBS 实现存算分离

9.1 大数据场景下使用 OBS 实现存算分离方案概述

应用场景

随着大数据技术的飞速发展，对数据价值的认识逐渐加深，大数据已经融入到了各行各业。根据相关调查报告数据显示，超过39.6%的企业正在应用大数据并从中获益；超过89.6%的企业已经成立或计划成立相关的大数据分析部门；超过六成的企业在扩大大数据的投入力度。对各行业来讲，大数据的使用能力成为未来取得竞争优势的关键能力之一。

在大数据场景下，数据已成为新资产，智能已成为新生产力。企业迫切需要完成数字化转型，提高生产力，使数据资产发挥最大价值。而传统企业在业务未上云之前，业务部署和数据存储往往都在本地IDC机房的多个集群，且一台服务器同时提供计算和存储能力，这种方式导致的如**表9-1**所示的几个关键问题，已成为企业数字化转型的阻碍。

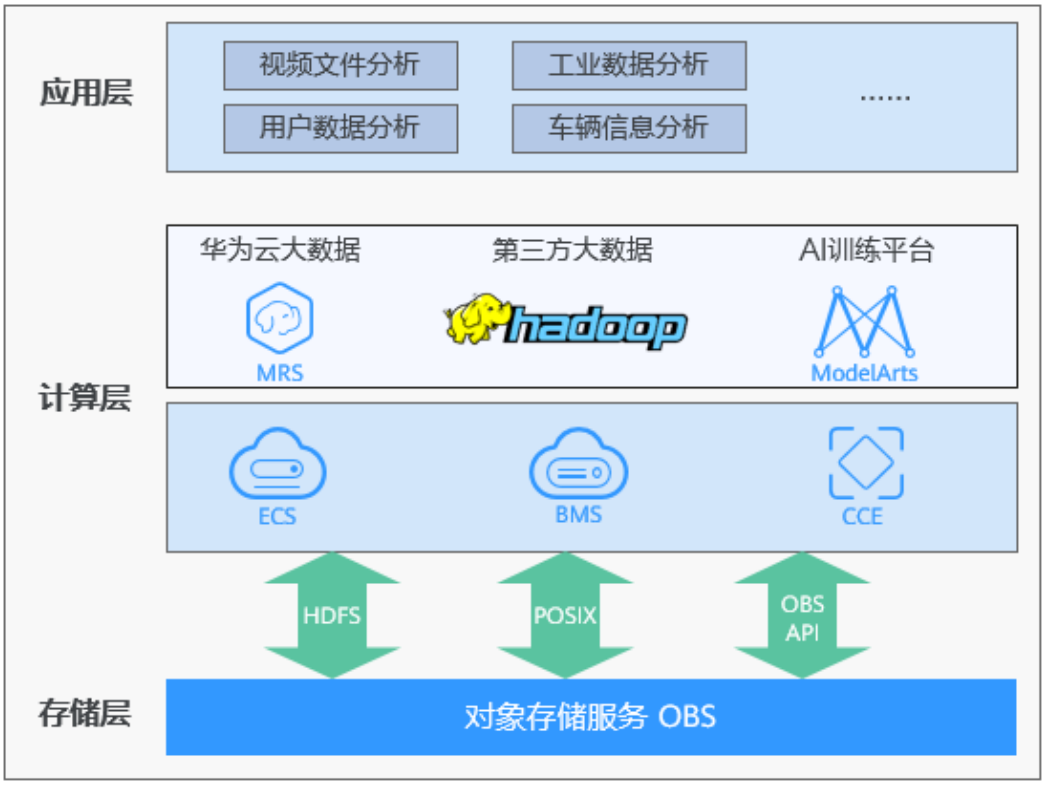
表 9-1 传统企业在大数据场景面临的关键问题

序号	关键问题	详细描述
1	多集群数据共享难	企业数据往往分别存储在IDC多个集群，存在如下问题： ● 无全局视图，数据只能在集群内部使用。 ● 拷贝是跨集群数据共享的唯一途径，数据拷贝耗时长。 ● 公共数据集多份存储，数据冗余。
2	计算存储资源绑定，导致资源浪费	计算和存储资源无法均衡，当计算和存储需求不一致时，只能等比扩容，势必造成一种资源的浪费。
3	数据三副本存储，利用率低，成本高	Hadoop分布式文件系统（HDFS）使用三副本保存数据，磁盘空间利用率仅33%，单盘利用率低于70%。

方案架构

针对传统企业在大数据场景面临的问题，华为云提供了基于对象存储服务OBS作为统一数据湖存储的大数据存算分离方案。

图 9-1 基于 OBS 的华为云大数据存算分离方案



华为云大数据存算分离方案基于对象存储服务OBS的大容量高带宽能力，以及多协议共享访问技术（HDFS/POSIX/OBS API），实现Hadoop生态多计算引擎（Hive、Spark等）兼容对接。

方案优势

相比传统企业在本地IDC机房部署大数据业务，华为云数据存算分离方案的主要优势如表9-2。

表 9-2 华为云大数据存算分离相比传统大数据方案的优势

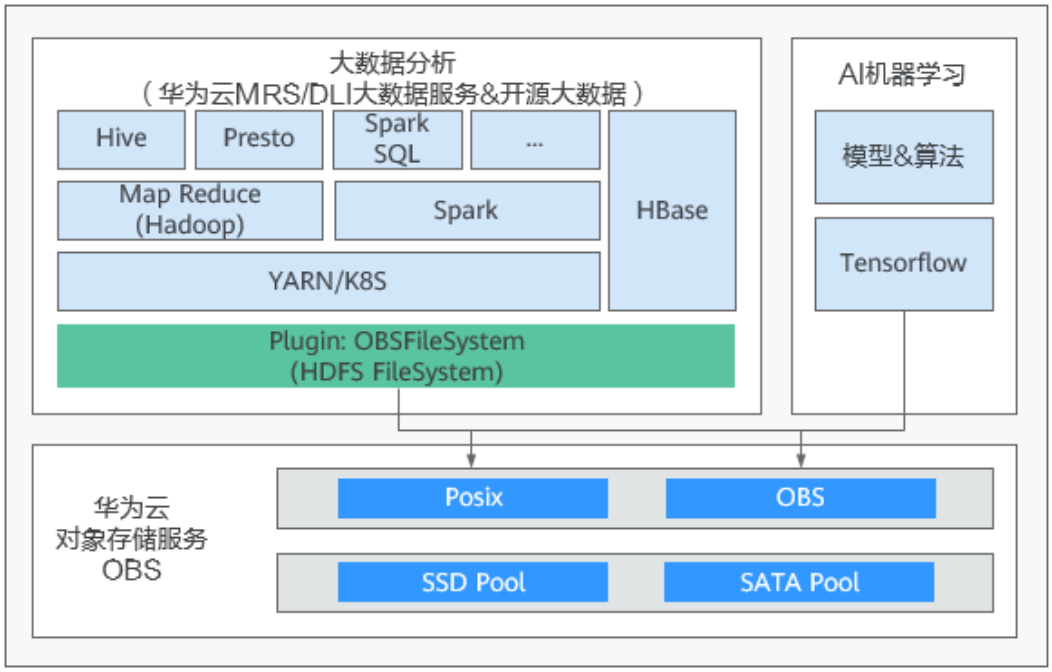
序号	主要优势	详细描述
1	融合高效，协同分析	• 通过统一的权限控制，实现多集群间的数据共享。 • 数据“0”拷贝。 • 大数据和AI一体化，减少作业耗时。
2	存算分离，资源利用率高	计算存储解耦，支持独立扩容或缩容，计算资源可弹性伸缩，资源利用率提升。

序号	主要优势	详细描述
3	数据EC冗余存储，利用率高，成本低	对象存储服务OBS支持利用率最高的分布式数据容错技术Erasure code，磁盘利用率大幅提升，数据存储空间需求远低于三副本。

此外，对象存储服务OBS提供了**OBSFileSystem插件（OBSA-HDFS）**，可与上层大数据平台无缝对接，实现业务零改造。

OBSFileSystem的主要作用：提供HDFS文件系统的相关接口实现，让大数据计算引擎（Hive、Spark等）可以将OBS作为HDFS协议的底层存储。

图 9-2 存算分离方案中的 OBSFileSystem



说明

OBS服务支持对象存储桶（对象语义）和并行文件系统（POSIX文件语义），在大数据场景下建议选择并行文件系统。并行文件系统支持POSIX文件语义，通过OBSFileSystem封装，相较对象语义增加Rename、Append、hflush/hsync接口，实现完善的HDFS语义，为大数据计算提供了更好的性能。

基于上述优势，华为云存算分离大数据方案相比传统大数据方案，在同样的业务规模下所使用的计算资源、存储资源以及服务器数量都会有明显下降，同时资源利用率也能得到显著提升，可帮助企业降低业务综合成本。

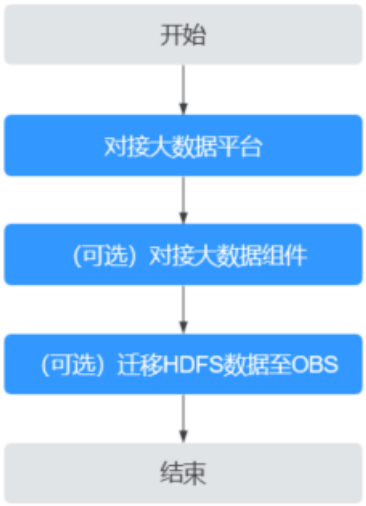
文档使用范围

本最佳实践主要提供华为云大数据存算分离方案中不同大数据平台和大数据组件与对象存储服务OBS的对接指导，以及HDFS数据迁移至对象存储服务OBS的方案。

9.2 操作流程

大数据场景下使用OBS实现存算分离的操作流程如图9-3所示。

图 9-3 操作流程



1. 配置的核心是完成大数据平台与OBS对接，实现OBS作为大数据的统一数据湖存储。本文档提供三种主流大数据平台的对接指导，详情请参见**支持的大数据平台简介**。
2. （可选）OBS除了可以与主流大数据平台对接外，还可以直接与开源的大数据组件对接。当您使用开源的大数据组件时，可参考**支持的大数据组件简介**完成与OBS对接。
3. （可选）如果您的数据仍存储在本地HDFS，需要先将数据迁移到华为云OBS中。详情请参见**迁移HDFS数据至OBS**。

9.3 对接大数据平台

9.3.1 支持的大数据平台简介

华为云大数据存算分离方案中，OBS支持与多种大数据平台对接，包括华为云MapReduce服务（MRS）、Cloudera CDH和Hortonworks HDP，满足用户业务的灵活诉求。

华为云 MapReduce 服务（MRS）

华为云MapReduce服务（MRS）是华为云提供的大数据服务，可以在华为云上部署和管理Hadoop系统，一键即可部署Hadoop集群。

MRS提供用户完全可控的一站式企业级大数据集群云服务，完全兼容开源接口，结合华为云计算、存储优势及大数据行业经验，为客户提供高性能、低成本、灵活易用的全栈大数据平台，轻松运行Hadoop、Spark、HBase、Kafka、Storm等大数据组件，并具备在后续根据业务需要进行定制开发的能力，帮助企业快速构建海量数据信息处

理系统，并通过对海量信息数据实时与非实时的分析挖掘，发现全新价值点和企业商机。

MRS与OBS对接的具体操作，请参见**华为云MRS对接OBS**。

Cloudera CDH

CDH是Cloudera基于Apache Hadoop生态系统构建的大数据分析管理平台发行版。

Cloudera CDH与OBS对接的具体操作，请参见**Cloudera CDH对接OBS**。

Hortonworks HDP

HDP是Hortonworks基于Apache Hadoop生态系统开源组件构建的大数据分析管理平台。

Hortonworks HDP与OBS对接的具体操作，请参见**Hortonworks HDP对接OBS**

9.3.2 华为云 MRS 对接 OBS

对接步骤

步骤1 配置存算分离集群。

详细操作，请参见**使用委托方式配置存算分离集群**。

步骤2 使用存算分离集群。

详细操作，请参见**使用存算分离集群**。

----结束

9.3.3 Cloudera CDH 对接 OBS

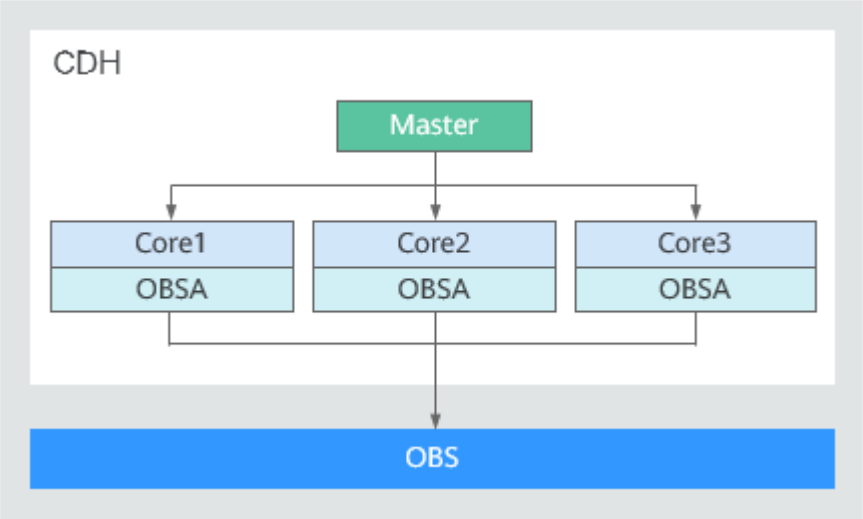
部署视图

安装版本

硬件：1Master+3Core（配置：8U32G，操作系统：CentOS 7.5）

软件：CDH 6.0.1

部署视图



更新 OBSA-HDFS 工具

步骤1 下载与hadoop版本配套的OBSA-HDFS工具：**下载地址**。

并将OBSA-HDFS工具jar包（如hadoop-huaweicloud-3.1.1-hw-53.8.jar）上传到CDH各节点/opt/obsa-hdfs目录中。

说明

- hadoop-huaweicloud-x.x.x-hw-y.jar包含义：前三位x.x.x为配套hadoop版本号；最后一位y为OBSA版本号，y值最大为最新版本。如：hadoop-huaweicloud-3.1.1-hw-53.8.jar，3.1.1是配套hadoop版本号，53.8是OBSA的版本号。
- 如hadoop版本为3.1.x，则选择hadoop-huaweicloud-3.1.1-hw-53.8.jar。

步骤2 增加hadoop-huaweicloud的jar包。

在CDH集群各节点执行以下命令，命令请根据hadoop-huaweicloud的jar包名字及实际CDH版本进行适配使用。

1. 执行如下命令，将OBSA-HDFS工具的jar包放到/opt/cloudera/parcels/CDH-6.0.1-1.cdh6.0.1.p0.590678/jars/目录中。

   cp /opt/obsa-hdfs/hadoop-huaweicloud-3.1.1-hw-53.8.jar /opt/cloudera/parcels/CDH-6.0.1-1.cdh6.0.1.p0.590678/jars/

2. 执行如下命令，建立各目录的软连接，将hadoop-huaweicloud的jar包放入如下目录。

   ln -s /opt/cloudera/parcels/CDH-6.0.1-1.cdh6.0.1.p0.590678/jars/hadoop-huaweicloud-3.1.1-hw-53.8.jar /opt/cloudera/parcels/CDH-6.0.1-1.cdh6.0.1.p0.590678/jars/hadoop-huaweicloud.jar

   ln -s /opt/cloudera/parcels/CDH-6.0.1-1.cdh6.0.1.p0.590678/jars/hadoop-huaweicloud.jar /opt/cloudera/cm/cloudera-navigator-server/libs/cdh6/hadoop-huaweicloud.jar

   ln -s /opt/cloudera/parcels/CDH-6.0.1-1.cdh6.0.1.p0.590678/jars/hadoop-huaweicloud.jar /opt/cloudera/cm/common_jars/hadoop-huaweicloud.jar

   ln -s /opt/cloudera/parcels/CDH-6.0.1-1.cdh6.0.1.p0.590678/jars/hadoop-huaweicloud.jar /opt/cloudera/cm/lib/cdh6/hadoop-huaweicloud.jar

ln -s /opt/cloudera/parcels/CDH-6.0.1-1.cdh6.0.1.p0.590678/jars/hadoop-huaweicloud.jar /opt/cloudera/cm/cloudera-scm-telepub/libs/cdh6/hadoop-huaweicloud.jar

ln -s /opt/cloudera/parcels/CDH-6.0.1-1.cdh6.0.1.p0.590678/jars/hadoop-huaweicloud.jar /opt/cloudera/parcels/CDH-6.0.1-1.cdh6.0.1.p0.590678/lib/hadoop/hadoop-huaweicloud.jar

ln -s /opt/cloudera/parcels/CDH-6.0.1-1.cdh6.0.1.p0.590678/jars/hadoop-huaweicloud.jar /opt/cloudera/parcels/CDH-6.0.1-1.cdh6.0.1.p0.590678/lib/hadoop/client/hadoop-huaweicloud.jar

ln -s /opt/cloudera/parcels/CDH-6.0.1-1.cdh6.0.1.p0.590678/jars/hadoop-huaweicloud.jar /opt/cloudera/parcels/CDH-6.0.1-1.cdh6.0.1.p0.590678/lib/spark/jars/hadoop-huaweicloud.jar

ln -s /opt/cloudera/parcels/CDH-6.0.1-1.cdh6.0.1.p0.590678/jars/hadoop-huaweicloud.jar /opt/cloudera/parcels/CDH-6.0.1-1.cdh6.0.1.p0.590678/lib/impala/lib/hadoop-huaweicloud.jar

ln -s /opt/cloudera/parcels/CDH-6.0.1-1.cdh6.0.1.p0.590678/jars/hadoop-huaweicloud.jar /opt/cloudera/parcels/CDH-6.0.1-1.cdh6.0.1.p0.590678/lib/hadoop-mapreduce/hadoop-huaweicloud.jar

ln -s /opt/cloudera/parcels/CDH-6.0.1-1.cdh6.0.1.p0.590678/jars/hadoop-huaweicloud.jar /opt/cloudera/cm/lib/cdh5/hadoop-huaweicloud.jar

ln -s /opt/cloudera/parcels/CDH-6.0.1-1.cdh6.0.1.p0.590678/jars/hadoop-huaweicloud.jar /opt/cloudera/cm/cloudera-scm-telepub/libs/cdh5/hadoop-huaweicloud.jar

ln -s /opt/cloudera/parcels/CDH-6.0.1-1.cdh6.0.1.p0.590678/jars/hadoop-huaweicloud.jar /opt/cloudera/cm/cloudera-navigator-server/libs/cdh5/hadoop-huaweicloud.jar

----结束

HDFS 和 Yarn 集群对接 OBS 配置项

步骤1 在HDFS集群配置中选择“高级”，在core-site.xml的群集范围高级配置代码段（安全阀）增加OBS的ak、sk、endpoint和impl配置，对应名称为fs.obs.access.key、fs.obs.secret.key、fs.obs.endpoint、fs.obs.impl。

说明

1. 访问密钥AK/SK和终端节点Endpoint请根据实际填写，AK/SK获取方式请参见**访问密钥（AK/SK）**，Endpoint获取方式请参见**终端节点（Endpoint）和访问域名**。
2. fs.obs.impl配置为org.apache.hadoop.fs.obs.OBSFileSystem。

步骤2 修改后“重启”或“滚动重启”HDFS集群，再重启“部署客户端配置”。

步骤3 进入YARN集群，重启“部署客户端配置”。

步骤4 查看节点中/etc/hadoop/conf/core-site.xml中是否已增加OBS的ak、sk、endpoint和impl配置。

```
<property>
<name>fs.obs.access.key</name>
<value> *****</value>
</property>
<property>
```



```
<name>fs.obs.secret.key</name>
<value>**********</value>
</property>
<property>
<name>fs.obs.endpoint</name>
<value>{Target Endpoint}</value>
</property>
<property>
<name>fs.obs.impl</name>
<value>org.apache.hadoop.fs.obs.OBSFileSystem</value>
</property>
```

----结束

Spark 集群对接 OBS 配置项

步骤1 Spark应用对接OBS，需要在YARN集群中进行core-site.xml配置，包括：ak、sk、endpoint、impl等。

步骤2 core-site.xml配置完成后“重启”YARN集群，再重启Spark集群的“部署客户端配置”。

----结束

Hive 集群对接 OBS 配置项

步骤1 Hive应用对接OBS，需要在Hive集群中进行core-site.xml配置，包括：ak、sk、endpoint、impl等。

步骤2 core-site.xml配置完成后“重启”Hive集群，再重启Hive集群的“部署客户端配置”。

----结束

9.3.4 Hortonworks HDP 对接 OBS

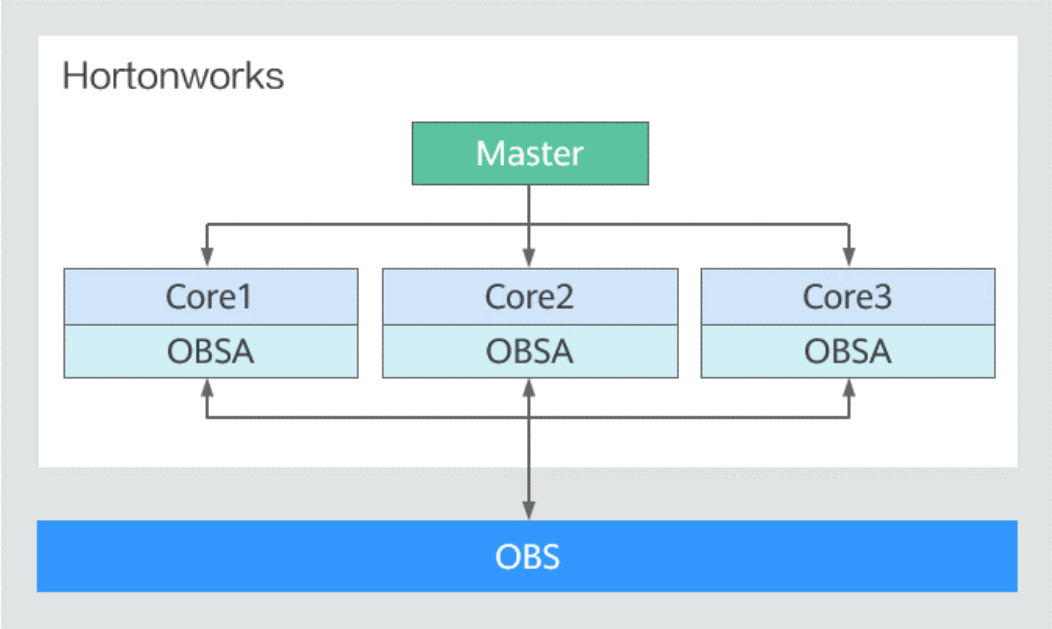
部署视图

安装版本

硬件：1master+3core（配置：8U32G，操作系统：CentOS 7.5）

软件：Ambari：2.7.1.0，HDP：3.0.1.0

部署视图



更新 OBSA-HDFS 工具

步骤1 下载与hadoop版本配套的OBSA-HDFS工具：**下载地址**。

下载OBSA-HDFS工具的jar包（如hadoop-huaweicloud-3.1.1-hw-53.8.jar）到/mnt/obsjar目录。

说明

- hadoop-huaweicloud-x.x.x-hw-y.jar包含义：前三位x.x.x为配套hadoop版本号；最后一位y为OBSA版本号，y值最大为最新版本。如：hadoop-huaweicloud-3.1.1-hw-53.8.jar，3.1.1是配套hadoop版本号，53.8是OBSA的版本号。
- 如hadoop版本为3.1.x，则选择hadoop-huaweicloud-3.1.1-hw-53.8.jar。

步骤2 执行以下命令，将OBSA-HDFS工具jar包（如hadoop-huaweicloud-3.1.1-hw-53.8.jar）拷贝到如下目录中。

cp /mnt/obsjar/hadoop-huaweicloud-3.1.1-hw-53.8.jar /usr/hdp/share/hst/activity-explorer/lib/

cp /mnt/obsjar/hadoop-huaweicloud-3.1.1-hw-53.8.jar /usr/hdp/3.0.1.0-187/hadoop-mapreduce/

cp /mnt/obsjar/hadoop-huaweicloud-3.1.1-hw-53.8.jar /usr/hdp/3.0.1.0-187/spark2/jars/

cp /mnt/obsjar/hadoop-huaweicloud-3.1.1-hw-53.8.jar /usr/hdp/3.0.1.0-187/tez/lib/

cp /mnt/obsjar/hadoop-huaweicloud-3.1.1-hw-53.8.jar /var/lib/ambari-server/resources/views/work/CAPACITY-SCHEDULER{1.0.0}/WEB-INF/lib/

cp /mnt/obsjar/hadoop-huaweicloud-3.1.1-hw-53.8.jar /var/lib/ambari-server/resources/views/work/FILES{1.0.0}/WEB-INF/lib/

cp /mnt/obsjar/hadoop-huaweicloud-3.1.1-hw-53.8.jar /var/lib/ambari-server/resources/views/work/WORKFLOW_MANAGER{1.0.0}/WEB-INF/lib/

ln -s /usr/hdp/3.0.1.0-187/hadoop-mapreduce/hadoop-huaweicloud-3.1.1-hw-53.8.jar /usr/hdp/3.0.1.0-187/hadoop-mapreduce/hadoop-huaweicloud.jar

----结束

在 HDFS 集群中增加配置项

步骤1 在HDFS集群CONFIGS的ADVANCED配置项中增加Custom core-site.xml文件中的配置项，包括：fs.obs.access.key，fs.obs.secret.key，fs.obs.endpoint和fs.obs.impl。

说明

1. fs.obs.access.key、fs.obs.secret.key、fs.obs.endpoint分别为用户的ak、sk和endpoint。访问密钥AK/SK和终端节点Endpoint请根据实际填写，AK/SK获取方式请参见**访问密钥（AK/SK）**，Endpoint获取方式请参见**终端节点（Endpoint）和访问域名**。
2. fs.obs.impl配置为org.apache.hadoop.fs.obs.OBSFileSystem。

步骤2 重启HDFS集群。

----结束

在 MapReduce2 集群中增加配置项

步骤1 在MapReduce2集群CONFIGS的ADVANCED配置项中修改mapred-site.xml文件中的mapreduce.application.classpath配置项，添加路径为/usr/hdp/3.0.1.0-187/hadoop-mapreduce/*。

步骤2 重启MapReduce2集群。

----结束

增加 Hive 对接 OBS 的 jar 包

步骤1 执行以下命令，在Hive Server节点创建auxlib文件夹。

mkdir /usr/hdp/3.0.1.0-187/hive/auxlib

步骤2 执行以下命令，将OBSA-HDFS工具的jar包放到auxlib文件夹。

cp /mnt/obsjar/hadoop-huaweicloud-3.1.1-hw-53.8.jar /usr/hdp/3.0.1.0-187/hive/auxlib

步骤3 重启Hive集群。

----结束

9.4 对接大数据组件

9.4.1 支持的大数据组件简介

在华为云大数据存算分离方案中，OBS除了可以与大数据平台对接外，还可以直接与开源的大数据组件对接。

当前支持的大数据组件如下：

- **Hadoop**
- **Hive**
- **Spark**
- **Flume**
- **DataX**
- **Druid**
- **Flink**
- **logstash**

9.4.2 Hadoop 对接 OBS

概述

Hadoop系统提供了分布式存储、计算和资源调度引擎，用于大规模数据处理和分析。OBS服务实现了Hadoop的HDFS协议，在大数据场景中可以替代Hadoop系统中的HDFS服务，实现Spark、MapReduce、Hive等大数据生态与OBS服务的对接，为大数据计算提供“数据湖”存储。

说明

HDFS协议：Hadoop中定义了HDFS协议（通过FileSystem抽象类），其他各类存储系统均可以实现HDFS协议，例如Hadoop中内置的HDFS服务，华为云的对象存储服务OBS。

约束与限制

不支持以下HDFS语义：

- Lease
- Symbolic link operations
- Proxy users
- File concat
- File checksum
- File replication factor
- Extended Attributes(XAttrs) operations
- Snapshot operations
- Storage policy
- Quota
- POSIX ACL
- Delegation token operations

注意事项

为了减少日志输出，在/opt/hadoop-3.1.1/etc/hadoop/log4j.properties文件中增加配置：

```
log4j.logger.com.obs=ERROR
```


对接步骤

以Hadoop 3.1.1为例（建议使用最新的版本，不推荐使用低于2.8.3版本的hadoop与hadoop-huaweicloud配套使用）。

步骤1 下载hadoop-3.1.1.tar.gz，并解压到/opt/hadoop-3.1.1目录。

步骤2 在/etc/profile文件中增加配置内容：

```
export HADOOP_HOME=/opt/hadoop-3.1.1
export PATH=$HADOOP_HOME/bin:$HADOOP_HOME/sbin:$PATH
```

步骤3 安装hadoop-huaweicloud。

1. 在官方Github下载hadoop-huaweicloud：**下载地址**。

   说明

   如果没有匹配版本的jar包，可自行修改hadoop-huaweicloud目录下pom文件中的hadoop版本重新编译生成。

2. 将hadoop-huaweicloud-x.x.x-hw-y.jar拷贝到/opt/hadoop-3.1.1/share/hadoop/tools/lib和/opt/hadoop-3.1.1/share/hadoop/common/lib目录下。

   说明

   hadoop-huaweicloud-x.x.x-hw-y.jar包含义：前三位x.x.x为配套hadoop版本号；最后一位y为OBSA版本号，y值最大为最新版本。如：hadoop-huaweicloud-3.1.1-hw-40.jar，3.1.1是配套hadoop版本号，40是OBSA的版本号。

步骤4 配置hadoop。

修改 /opt/hadoop-3.1.1/etc/hadoop/core-site.xml，增加OBS相关配置信息：

```
<property>
<name>fs.obs.impl</name>
<value>org.apache.hadoop.fs.obs.OBSFileSystem</value>
</property>
<property>
<name>fs.AbstractFileSystem.obs.impl</name>
<value>org.apache.hadoop.fs.obs.OBS</value>
</property>
<property>
<name>fs.obs.access.key</name>
<value>xxx</value>
<description>HuaweiCloud Access Key Id</description>
</property>
<property>
<name>fs.obs.secret.key</name>
<value>xxx</value>
<description>HuaweiCloud Secret Access Key</description>
</property>
<property>
<name>fs.obs.endpoint</name>
<value>xxx</value>
<description>HuaweiCloud Endpoint</description>
</property>
```

步骤5 验证是否对接成功。

您可以通过命令行和MR程序两种方式进行验证。示例如下：

- 命令行

  hadoop fs -ls obs://obs-bucket/

  回显如下信息：


```
-rw-rw-rw- 1 root root 1087 2018-06-11 07:49 obs://obs-bucket/test1
-rw-rw-rw- 1 root root 1087 2018-06-11 07:49 obs://obs-bucket/test2
```

- MR程序

  hadoop jar share/hadoop/mapreduce/hadoop-mapreduce-examples-3.1.1.jar wordcount obs://example-bucket/input/test.txt obs://obs-bucket/output

----结束

【附】hadoop-huaweicloud 相关配置

配置项	默认值	是否必填	说明
fs.obs.impl	org.apache.hadoop.fs.obs.OBSFileSystem	是	-
fs.AbstractFileSystem.obs.impl	org.apache.hadoop.fs.obs.OBS	是	-
fs.obs.endpoint	无	是	华为云OBS的终端节点（Endpoint）。
fs.obs.access.key	无	是	华为云的AK（Access Key Id），需要具备访问OBS对应桶的权限。
fs.obs.secret.key	无	是	华为云的SK（Secret Access Key），需要具备访问OBS对应桶的权限。
fs.obs.session.token	无	否	华为云的securitytoken，需要具备访问OBS对应桶的权限。当使用临时AK/SK时需要。
fs.obs.security.provider	无	否	实现com.obs.services.IObsCredentialsProvider接口的类，用于获取访问OBS的凭证。
fs.obs.connection.ssl.enabled	FALSE	否	是否通过HTTPS访问OBS。
fs.obs.threads.keepalivetime	60	否	控制读写线程池参数keepAliveTime。
fs.obs.threads.max	20	否	控制读写线程池参数corePoolSize和maximumPoolSize
fs.obs.max.total.tasks	20	否	控制读写线程池参数BlockingQueue的容量，其等于fs.obs.threads.max +fs.obs.max.total.tasks

配置项	默认值	是否必填	说明
fs.obs.multipart.size	104857600	否	写相关配置，多段上传大小。
fs.obs.fast.upload.buffer	disk	否	写相关配置，所有数据在写入OBS前都会先缓存然后再上传到OBS，此参数用于设置缓存方式，取值范围： ● disk：缓存在磁盘 ● array：缓存在JVM堆内内存 ● bytebuffer：缓存在JVM堆外内存
fs.obs.buffer.dir	${hadoop.tmp.dir}	否	写相关配置，当fs.obs.fast.upload.buffer为disk时的缓存目录，支持多目录并以逗号分隔。
fs.obs.bufferdir.verify.enable	FALSE	否	写相关配置，当fs.obs.fast.upload.buffer为disk时是否验证缓存目录是否存在以及是否具备写权限。
fs.obs.fast.upload.active.blocks	4	否	写相关配置，每个流操作最大可以使用的缓存个数（通过多段上传线程池最多可以提交的线程任务个数），从而限制每个流操作最大可以使用的缓存空间fs.obs.fast.upload.active.blocks*fs.obs.multipart.size。
fs.obs.fast.upload.array.first.buffer	1048576	否	写相关配置，当fs.obs.fast.upload.buffer为array时，此参数控制JVM堆内缓存初始化大小
fs.obs.readahead.range	1048576	否	写相关配置，预读片段大小。
fs.obs.multiobject.delete.enable	TRUE	否	删除相关配置，删除目录时是否启动批量删除。
fs.obs.delete.threads.max	20	否	删除相关配置，控制线程池参数maximumPoolSize和corePoolSize
fs.obs.multiobject.delete.maximum	1000	否	删除相关配置，批量删除时单次OBS批量删除请求中支持的最多可删除对象的个数，最大值为1000。
fs.obs.multiobject.delete.threshold	3	否	删除相关配置，批量删除时当对象个数小于此参数值时将不启动批量删除。

配置项	默认值	是否必填	说明
fs.obs.list.threads.core	30	否	List相关配置，控制线程池参数corePoolSize
fs.obs.list.threads.max	60	否	List相关配置，控制线程池参数maximumPoolSize
fs.obs.list.workqueue.capacity	1024	否	List相关配置，控制线程池参数BlockingQueue的容量
fs.obs.list.parallel.factor	30	否	List相关配置，控制并发因子参数。
fs.obs.paging.maximum	1000	否	List相关配置，单次OBS List请求最多返回的对象个数，最大值为1000。
fs.obs.copy.threads.max	40	否	对象桶rename相关配置，对象桶rename目录时copy线程池配置参数maximumPoolSize，corePoolSize的值为此参数的一半，BlockingQueue的容量为1024。
fs.obs.copypart.size	104857600	否	对象桶rename相关配置，单个对象copy时当对象的大小超过了此参数值则进行多段copy，且段大小为此参数值；否则进行简单copy。
fs.obs.copypart.threads.max	5368709120	否	对象桶rename相关配置，单个对象copy时如果进行了多段copy，多段copy线程池配置参数maximumPoolSize，corePoolSize的值为此参数的一半，BlockingQueue的容量为1024。
fs.obs.getcanonicalservicename.enable	FALSE	否	控制getCanonicalServiceName()接口的返回值。 ● TRUE：obs://bucketname ● FALSE：null
fs.obs.multipart.purge	FALSE	否	初始化OBSFilesystem时是否清理桶内的多段上传任务。
fs.obs.multipart.purge.age	86400	否	初始化OBSFilesystem时清理桶内多久之前的多段上传任务。
fs.obs.trash.enable	FALSE	否	是否开启垃圾回收功能。
fs.obs.trash.dir	无	否	垃圾回收目录。
fs.obs.block.size	134217728	否	块大小。

9.4.3 Hive 对接 OBS

概述

Hive是一个数据仓库工具，可以对存储在分布式存储中的大规模数据进行数据提取、转化和加载，它提供了丰富的SQL查询方式来进行数据分析。

前提条件

已安装Hadoop，具体请参见**Hadoop对接OBS**。

对接步骤

以Hive 2.3.3为例。

步骤1 下载apache-hive-2.3.3-bin.tar.gz，并解压到/opt/hive-2.3.3。

步骤2 在/etc/profile文件中增加配置内容：

```
export HIVE_HOME=/opt/hive-2.3.3
export PATH=$HIVE_HOME/bin:$PATH
```

步骤3 配置Hive。

1. 重命名/opt/hive-2.3.3/conf/hive-env.sh.template为hive-env.sh。
2. 重命名opt/hive-2.3.3/conf/hive-log4j2.properties.template为hive-log4j2.properties。
3. 创建hive-site.xml文件，添加配置：

   ```
   <property>
   <name>hive.metastore.warehouse.dir</name>
   <value>obs://obs-bucket/warehouse/hive</value>
   </property>
   ```

   说明

   可选配置，当添加了上述配置后在创建Hive表时将不用再显示指定location，创建的Hive表将自动落在OBS上。

4. 执行以下命令，初始化元数据。

   /opt/hive-2.3.3/bin/schematool -dbType derby -initSchema

步骤4 验证是否对接成功。

示例如下，示例中的location为obs://obs-bucket/warehouse/hive/student。

```
hive>
create table student(id int comment "学生id",name string comment "学生姓名",age int comment "学生年龄
")
comment "学生信息表"
row format delimited fields terminated by ",";

insert into table student select 6,"yangdong",29;
```

----结束

9.4.4 Spark 对接 OBS

概述

Apache Spark是专为大规模数据处理而设计的快速通用的计算引擎。

前提条件

已安装Hadoop，具体请参见**Hadoop对接OBS**。

注意事项

为了减少日志输出，在/opt/spark-2.3.3/conf/log4j.properties文件中增加配置：

```
log4j.logger.com.obs= ERROR
```

对接步骤

以Spark2.3.3为例。

步骤1 下载spark-2.3.3-bin-without-hadoop.tgz，并解压到/opt/spark-2.3.3。

步骤2 在/etc/profile文件中增加配置内容：

```
export SPARK_HOME=/opt/spark-2.3.3
export PATH=$SPARK_HOME/bin:$SPARK_HOME/sbin:$PATH
```

步骤3 配置spark。

1. 重命名/opt/spark-2.3.3/conf/spark-env.sh.template为spark-env.sh并增加配置：
   ```
   export SPARK_DIST_CLASSPATH=$(hadoop classpath)
   ```
   更多配置内容请参见**Apache Hadoop**。
2. 重命名/opt/spark-2.3.3/conf/log4j.properties.template为log4j.properties。

步骤4 执行以下命令，验证是否对接成功。

$SPARK_HOME/bin/run-example org.apache.spark.examples.JavaWordCount obs://obs-bucket/input/test.txt

----结束

9.4.5 Presto 对接 OBS

概述

Presto分为prestoSql（现更名为Trino）和PrestoDB两大分支或是发行版。

Presto on OBS仅支持prestoSql/Trino发行版，下述对接步骤以prestoSql-333版本为例（从prestoSql-332版本开始Presto服务端必须使用JDK 11）。

说明

本章节中的Presto指prestoSql/Trino发行版。

前提条件

- 已安装Hadoop，具体请参见**Hadoop对接OBS**。
- 已安装Hive，具体请参见**Hive对接OBS**。

安装 presto server

版本：prestoSQL-333

步骤1 下载Presto客户端和服务端。

下载客户端

下载服务端

步骤2 下载hadoop-huaweicloud插件：**下载地址**。

步骤3 执行以下命令，解压Presto服务端。

tar –zxvf presto-server-333.tar.gz

在presto根目录/plugin/hive-hadoop2下放入如下两个jar包。

- **hadoop-huaweicloud-${hadoop.version}-hw-${version}.jar**
- Apache commons-lang-xxx.jar
  可从maven中央仓库下载或从hadoop目录中拷贝。

----结束

配置 presto

在安装目录里创建etc目录。这目录会有以下配置（自己创建）：

- 节点配置文件：每个节点的环境配置
- JVM配置文件：Java虚拟机的命令行选项
- Server配置文件（Config Properties）：Presto server的配置
- Catalog配置文件：配置presto的各种Connector（数据源）
- 日志配置文件：配置presto日志

节点配置文件

节点属性文件etc/node.properties，包含每个节点的配置。一个节点是一个Presto实例。这文件一般是在Presto第一次安装时创建的。以下是最小配置：

```
node.environment=production
node.id=ffffffff-ffff-ffff-ffff-ffffffffffff
node.data-dir=/var/presto/data
```

解释：

node.environment：环境名字，Presto集群中的节点的环境名字都必须是一样的。

node.id：唯一标识，每个节点的标识都必须是唯一的。就算重启或升级Presto都必须还保持原来的标识。

node.data-dir：数据目录，Presto用它来保存log和其他数据

示例：

node.environment=presto_cluster

node.id=bigdata00

node.data-dir=/home/modules/presto-server-0.215/data #data需要自己手动创建

JVM 配置文件

JVM配置文件etc/jvm.config，包含启动Java虚拟机时的命令行选项。格式是每一行是一个命令行选项。此文件数据是由shell解析，所以选项中包含空格或特殊字符会被忽略。

以下是参考配置：

```
-server
-Xmx16G
-XX:-UseBiasedLocking
-XX:+UseG1GC
-XX:G1HeapRegionSize=32M
-XX:+ExplicitGCInvokesConcurrent
-XX:+ExitOnOutOfMemoryError
-XX:+UseGCOverheadLimit
-XX:+HeapDumpOnOutOfMemoryError
-XX:ReservedCodeCacheSize=512M
-Djdk.attach.allowAttachSelf=true
-Djdk.nio.maxCachedBufferSize=2000000
```

备注：以上参数都是官网参数，实际环境需要调整

Server 配置文件

配置属性文件etc/config.properties，包含Presto server的配置。Presto server可以同时为coordinator和worker，但一个大集群里最好就是只指定一台机器为coordinator。

1. coordinator节点的配置文件

```
coordinator=true
node-scheduler.include-coordinator=true
http-server.http.port=5050
discovery-server.enabled=true
discovery.uri=http://192.168.XX.XX:5050
query.max-memory=20GB
query.max-memory-per-node=1GB
query.max-total-memory-per-node=2GB
```

2. worker节点的配置文件

```
coordinator=false
http-server.http.port=5050
discovery.uri=http://192.168.XX.XX:5050
query.max-memory=20GB
query.max-memory-per-node=1GB
query.max-total-memory-per-node=2GB
```

解释：

coordinator：是否运行该实例为coordinator（接受client的查询和管理查询执行）。

node-scheduler.include-coordinator:coordinator是否也作为work。对于大型集群来说，在coordinator里做worker的工作会影响查询性能。

http-server.http.port:指定HTTP端口。Presto使用HTTP来与外部和内部进行交流。

query.max-memory：查询能用到的最大总内存。

query.max-memory-per-node：查询能用到的最大单节点内存。

discovery-server.enabled：Presto使用Discovery服务去找到集群中的所有节点。每个Presto实例在启动时都会在Discovery服务里注册。这样可以简化部署，不需要额外的服务，Presto的coordinator内置一个Discovery服务。

discovery.uri：Discovery服务的URI。将example.net:8080替换为coordinator的host和端口。这个URI不能以斜杠结尾，这个错误需特别注意，不然会报404错误。

另外还有以下属性：

jmx.rmiregistry.port：指定JMX RMI的注册。JMX client可以连接此端口

jmx.rmiserver.port：指定JMX RMI的服务器。可通过JMX监听。

Catalog 配置文件（重点）

hive connector配置如下:

1. 在etc目录下创建catalog目录
2. 创建一个hive connector的配置文件：hive.properties

```
# hive.properties
#连接名
connector.name=hive-hadoop2
#配置hive metastore连接
hive.metastore.uri=thrift://192.168.XX.XX:9083
#指定hadoop的配置文件，注意core-site.xml需要按照https://github.com/huaweicloud/obsa-hdfs/tree/master/release/doc配置
hive.config.resources=/home/modules/hadoop-2.8.3/etc/hadoop/core-site.xml,/home/modules/hadoop-2.8.3/etc/hadoop/hdfs-site.xml,/home/modules/hadoop-2.8.3/etc/hadoop/mapred-site.xml
#给删表权限
hive.allow-drop-table=true
```

日志配置文件

创建文件log.properties

写入内容：com.facebook.presto=INFO

备注：日志级别有四种：DEBUG、INFO、WARN和ERROR。

启动 presto

步骤如下：

步骤1 启动hive metastore：hive --service metastore &

步骤2 启动presto server：bin/launcher start (如何关闭presto服务：bin/launcher stop)

步骤3 启动presto client：

1. 重命名presto-cli-333-executable.jar为presto,放在bin目录下，然后赋予执行权限：chmod +x presto
2. 启动client：./presto --server XX.XX.XX.XX:5050 --catalog hive --schema default

----结束

Presto 查询 OBS

创建hive表

```
hive>
CREATE TABLE sample01(id int,name string,address string)
ROW FORMAT DELIMITED
FIELDS TERMINATED BY ','
STORED AS TEXTFILE
```



```
LOCATION 'obs://obs-east-bkt001/sample01';

insert into sample01 values(1,'xiaoming','cd');
insert into sample01 values(2,'daming','sh');
```

presto查询hive表

./presto --server XX.XX.XX.XX:5050 --catalog hive --schema default

```
presto:default>
select * from sample01;
```

9.4.6 Flume 对接 OBS

概述

Flume是一个分布式的、可靠的和高可用的服务，用于收集、聚合以及移动大量日志数据，具体请参见**Apache Flume**。OBS在大数据场景中可以替代Hadoop系统中的HDFS服务。

注意事项

- 多sink写同一文件

  OBS和HDFS在一致性保证上是有差别的：HDFS租约机制可以保证并发写同一个文件时不会产生一致性问题，但是OBS实现的HDFS协议不支持租约Lease机制（并发写同一个文件时将产生不可确定的状态），所以在flume场景下可以通过文件命名规则进行解决。

  如sink文件的命名规则：hostname-sinkname作为文件的前缀，如果一个主机上部署了多个flume agent，不同的agent要有不同的sinkname。

- flume日志配置

  为了减少日志输出，在/opt/apache-flume-1.9.0-bin/conf/log4j.properties文件中增加配置：

  ```
  log4j.logger.com.obs=ERROR
  ```

- obsa写入时临时文件的目录配置

  Flume写OBS时会先写入本地磁盘缓冲区，然后上传到OBS，如果对写入OBS有极致性能要求请选择高性能磁盘作为缓冲区，在core-site.xml文件中增加配置：

  ```
  <property>
  <name>fs.obs.buffer.dir</name>
  <value>xxx</value>
  </property>
  ```

对接步骤

以flume 1.9版本为例。

步骤1 下载apache-flume-1.9.0-bin.tar.gz。

步骤2 安装flume。

解压apache-flume-1.9.0-bin.tar.gz到/opt/apache-flume-1.9.0-bin目录。

- 已部署Hadoop的环境：无需额外操作，部署Hadoop请参见**Hadoop对接OBS**。
- 未部署Hadoop的环境：
  a. 将hadoop中的相关jar包复制到/opt/apache-flume-1.9.0-bin/lib目录下，包含hadoop-huaweicloud-xxx.jar。

b. 将添加了OBS相关配置的core-site.xml文件复制到/opt/apache-flume-1.9.0-bin/conf目录下。

步骤3 验证是否对接成功。

示例：以flume内置的StressSource为source，以file为channel，以obs为sink。

1. 创建flume配置文件：sink2obs.properties。

```
agent.sources = r1
agent.channels = c1
agent.sinks = k1

agent.sources.r1.type = org.apache.flume.source.StressSource
agent.sources.r1.channels = c1
agent.sources.r1.size = 1024
agent.sources.r1.maxTotalEvents = 100000
agent.sources.r1.maxEventsPerSecond = 10000
agent.sources.r1.batchSize=1000

agent.sources.r1.interceptors = i1
agent.sources.r1.interceptors.i1.type = host
agent.sources.r1.interceptors.i1.useIP = false

agent.channels.c1.type = file
agent.channels.c1.dataDirs = /data/agent/flume-data
agent.channels.c1.checkpointDir = /data/agent/flume-checkpoint
agent.channels.c1.capacity = 500000
agent.channels.c1.transactionCapacity = 50000

agent.sinks.k1.channel = c1
agent.sinks.k1.type = hdfs
agent.sinks.k1.hdfs.useLocalTimeStamp = true
agent.sinks.k1.hdfs.filePrefix = %{host}_k1
agent.sinks.k1.hdfs.path = obs://obs-bucket/flume/create_time=%Y-%m-%d-%H-%M
agent.sinks.k1.hdfs.fileType = DataStream
agent.sinks.k1.hdfs.writeFormat = Text
agent.sinks.k1.hdfs.rollSize = 0
agent.sinks.k1.hdfs.rollCount = 1000
agent.sinks.k1.hdfs.rollInterval = 0
agent.sinks.k1.hdfs.batchSize = 1000
agent.sinks.k1.hdfs.round = true
agent.sinks.k1.hdfs.roundValue = 10
agent.sinks.k1.hdfs.roundUnit = minute
```

2. 执行以下命令，启动flume agent。

   ./bin/flume-ng agent -n agent -c conf/ -f conf/sink2obs.properties

----结束

9.4.7 DataX 对接 OBS

概述

DataX是一个数据同步框架，实现了包括MySQL、SQL Server、Oracle、PostgreSQL、HDFS、Hive、HBase、OTS、ODPS等各种异构数据源之间高效的数据同步功能。OBS在大数据场景中可以替代Hadoop系统中的HDFS服务，本文介绍DataX如何对接OBS。

对接步骤

步骤1 下载datax源码，以发布版本datax_v202308为例：**下载地址**。

步骤2 修改编译datax。

1. 升级hdfsreader和hdfswriter模块依赖的hadoop版本，以升级到2.8.3版本为例。
   修改datax\hdfswriter\pom.xml和datax\hdfsreader\pom.xml文件配置：

   ```
   <properties>
   <!--由2.7.1升级到2.8.3-->
   <hadoop.version>2.8.3</hadoop.version>
   </properties>
   ```

2. 编译datax。
3. 执行以下命令，在datax源码根目录/target目录下生成datax.tar.gz压缩文件。
   mvn -U clean package assembly:assembly -Dmaven.test.skip=true

步骤3 安装datax。

1. 解压datax.tar.gz到/opt/datax目录。
2. 在Github下载hadoop-huaweicloud：**下载地址**。（建议使用hadoop 2.8.3版本下最新版本的hadoop-huaweicloud版本，例如hadoop-huaweicloud-2.8.3-hw-53.8，以最新版本为准）
3. 将上述下载的jar包放入/opt/datax/plugin/writer/hdfswriter/libs和/opt/datax/plugin/reader/hdfsreader/libs。

步骤4 验证是否对接成功。

示例：以txtfilereader为源端，以OBS为目的端。

1. 创建作业配置文件file2obs.json。

```
{
   "setting":{

   },
   "job":{
      "setting":{
         "speed":{
            "channel":2
         }
      },
      "content":[
         {
            "reader":{
               "name":"txtfilereader",
               "parameter":{
                  "path":[
                     "/opt/test.txt"
                  ],
                  "encoding":"UTF-8",
                  "column":[
                     {
                        "index":0,
                        "type":"STRING"
                     },
                     {
                        "index":1,
                        "type":"STRING"
                     }
                  ],
                  "fieldDelimiter":"\t"
               }
            },
            "writer":{
               "name":"hdfswriter",
               "parameter":{
                  "defaultFS":"obs://obs-bucket",##obs桶
                  "fileType":"text",
                  "path":"/test",##obs桶中的路径
                  "fileName":"test",
```



```
                "column":[
                   {
                      "name":"col1",
                      "type":"STRING"
                   },
                   {
                      "name":"col2",
                      "type":"STRING"
                   }
                ],
                "writeMode":"append",
                "fieldDelimiter":"\t",
                "hadoopConfig":{##此部分hadoop配置必须添加
                   "fs.obs.impl":"org.apache.hadoop.fs.obs.OBSFileSystem",
                   "fs.obs.access.key":"可访问OBS的ak",
                   "fs.obs.secret.key":"可访问OBS的sk",
                   "fs.obs.endpoint":"OBS桶所在region"
                }
             }
          }
       }
    ]
  }
}
```

2. 启动datax。

   python /opt/datax/bin/datax.py file2obs.json

----结束

9.4.8 Druid 对接 OBS

概述

Druid专为需要快速数据查询与摄入的工作流程而设计，在即时数据可见性、即席查询、运营分析以及高并发等方面表现非常出色。

通过HDFS接口对接OBS，使用OBS提供的OBSA-HDFS工具，无需重新编译druid，将OBS配置为deep storage。

对接步骤

步骤1 配置Druid。

1. 修改配置：

   conf/druid/single-server/micro-quickstart/_common/common.runtime.properties

   将druid-hdfs-storage加入druid.extensions.loadList。

```
# If you specify `druid.extensions.loadList=[]`, Druid won't load any extension from file system.
# If you don't specify `druid.extensions.loadList`, Druid will load all the extensions under root extension directory.
# More info: https://druid.apache.org/docs/latest/operations/including-extensions.html
druid.extensions.loadList=["druid-hdfs-storage", "druid-kafka-indexing-service", "druid-datasketches"]
```

2. 配置Deep storage在OBS中的存储路径。

```
#
# Deep storage
#

# For local disk (only viable in a cluster if this is a network mount):
#druid.storage.type=local
#druid.storage.storageDirectory=var/druid/segments

# For HDFS:
druid.storage.type=hdfs
druid.storage.storageDirectory=obs://wxg-sg-oms-test/druidhdfs/segments
```

```
#
# Indexing service logs
#

# For local disk (only viable in a cluster if this is a network mount):
#druid.indexer.logs.type=file
#druid.indexer.logs.directory=var/druid/indexing-logs

# For HDFS:
druid.indexer.logs.type=hdfs
druid.indexer.logs.directory=obs://wxg-sg-oms-test/druidhdfs/indexing-logs
```

步骤2 配置OBSA-HDFS插件。

1. 在官方Github下载OBSA-HDFS插件：**下载地址**，然后拷贝到extensions/druid-hdfs-storage/ 目录。
2. 在配置目录conf/druid/single-server/micro-quickstart/_common/下增加hdfs-site.xml，配置如下（其中endpoint按照桶所在的实际endpoint填写）：


```
<configuration>
 <property>
   <name>fs.obs.access.key</name>
   <value>                                  </value>
 </property>
 <property>
   <name>fs.obs.secret.key</name>
   <value>                                                  </value>
 </property>
 <property>
   <name>fs.obs.endpoint</name>
   <value>obs.ap-southeast-3.myhuaweicloud.com</value>
 </property>
 <property>
   <name>fs.obs.buffer.dir</name>
   <value>/home/modules/data/buf</value>
 </property>
 <property>
   <name>fs.obs.impl</name>
   <value>org.apache.hadoop.fs.obs.OBSFileSystem</value>
 </property>
</configuration>
```

步骤3 启动Druid服务。

----结束

9.4.9 Flink 对接 OBS

概述

Flink是一个分布式的数据处理引擎，用于处理有界和无界流式数据。Flink定义了文件系统抽象，OBS服务实现了Flink的文件系统抽象，使得OBS可以作为flink StateBackend和数据读写的载体。

注意事项

- flink-obs-fs-hadoop目前仅支持OBS并行文件系统。
- 为了减少日志输出，在/opt/flink-1.12.1/conf/log4j.properties文件中增加配置：
  ```
  logger.obs.name=com.obs
  logger.obs.level=ERROR
  ```
- flink-obs-fs-hadoop的实现基于flink的plugin加载机制（flink从1.9开始引入），flink-obs-fs-hadoop必须通过flink的plugin机制进行加载，即将flink-obs-fs-hadoop放入/opt/flink-1.12.1/plugins/obs-fs-hadoop目录下。

对接步骤

以flink-1.12.1为例。

步骤1 下载flink-1.12.1-bin-scala_2.11.tgz，并解压到/opt/flink-1.12.1目录。

步骤2 在/etc/profile文件中增加配置：

```
export FLINK_HOME=/opt/flink-1.12.1
export PATH=$FLINK_HOME/bin:$PATH
```

步骤3 安装flink-obs-fs-hadoop。

1. 在Github下载flink-obs-fs-hadoop：**下载地址**。

   说明

   - flink-obs-fs-hadoop-${flinkversion}-hw-${version}.jar版本规则：flinkversion为对应的flink版本号，version为flink-obs-fs-hadoop版本号。
   - 如果没有匹配版本的jar包，可自行修改flink-obs-fs-hadoop目录下pom文件中的flink版本重新编译生成。详情见**编译指南**。
   - 自行编译flink-obs-fs-hadoop时，推荐编译依赖的hadoop.huaweicloud版本（hadoop.huaweicloud.version）不低于53.8版本。

2. 在/opt/flink-1.12.1/plugins目录下创建obs-fs-hadoop目录，并将上述jar放入此目录。

步骤4 配置flink。

在/opt/flink-1.12.1/conf/flink-conf.yaml文件中或在代码中设置如下参数：

```
fs.obs.impl: org.apache.hadoop.fs.obs.OBSFileSystem
fs.obs.access.key: xxx
fs.obs.secret.key: xxx
fs.obs.endpoint: xxx
fs.obs.buffer.dir: /data/buf #写数据到OBS时需要的本地临时目录，flink程序需具备此目录读写权限
```

步骤5 编写flink应用程序。

1. StateBackend设置为OBS中的路径。

   示例：

   ```
   env.setStateBackend(new FsStateBackend("obs://obs-bucket/test/checkpoint"));
   ```

2. StreamingFileSink设置为OBS中的路径。

   示例：

   ```
   final StreamingFileSink<String> sink = StreamingFileSink
   .forRowFormat(new Path("obs://obs-bucket/test/data"),
   new SimpleStringEncoder<String>("UTF-8"))
   .withBucketAssigner(new BasePathBucketAssigner())
   .withRollingPolicy(rollingPolicy)
   .withBucketCheckInterval(1000L)
   .build();
   ```

----结束

9.4.10 Logstash 对接 OBS

概述

Logstash能够从多个来源采集数据、转换数据并将数据发送到存储系统中，具体请参见**Logstash**。本文用于描述Logstash如何对接使用OBS。

注意事项

请使用较新版本的logstash，例如≥7.10.2的版本，避免使用较老版本的logstash。

对接步骤

以logstash-7.10.2为例。

步骤1 下载logstash-7.10.2-linux-x86_64.tar.gz，并解压到/opt/logstash-7.10.2-linux-x86_64目录。

步骤2 验证是否对接成功。

示例：以file为源端，以OBS为目的端。

1. 创建配置文件file2obs.conf。参数说明见**表9-3**，更多详情请参见**这里**。

```
input {
  file {
    path => "/opt/nginx/logs/access.log"
    start_position => "beginning"
  }
}

output {
  s3 {
    endpoint => "obs endpoint"   # The endpoint should be an HTTP or HTTPS URL
    access_key_id => "ak"
    secret_access_key => "sk"
    bucket => "obs bucket name"
    size_file => 1048576
    time_file => 1
    prefix => "logstash/"
    enable_metric => true
  }
}
```

表 9-3 参数说明

参数	说明
endpoint	OBS的endpoint，例如 – https://obs.cn-north-4.myhuaweicloud.com – http://obs.cn-north-4.myhuaweicloud.com
access_key_id	具备访问OBS权限的ak。
secret_access_key	具备访问OBS权限的sk。
bucket	OBS的桶名称。
size_file	指定文件滚动大小（字节）。当文件大小达到设定的值时，会生成一个新的文件。
time_file	设置文件滚动周期（分钟）。当数据写入达到设定周期时，会生成一个新的文件。
prefix	指定文件存储的目录，例如“logstash/”，此时文件会写入到桶的logstash/目录下（注意路径不要以/开头）。

2. 执行以下命令，运行logstash。

   bin/logstash -f ../conf/file2obs.conf

----结束

9.4.11 Spark on iceberg 最佳实践

概述

Iceberg是一种开放的数据湖表格式。您可以借助Iceberg快速地在HDFS或者华为云OBS上构建自己的数据湖存储服务，并借助开源大数据生态的Spark、Flink、Hive和Trino等计算引擎来实现数据湖的分析。

前提条件

- 完成Hadoop部署和对接OBS，详情参考**Hadoop对接OBS**。
- 完成Spark部署。

  如果数据目录Catalog选择Hive，Spark请使用预构建的包含Hive的Spark版本，可以spark-xxx-bin-hadoop3.tgz或者使用以下命令构建：

  ```
  mvn -DskipTests clean package -Phive -Phive-thriftserver
  ```

  注意，spark-xxx-bin-without-hadoop.tgz预构建没有包含Hive，请避免使用。

配置 spark on iceberg 环境

步骤1 下载iceberg-spark-runtime-xxx.jar。

步骤2 将iceberg-spark-runtime-xxx.jar复制到${SPARK_HOME}/jars

----结束

创建 Spark Catalog

您可以根据自身业务环境选择使用HMS或者Hadoop提供Catalog。

选项一：使用HMS（Hive MetaStore Service）提供Catalog

步骤1 部署HMS，推荐您使用远程模式部署。

步骤2 配置HMS和OBS。

执行以下命令，进入配置文件编辑页面：

```
vim ${SPARK_HOME}/conf/spark-defaults.conf
```

在配置文件中写入以下配置项：

```
spark.sql.catalog.hive_prod = org.apache.iceberg.spark.SparkCatalog
spark.sql.catalog.hive_prod.type = hive
spark.sql.catalog.hive_prod.uri = thrift://jtc-vm:9083
spark.sql.catalog.hive_prod.warehouse = obs://jtc-pfs001/warehouse/spark-iceberg
```

其中uri参数为HMS服务的URI，warehouse参数为OBS桶内目录的路径，您需要结合自身的业务和环境进行配置。

修改完成后，按“Esc”，输入**:wq**保存并退出文件编辑。

步骤3 启动spark-sql，命令如下：

```
${SPARK_HOME}/bin/spark-sql
```

步骤4 启动成功后，指定catalog，命令如下：

```
use hive_prod;
```


步骤5 创建数据库和表，命令如下：

```
CREATE DATABASE db_xxx;
use db_xxx;
CREATE TABLE tbl_xxx(...);
```

----结束

选项二：使用Hadoop提供Catalog

步骤1 配置Hadoop和OBS。

执行以下命令，进入配置文件编辑页面：

```
vim ${SPARK_HOME}/conf/spark-defaults.conf
```

在配置文件中写入以下配置项：

```
spark.sql.catalog.hadoop_prod = org.apache.iceberg.spark.SparkCatalog
spark.sql.catalog.hadoop_prod.type = hadoop
spark.sql.catalog.hadoop_prod.warehouse = obs://jtc-pfs001/warehouse/spark-iceberg-hadoop-prod
```

其中warehouse参数为OBS桶内目录的路径，您需要结合自身的业务和环境进行配置。

修改完成后，按“Esc”，输入**:wq**保存并退出文件编辑。

步骤2 启动spark-sql，命令如下：

```
${SPARK_HOME}/bin/spark-sql
```

步骤3 启动成功后，指定Catalog，命令如下：

```
use hadoop_prod;
```

步骤4 创建数据库和表，命令如下：

```
CREATE DATABASE db_xxx;
use db_xxx;
CREATE TABLE tbl_xxx(...);
```

----结束

9.4.12 Trino on iceberg 最佳实践

概述

Iceberg是一种开放的数据湖表格式。您可以借助Iceberg快速地在HDFS或者华为云OBS上构建自己的数据湖存储服务，并借助开源大数据生态的Spark、Flink、Hive和Trino等计算引擎来实现数据湖的分析。其中，Trino是针对OLAP设计的用于高效的分布式查询大量数据的分析引擎。主要具备下列优点：

- 屏蔽底层数据源，提供统一查询接口。
- 基于内存计算，可以跨不同数据源完成联邦查询。
- 使用Trino进行数据治理，可以通过Trino进行异构数据的提取、整合与分析，打破数据孤岛、提高数据治理能力。

前提条件

- 完成Trino部署，了解更多请参考**Trino最新版本的官方文档**，如需查看指定版本的官方文档，请访问https://trino.io/docs/*VersionID*/ ，将*VersionID*替换为版本号，比如https://trino.io/docs/460/ 即访问Trino 460的官方文档。

- 完成Hadoop部署并对接OBS，详情参考**Hadoop对接OBS**。

配置 OBS 对接

步骤1 复制hadoop-huaweicloud-3.1.1-hw-xxx.jar到${TRINO_HOME}/plugin/iceberg/hdfs目录。

步骤2 部署Hive MetaStore，推荐使用远程模式。

步骤3 配置catalog。

执行以下命令，进入配置文件编辑页面：

```
vim $TRINO_HOME/etc/catalog/iceberg.properties
```

在配置文件中写入以下配置项：

```
connector.name=iceberg
hive.metastore.uri=thrift://jtc-vm:9083
fs.hadoop.enabled=true
hive.config.resources=${HADOOP_HOME}/etc/hadoop/core-site.xml
```

其中uri参数为HMS服务的URI，您需要结合自身的业务和环境进行配置。

修改完成后，按“Esc”，输入**:wq**保存并退出文件编辑。

步骤4 使用Trino Client CLI连接Trino Server进行验证，连接时使用参数--catalog指定Catalog名称。

```
trino Trino_URI --catalog Catalog_Name
```

其中*Trino_URI*请参考${TRINO_HOME}/etc/config.properties。*Catalog_Name*为上一步配置的connector.name。例如：

```
trino http://jtc-vm:8080 --catalog iceberg
```

步骤5 创建SCHEMA并指定LOCATION，请执行以下命令：

```
CREATE SCHEMA schema_name AUTHORIZATION user_name WITH (LOCATION = file_path);
```

- schema_name：SCHEMA名称，此处以schema_example为例。
- user_name：用户名。此处以root为例。
- file_path：OBS桶中目录的路径，例如桶名为jtc-pfs001，目录名为warehouse/trino-iceberg：

  ```
  CREATE SCHEMA schema_example AUTHORIZATION root WITH (LOCATION = 'obs://jtc-pfs001/warehouse/trino-iceberg');
  ```

步骤6 创建TABLE，指定上一步的SCHEMA。

```
CREATE TABLE IF NOT EXISTS schema_example.orders(
    order_key bigint,
    order_status varchar,
    total_price double,
    order_date date);
```

----结束

9.4.13 Spark on Paimon 最佳实践

概述

Apache Paimon是一个流式数据湖存储技术，它提供高吞吐、低延迟的数据摄入、流式订阅和实时查询。采用开放的ORC、Parquet、Avro文件格式，与Flink、Spark等计算引擎兼容。

前提条件

- 完成Hadoop部署并对接OBS，详情参考**Hadoop对接OBS**。
- 完成Spark部署。

  如果数据目录Catalog选择Hive，Spark请使用预构建的包含Hive的Spark版本，可以使用spark-xxx-bin-hadoop3.tgz或者使用以下命令构建：

  ```
  mvn -DskipTests clean package -Phive -Phive-thriftserver
  ```

  注意，spark-xxx-bin-without-hadoop.tgz预构建没有包含Hive，请避免使用。

配置 Spark on Paimon 环境

进入**Apache Paimon官方文档**，选择需要使用Paimon版本，参考对应版本文档的Engine Spark>Quick Start章节，完成Spark与Paimon的对接。

创建 spark catalog

您可以根据自身业务环境选择Catalog type使用filesystem或者hive。

选项1：配置Paimon对接OBS，Catalog type使用filesystem

步骤1 启动spark-sql执行Paimon Catalog配置。

```
spark-sql \
  --conf "spark.driver.extraJavaOptions=-Dspark.sql.catalogImplementation=in-memory"
  --conf "spark.sql.catalog.paimon=org.apache.paimon.spark.SparkCatalog" \
  --conf "spark.sql.catalog.paimon.metastore=filesystem" \
  --conf "spark.sql.catalog.paimon.warehouse=obs://xxx/xxx" \
  --conf "spark.sql.extensions=org.apache.paimon.spark.extensions.PaimonSparkSessionExtensions"
```

或者您也可以在spark-default.conf 中配置，执行以下命令，进入配置文件编辑页面：

```
vim ${SPARK_HOME}/conf/spark-defaults.conf
```

在配置文件中写入以下配置项：

```
spark.sql.catalogImplementation=in-memory
spark.sql.catalog.paimon=org.apache.paimon.spark.SparkCatalog
spark.sql.catalog.paimon.metastore=filesystem
spark.sql.catalog.paimon.warehouse=obs://xxx/xxx
spark.sql.extensions=org.apache.paimon.spark.extensions.PaimonSparkSessionExtensions
```

修改完成后，按“Esc”，输入**:wq**保存并退出文件编辑。

步骤2 切换到指定Catalog，命令如下：

```
USE paimon;
```

步骤3 创建数据库和表，命令如下：

```
CREATE DATABASE db_xxx;
use db_xxx;
CREATE TABLE tbl_xxx(...);
```

----结束

选项2：配置Paimon对接OBS，Catalog type使用hive

步骤1 启动spark-sql执行Paimon Catalog配置，命令如下：

```
spark-sql \
   --conf "spark.sql.catalog.paimon=org.apache.paimon.spark.SparkCatalog" \
   --conf "spark.sql.catalog.paimon.warehouse=obs://xxx/xxx" \
   --conf "spark.sql.catalog.paimon.metastore=hive"
```

或者您也可以在spark-default.conf 中配置，执行以下命令，进入配置文件编辑页面：


```
vim ${SPARK_HOME}/conf/spark-defaults.conf
```

在配置文件中写入以下配置项：

```
spark.sql.catalog.paimon=org.apache.paimon.spark.SparkCatalog
spark.sql.catalog.paimon.metastore=hive
spark.sql.catalog.paimon.warehouse=obs://xxx/xxx
```

修改完成后，按“Esc”，输入**:wq**保存并退出文件编辑。

步骤2 切换到指定catalog，命令如下：

```
use paimon;
```

步骤3 创建数据库和表，命令如下：

```
CREATE DATABASE db_xxx;
use db_xxx;
CREATE TABLE tbl_xxx(...);
```

----结束

9.4.14 Flink on Paimon 最佳实践

概述

Apache Paimon是一个流式数据湖存储技术，它提供高吞吐、低延迟的数据摄入、流式订阅和实时查询。采用开放的ORC、Parquet、Avro文件格式，与Flink、Spark等计算引擎兼容。

前提条件

- 完成Hadoop部署并对接OBS，详情参考**Hadoop对接OBS**。
- 已部署Flink，并集成Paimon到Flink中，详情参考**Flink官方文档**。

Flink 对接 OBS

步骤1 **下载**flink-obs。

步骤2 使用mvn构建flink对应版本的flink-obs-fs-hadoop-xxx.jar。

步骤3 创建${FLINK_HOME}/plugins/obs-fs-hadoop目录。

步骤4 复制**2**中构建的flink-obs-fs-hadoop-xxx.jar到${FLINK_HOME}/plugins/obs-fs-hadoop目录。

步骤5 配置环境变量，命令如下：

```
export HADOOP_CLASSPATH=$(hadoop classpath)
```

步骤6 在Flink的配置文件中配置OBSA参数：flink-conf.yaml(1.19之前)，config.yaml(1.19及以后)

```
fs.obs.impl: org.apache.hadoop.fs.obs.OBSFileSystem
fs.obs.access.key: xxx
fs.obs.secret.key: xxx
fs.obs.endpoint: obs.xxx.myhuaweicloud.com
fs.obs.buffer.dir: /opt/data/obsa_buffer
```

----结束

配置 Paimon 对接 OBS

步骤1 创建Paimon Catalog，warehouse路径指定为OBS桶中目录，例如指定为jtc-pfs001桶中的flink/paimon101目录：

```
CREATE CATALOG paimon101_catlog WITH (
    'type'='paimon',
    'warehouse'='obs://jtc-pfs001/flink/paimon101'
);
```

步骤2 创建数据库，指定catalog创建或使用use catalog *catalog_name*指定catalog。

```
use catalog paimon101_catlog;
create paimon_db;
create paimon101_catlog.paimon_db;
```

----结束

9.4.15 Flink 使用 Hive connector 对接 OBS 指导

概述

通过使用Hive Catalog，Apache Flink可以对Apache Hive表做统一的批处理和流处理。这意味着Flink可以成为Hive批处理引擎的一个性能更好的选择，或者连续读写Hive表中的数据以支持实时数据仓库应用。

前提条件

参考**Flink对接OBS**完成Flink对接OBS。

配置 Flink 的 Hive connector 连接

参考**Flink官网文档**完成Flink的Hive connector连接。注意：Hive connector仅支持JDK8.x，不支持JDK11+。

运行

步骤1 启动Flink。

步骤2 启动SQL Client。

步骤3 创建Flink HiveCatalog，命令如下：

```
CREATE CATALOG obs_hive WITH (
    'type' = 'hive',
    'default-database' = 'userdb',
    'hive-conf-dir' = '/opt/flink-1.20.0/conf/'
);
```

步骤4 使用HiveCatalog，命令如下：

```
USE CATALOG obs_hive;
```

步骤5 使用Hive dialect，命令如下：

```
SET table.sql-dialect = hive;
```

步骤6 创建外表并指定LOCATION，命令如下：

```
CREATE EXTERNAL TABLE IF NOT EXISTS table_xxx(
  id INT,
  name STRING,
  age INT
```



```
)
LOCATION 'obs://bucket_xxx/flink/warehouse/userdb.db/table_xxx;
```

----结束

9.4.16 StarRocks 访问 Apache Hive+OBS 存算分离指导

概述

StarRocks 是一款高性能分析型数据仓库，使用向量化、MPP 架构、CBO、智能物化视图、可实时更新的列式存储引擎等技术实现多维、实时、高并发的数据分析。StarRocks既支持从各类实时和离线的数据源高效导入数据，也支持直接分析数据湖上各种格式的数据。StarRocks 兼容MySQL协议，可使用MySQL客户端和常用BI工具对接。同时StarRocks具备水平扩展，高可用、高可靠、易运维等特性。广泛应用于实时数仓、OLAP 报表、数据湖分析等场景。

Hive Catalog是一种External Catalog，自2.3版本开始支持，通过Hive Catalog您可以：

- 无需手动建表，通过Hive Catalog直接查询Hive内的数据。
- 通过INSERT INTO或异步物化视图（3.1 版本及以上）将Hive内的数据进行加工建模，并导入至StarRocks。
- 在StarRocks侧创建或删除Hive库表，或通过INSERT INTO把StarRocks表数据写入到Parquet格式（3.2 版本及以上）、以及ORC或Textfile格式（3.3 版本及以上）的Hive表中。

Hadoop 配置

步骤1 将HDFS集群中的core-site.xml文件放到每个FE的 $FE_HOME/conf路径下，以及每个BE的$BE_HOME/conf路径下。以下是一个core-site.xml文件的示例：

```
<?xml version="1.0" encoding="UTF-8"?>
<?xml-stylesheet type="text/xsl" href="configuration.xsl"?>
<!--
  Licensed under the Apache License, Version 2.0 (the "License");
  you may not use this file except in compliance with the License.
  You may obtain a copy of the License at

    http://www.apache.org/licenses/LICENSE-2.0

  Unless required by applicable law or agreed to in writing, software
  distributed under the License is distributed on an "AS IS" BASIS,
  WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
  See the License for the specific language governing permissions and
  limitations under the License. See accompanying LICENSE file.
-->

<!-- Put site-specific property overrides in this file. -->

<configuration>
    <property>
        <name>fs.defaultFS</name>
        <value>obs://xxx/</value>
    </property>
    <property>
        <name>hadoop.tmp.dir</name>
        <value>/xxx</value>
    </property>
    <property>
        <name>fs.obs.impl</name>
        <value>org.apache.hadoop.fs.obs.OBSFileSystem</value>
```



```
    </property>
    <property>
        <name>fs.AbstractFileSystem.obs.impl</name>
        <value>org.apache.hadoop.fs.obs.OBS</value>
    </property>
    <property>
        <name>fs.obs.access.key</name>
        <value>xxx</value>
    </property>
    <property>
        <name>fs.obs.secret.key</name>
        <value>xxx</value>
    </property>
    <property>
        <name>fs.obs.endpoint</name>
        <value>obs.xxx.myhuaweicloud.com</value>
    </property>
</configuration>
```

步骤2 复制**hadoop-huaweicloud-xxx-hw-xxx.jar**到每个BE的$BE_HOME/lib/hadoop/common/lib目录下。

步骤3 配置每个BE的$BE_HOME/conf/be.conf文件。执行以下命令，进入配置文件编辑页面：

```
vim $BE_HOME/conf/be.conf
```

增加如下配置：

```
fallback_to_hadoop_fs_list = obs://
```

修改完成后，按“Esc”，输入**:wq**保存并退出文件编辑。

----结束

创建 Hive Catalog，使用 HMS

```
CREATE EXTERNAL CATALOG hive_catalog_hms
PROPERTIES
(
    "type" = "hive",
    "hive.metastore.type" = "hive",
    "hive.metastore.uris" = "thrift://xxx:9083"
);
```

切换 Hive Catalog 和数据库

您可以通过如下方法切换至目标 Hive Catalog 和数据库：

- 先通过 `SET CATALOG `指定当前会话生效的 Hive Catalog，然后再通过 `USE`指定数据库：

  ```
  -- 切换当前会话生效的 Catalog：
  SET CATALOG hive_catalog_hms;
  -- 指定当前会话生效的数据库：
  USE <db_name>
  ```

- 或者通过 `USE`直接将会话切换到目标 Hive Catalog 下的指定数据库：

  ```
  USE hive_catalog_hms.<db_name>
  ```


9.5 迁移 HDFS 数据至 OBS

操作场景

在华为云大数据存算分离方案中，对象存储服务OBS作为统一数据湖存储数据。如果用户数据仍存储在本地HDFS中，则需要先将HDFS的数据迁移至OBS。

用户可以使用以下迁移方案中的任意一种完成数据迁移，包括：**Distcp方式迁移**、**CDM方式迁移**和**OMS方式迁移**。

Distcp 方式迁移

Hadoop Distcp（Distributed copy）主要是用于Hadoop文件系统内部或之间进行大规模数据复制的工具，它使用Map/Reduce实现文件分发，错误处理和恢复，以及报告生成。它把文件和目录的列表作为map任务的输入，每个任务会完成源列表中部分文件的拷贝。

配置指南

参考**Hadoop对接OBS**中hadoop-huaweicloud的安装和配置方法，完成OBS相关配置。

使用示例

步骤1 以迁移HDFS上的“/data/sample”目录为例，执行以下命令查看HDFS文件系统上此目录下的文件与目录。

hadoop fs -ls hdfs:///data/sample

步骤2 执行以下命令，将HDFS文件系统上“/data/sample”目录下所有文件与目录迁移到OBS桶“obs-bigdata-posix-bucket”的“data/sample”目录下。

hadoop distcp hdfs:///data/sample obs://obs-bigdata-posix-bucket/data/sample

步骤3 执行以下命令，查看拷贝的文件。

hadoop fs -ls obs://obs-bigdata-posix-bucket/data/sample

----结束

CDM 方式迁移

云数据迁移（Cloud Data Migration，CDM）提供同构/异构数据源之间批量数据迁移服务，帮助您实现数据自由流动。支持关系数据库，数据仓库，NoSQL，大数据云服务等数据源。

详细内容请参见**云数据迁移**。

OMS 方式迁移

对象存储迁移服务（Object Storage Migration Service，OMS）是一种线上数据迁移服务，帮助您将其他云服务商对象存储服务中的数据在线迁移至华为云的对象存储服务（Object Storage Service，OBS）中。

详细内容请参见**对象存储迁移服务**。

10 面向 AI 场景使用 OBS+SFS Turbo 的存储加速实践

10.1 面向 AI 场景使用 OBS+SFS Turbo 的存储加速方案概述

应用场景

近年来，AI快速发展并应用到很多领域中，AI新产品掀起一波又一波热潮，AI应用场景越来越多，有自动驾驶、大模型、AIGC、科学AI等不同行业。AI人工智能的实现需要大量的基础设施资源，包括高性能算力，高速存储和网络带宽等基础设施，即“大算力、大存力、大运力”的AI基础大设施底座，让算力发展不要偏斜。

从过去的经典AI，到今天人人谈论的大模型，自动驾驶，我们看到AI模型的参数及AI算力规模呈现出指数级的爆发增长，对存储基础设施也带来全新的挑战。

1. **高吞吐的数据访问挑战**：随着企业使用 GPU/NPU 越来越多，底层存储的 IO 已经跟不上计算能力，企业希望存储系统能提供高吞吐的数据访问能力，充分发挥 GPU/NPU 的计算性能，包括训练数据的读取，以及为了容错做的检查点（以下简称Checkpoint）保存和加载。训练数据的读取要尽量读得快，减少计算对 I/O 的等待，而 Checkpoint主要要求高吞吐、减少训练中断的时间。
2. **文件接口方式的数据共享访问**：由于 AI 架构需要使用到大规模的计算集群（GPU/NPU服务器），集群中的服务器访问的数据来自一个统一的数据源，即一个共享的存储空间。这种共享访问的数据有诸多好处，它可以保证不同服务器上访问数据的一致性，减少不同服务器上分别保留数据带来的数据冗余等。另外以 AI 生态中非常流行的开源深度学习框架PyTorch为例，PyTorch默认会通过文件接口访问数据，AI算法开发人员也习惯使用文件接口，因此文件接口是最友好的共享存储访问方式。

说明

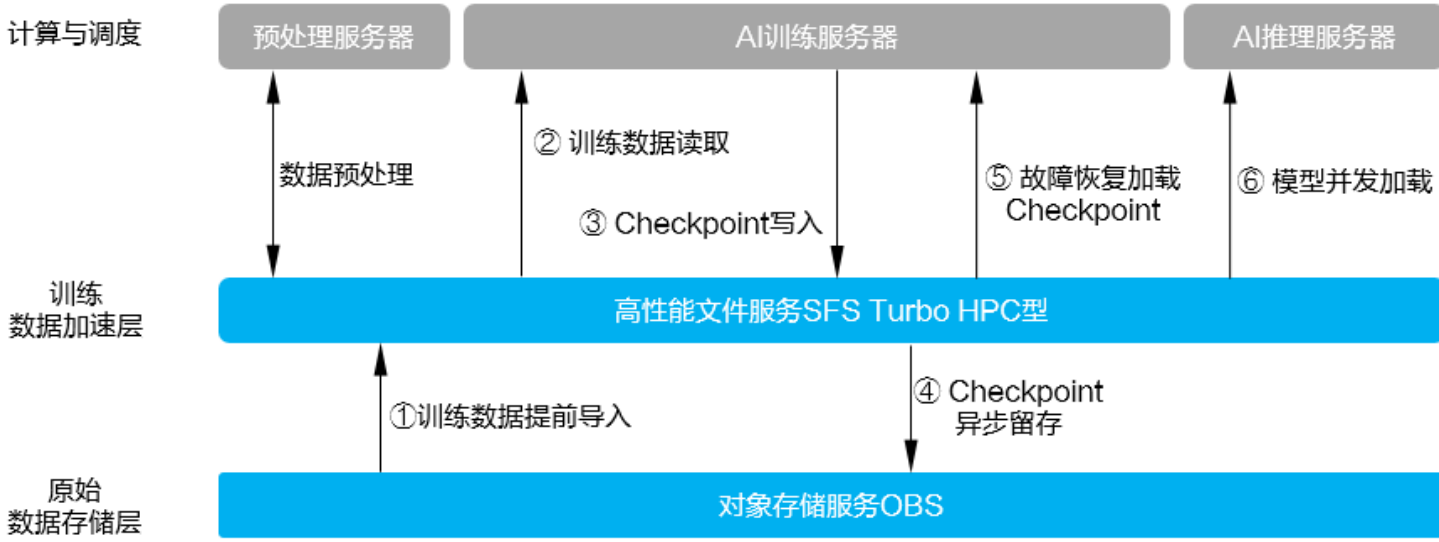
如果您想了解更多本方案相关信息，或在方案使用过程中存在疑问，可通过**方案咨询**渠道，寻求专业人员支持。

方案架构

针对AI训练场景中面临的问题，华为云提供了基于对象存储服务OBS+高性能文件服务SFS Turbo的AI云存储解决方案，如图所示，华为云高性能文件服务SFS Turbo HPC型

支持和OBS数据联动，您可以通过SFS Turbo HPC型文件系统来加速对OBS对象存储中的数据访问，并将生成的结果数据异步持久化到OBS对象存储中长期低成本保存。

图 10-1 基于 OBS+SFS Turbo 的华为云 AI 云存储解决方案



方案优势

华为云AI云存储解决方案的主要优势如下表所示。

表 10-1 华为云 AI 云存储解决方案的主要优势

序号	主要优势	详细描述
1	存算分离，资源利用率高	GPU/NPU算力和SFS Turbo存储解耦，各自按需扩容，资源利用率提升。
2	SFS Turbo高性能，加速训练过程	• 训练数据集高速读取，避免GPU/NPU因存储I/O等待产生空闲，提升GPU/NPU利用率。 • 大模型TB级Checkpoint文件秒级保存和加载，减少训练任务中断时间。 • 提供AITurbo SDK，**加速Checkpoint保存和加载**。
3	数据导入导出异步化，不占用训练任务时长，无需部署外部迁移工具	• 训练任务开始前将数据从OBS导入到SFS Turbo，训练过程中写入到SFS Turbo的Checkpoint数据异步导出到OBS，均不占用训练任务时长。 • SFS Turbo和OBS存储服务之间数据直接导入导出，无需部署外部数据拷贝机器及工具。
4	冷热数据自动流动，降低存储成本	• SFS Turbo支持自定义数据淘汰策略，冷数据自动分级到OBS，释放高性能存储空间用于接收新的热数据。 • 访问冷数据时SFS Turbo从OBS自动加载数据提升访问性能。

序号	主要优势	详细描述
5	多AI开发平台、生态兼容	pytorch、mindspore等主流AI应用框架，kubernetes容器引擎、算法开发场景通过文件语义访问共享数据，无需适配开发。

说明

如果您想了解更多本方案相关信息，或在方案使用过程中存在疑问，可通过**方案咨询**渠道，寻求专业人员支持。

10.2 资源和成本规划

本节介绍最佳实践中资源规划情况，包含以下内容：

表 10-2 资源和成本规划内容说明

维度	说明
资源规划	• OBS：存放训练数据集、预训练模型等数据资源的桶，桶存储类别为“标准存储”，桶策略为“私有”。 • SFS Turbo：文件系统类型为“HPC型”，存储类型请根据存储容量和性能需求选择，AI场景建议选择250MB/s/TiB及以上的存储类型。 • ModelArts：AI开发平台，采用多机多卡分布式训练。 • VPC：虚拟私有云和子网。 • 算法及数据：准备AI训练需要的算法及数据集，如Swin-Transformer算法，及ImageNet21K数据集。 **说明** 为了提供最佳加速性能，建议SFS Turbo HPC文件系统和ModelArts资源池就近选择在同一个Region的同一个可用区（AZ）。
成本规划	• OBS费用：详见**OBS计费说明**。 • SFS Turbo费用：详见**SFS计费说明**。 • ModelArts费用：详见**ModelArts计费说明**。 **须知** 本文提供的成本预估费用仅供参考，资源的实际费用以华为云管理控制台或价格计算器显示为准。

说明

如果您想了解更多本方案相关信息，或在方案使用过程中存在疑问，可通过**方案咨询**渠道，寻求专业人员支持。

10.3 操作流程

本文档介绍面向AI场景如何使用OBS+SFS Turbo的存储加速，流程如图10-2所示。

图 10-2 面向 AI 场景使用 OBS+SFS Turbo 的存储加速方案步骤

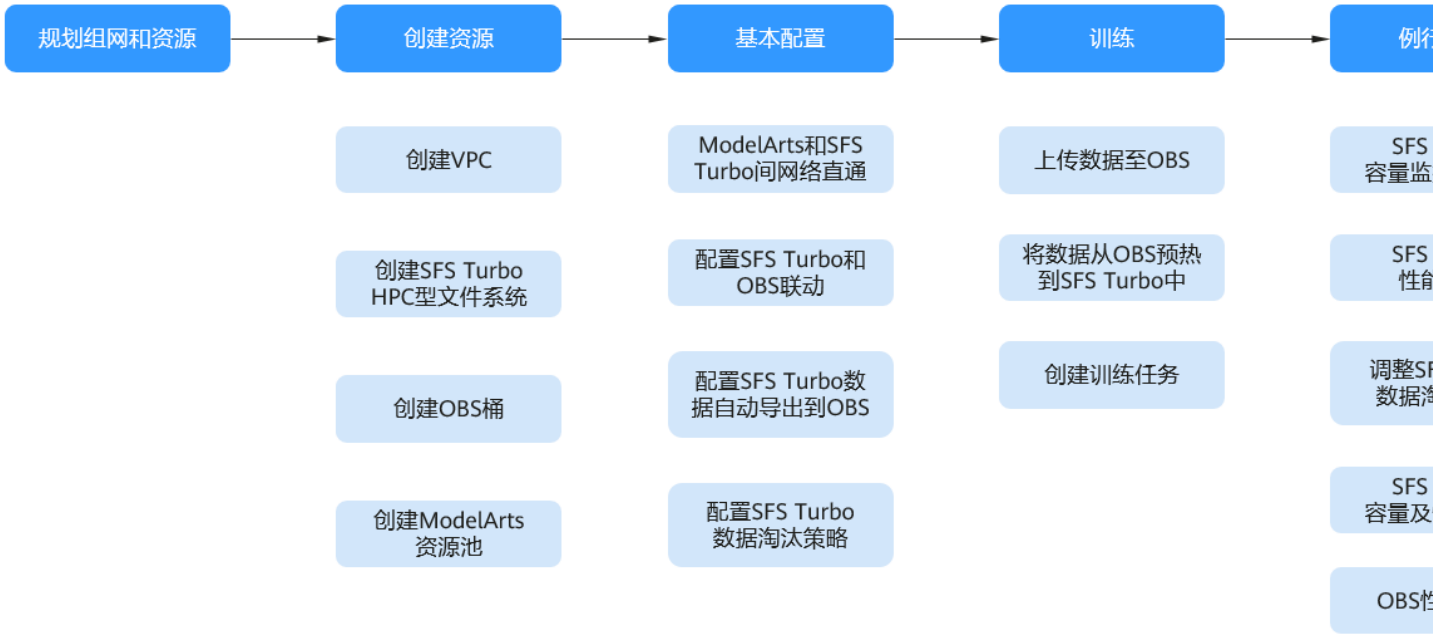


表 10-3 面向 AI 场景使用 OBS+SFS Turbo 的存储加速流程说明

序号	步骤	说明
1	规划组网和资源	此步骤请提交工单联系技术支持人员进行支撑配置。
2	创建资源	1. 创建VPC：创建1个虚拟私有云和子网。 2. 创建SFS Turbo HPC型文件系统：创建1个SFS Turbo文件系统，文件系统类型选择“HPC型”,存储类型请根据存储容量和性能需求选择，AI场景建议选择250MB/s/TiB及以上的存储类型。 3. 创建OBS桶：创建1个OBS桶，存储类别为“标准存储”，桶策略为“私有”。 4. 创建ModelArts资源池：创建1个专属资源池。
3	基本配置	1. 配置ModelArts和SFS Turbo间网络直通。 a. 创建委托授权ModelArts云服务使用SFS Turbo。 b. 配置ModelArts网络关联SFS Turbo。 2. 配置SFS Turbo和OBS联动。 3. 配置SFS Turbo数据自动导出到OBS桶。 4. 配置SFS Turbo数据淘汰策略。

序号	步骤	说明
4	训练	1. 上传数据至OBS并预热到SFS Turbo中。 2. 创建训练任务。
5	例行运维	使用OBS+SFS Turbo的存储加速方案的过程中，您可以进行采取以下运维措施，保证系统正常高效运行： • SFS Turbo容量监控及告警。 • SFS Turbo性能监控。 • 调整SFS Turbo数据淘汰策略。 • SFS Turbo容量及性能扩容。 • OBS性能监控。

说明

如果您想了解更多本方案相关信息，或在方案使用过程中存在疑问，可通过**方案咨询**渠道，寻求专业人员支持。

10.4 实施步骤

10.4.1 创建资源

本最佳实践方案需要使用到VPC、SFS Turbo HPC型文件系统、OBS桶、ModelArts资源池资源。

说明

为了提供最佳加速性能，建议SFS Turbo HPC文件系统和ModelArts资源池就近选择在同一个Region的同一个可用区（AZ）。

创建 VPC

虚拟私有云可以为您构建隔离的、用户自主配置和管理的虚拟网络环境，操作指导请参考**创建虚拟私有云和子网**。

创建 SFS Turbo HPC 型文件系统

创建SFS Turbo文件系统，文件系统类型选择“HPC型”，操作指导请参考**创建SFS Turbo文件系统**。

创建 OBS 桶

创建OBS桶，存储类别为“标准存储”，桶策略为“私有”，操作指导请参考**创建OBS桶**。

创建 ModelArts 资源池

以常见的专属资源池为例，专属资源池提供独享的计算资源，可用于Notebook、训练作业、部署模型。专属资源池不与其他用户共享，更加高效。在使用专属资源池之前，您需要先创建一个专属资源池，操作指导请参考**创建专属资源池**。

10.4.2 基本配置

10.4.2.1 配置 ModelArts 和 SFS Turbo 间网络直通

创建委托授权 ModelArts 云服务使用 SFS Turbo

步骤1 使用IAM管理员账号登录**IAM控制台**。

步骤2 在**IAM控制台**的左侧导航窗格中选择“权限管理 > 权限”，单击右上角的“创建自定义策略”，进入自定义策略配置页面。

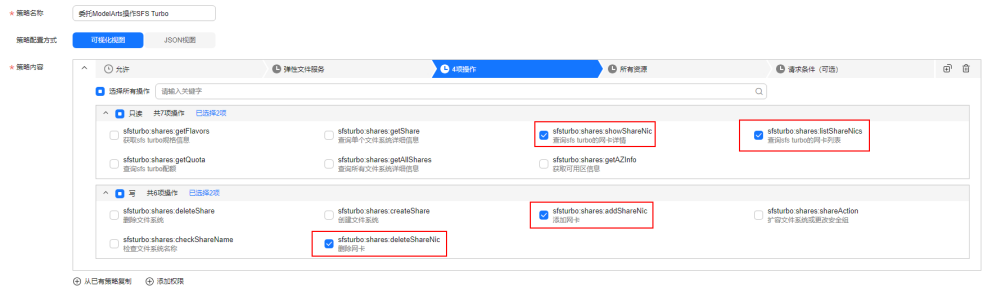
步骤3 输入“策略名称”，用户可根据需要自定义，例如“委托modelarts操作SFS Turbo”

步骤4 “**策略配置方式**”选择选择“**可视化视图**”或者“**JOSN视图**”均可。如果选择“**可视化视图**”请跳转至**步骤5**，如果选择“**JOSN视图**”请跳转至**步骤6**。

步骤5 在“策略内容”下配置策略，如**图**所示。

1. 选择“**允许**”。
2. 选择云服务，勾选“**弹性文件服务(SFSTurbo)**”。
3. 选择“**操作**”，勾选只读操作“**sfsturbo:shares:showShareNic**”、“**sfsturbo:shares:listShareNics**”，勾选写操作“**sfsturbo:shares:addShareNic**”、“**sfsturbo:shares:deleteShareNic**”。
4. 选择“**所有资源**”

图 10-3 创建委托授权 ModelArts 云服务使用 SFS Turbo



步骤6 在“策略内容”区域，填写以下授权语句。

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sfsturbo:shares:addShareNic",
                "sfsturbo:shares:listShareNics",
                "sfsturbo:shares:deleteShareNic",
                "sfsturbo:shares:showShareNic"
            ]
        }
```

```
  ]
}
```

步骤7 单击“确定”，完成自定义策略创建。

步骤8 在IAM控制台页面的左侧导航窗格中选择“委托”，单击右上方的“创建委托”。

步骤9 在创建委托页面，设置“委托名称”，例如设置为“modelarts_agency”。

步骤10 “委托类型”选择“云服务”，在“云服务”中选择“ModelArts”，持续时间根据用户需要选取，单击“下一步”，进入给委托授权页面。

步骤11 勾选步骤1到7创建的自定义策略，给委托授权，单击“下一步”。

步骤12 选择授权范围方案，选择“所有资源”。

步骤13 单击“确定”，委托创建完成。

----结束

配置 ModelArts 网络关联 SFS Turbo

ModelArts网络关联SFS Turbo后，可直接在ModelArts的Notebook开发及训练环境中挂载SFS Turbo共享文件系统，并访问其中的数据。

步骤1 登录ModelArts管理控制台，创建网络并打通创建资源中创建的创建虚拟私有云和子网，详细步骤参见ModelArts网络。

步骤2 单击1中创建生成的资源池“网络”所在行的“更多”，选择“关联sfsturbo”。

步骤3 在“关联sfsturbo”弹窗中，选择创建资源中创建的SFS Turbo HPC型文件系统。

图 10-4 关联 SFS Turbo

步骤4 选择完成后，单击“确定”创建关联。

----结束

说明

1. 使用过程中请不要解除关联，解除关联会导致ModelArts资源池无法访问SFS Turbo文件系统中的数据。
2. 一个SFS Turbo文件系统最多可关联1个网络。

10.4.2.2 配置 SFS Turbo 和 OBS 联动

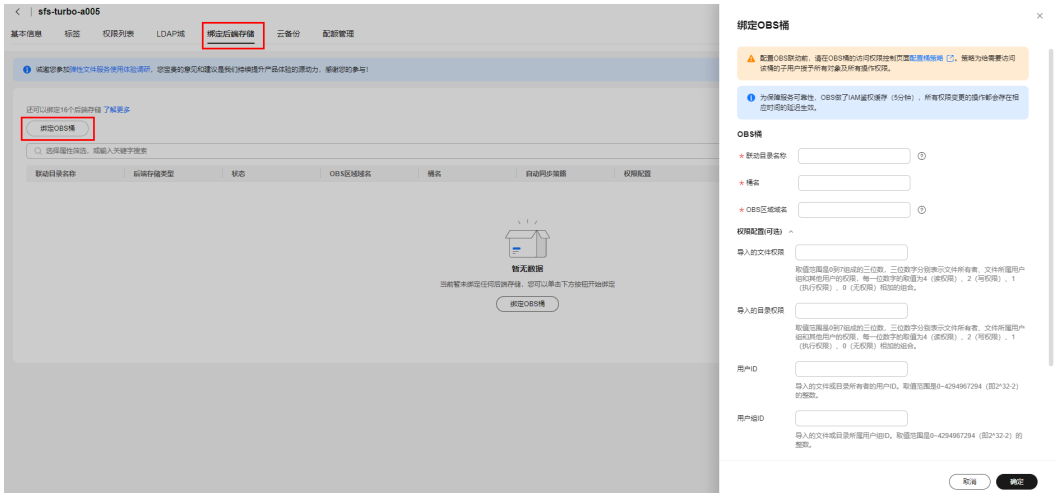
SFS Turbo HPC型文件系统支持无缝访问存储在对象存储OBS存储桶中的对象，您可以指定SFS Turbo内的文件目录与OBS对象存储桶进行关联。更多内容请参考**管理SFS Turbo文件系统与OBS桶的存储联动**。

步骤1 登录**SFS管理控制台**，在左侧导航窗格中选择“SFS Turbo”。

步骤2 在文件系统列表中，单击**创建资源**中创建的HPC型文件系统，进入文件系统详情页面。

步骤3 进入页签“绑定后端存储”，单击“绑定OBS桶”。

图 10-5 绑定 OBS 桶



步骤4 在右侧弹窗“绑定OBS目标”中，填写如下**表**所示参数。

表 10-4 绑定 OBS 目标配置参数

参数	含义	限制	配置后可编辑
动目录名称	SFS Turbo文件系统根目录下会以该名称创建一个子目录，该目录将绑定对应的OBS桶，且该目录名称不能和已有目录重名。	• 子目录名称不能重复，子目录名称长度不能超过63个字符。 • 子目录名称必须是文件系统根目录下不存在的目录名。 • 子目录名称不能是“.”或“..”。	不支持
桶名	OBS存储桶桶名。	• 无法绑定不存在的存储桶。 • 目前仅支持OBS存储桶，不支持OBS并行文件系统。	不支持

参数	含义	限制	配置后可编辑
OBS区域域名	OBS区域域名，即OBS的终端节点。	OBS存储桶必须和SFS Turbo文件系统在同一个Region。	不支持
导入的文件权限	导入的文件权限。输入的三位数字分别表示文件所有者、文件所属用户组和其他用户的权限，每一位数字的取值为4（读权限）、2（写权限）、1（执行权限）、0（无权限）相加的组合。	可选参数。取值范围是0到7组成的三位数。	支持
导入的目录权限	导入的目录权限。输入的三位数字分别表示文件所有者、文件所属用户组和其他用户的权限，每位数字的取值为4（读权限）、2（写权限）、1（执行权限）、0（无权限）相加的组合。	可选参数。取值范围是0到7组成的三位数。	支持
用户ID	导入的文件或目录所有者的用户ID。	可选参数。取值范围是0到4294967294（即2^32-2）。	支持
用户组ID	导入的文件或目录所属用户组ID。	可选参数。取值范围是0到4294967294（即2^32-2）。	支持

说明

ModelArts平台默认使用ma-user用户来访问SFS Turbo，建议把“导入的文件权限”和“导入的目录权限”设置为777。

步骤5 勾选“将OBS桶的读写权限通过桶策略授权给SFS Turbo云服务”。

步骤6 单击“确定”，完成绑定。

----结束

10.4.2.3 配置 SFS Turbo 数据自动导出到 OBS 桶

配置自动导出后，训练过程中周期性写入SFS Turbo文件系统的Checkpoint模型文件会自动以异步方式导出到关联的OBS桶中进行长期保存，无需手工导出，异步导出方式不会占用上层训练任务时间。

说明

文件导出速度受OBS服务的写入带宽上限影响，默认是16Gbit/s，如果大模型训练生成的Checkpoint文件过大、导出速度过慢，可**提交工单**申请调大OBS服务的写入带宽。

10.4.2.4 配置 SFS Turbo 数据淘汰策略

SFS Turbo HPC型文件系统绑定OBS后端之后，建议配置缓存数据淘汰功能。SFS Turbo会自动释放设定时间内没有访问过的文件数据内容，仅保留文件元数据，数据内

容释放后不占用SFS Turbo文件系统上的存储空间，再次访问该文件时，将重新从OBS中加载文件数据内容。

步骤1 登录**SFS管理控制台**。

步骤2 在文件系统列表中，单击创建的HPC型文件系统名称，进入文件系统详情页面。

步骤3 在“基本信息”页签，设置冷数据淘汰时间。

图 10-6 设置冷数据淘汰时间

----结束

说明

只有已经导出到OBS且满足淘汰时间的数据才会被淘汰。更多内容请参考**管理SFS Turbo文件系统与OBS桶的存储联动**。

10.4.3 训练

10.4.3.1 上传数据至 OBS 并预热到 SFS Turbo 中

上传数据至 OBS

下载ImageNet21K数据集，并上传ImageNet21K数据集至OBS，详细操作指导请参考**上传数据至OBS**。

说明

OBS针对不同场景提供了多种数据上云方案，您可根据数据量、耗时、费用等需求选择适合的方案上传数据至OBS，更多内容请参考**数据上云方案**。

将数据从 OBS 预热到 SFS Turbo 中

SFS Turbo HPC型文件系统绑定OBS桶后，可以使用数据预热功能，以减少后续训练首次访问数据耗时。

训练任务开始前可通过数据预热功能将文件元数据和数据内容全部从OBS导入到SFS Turbo高性能文件存储中。数据预热功能的具体操作可以参考**创建数据导入导出任务接口**或者**管理SFS Turbo文件系统与OBS桶的存储联动**章节的“数据预热功能”内容。

说明

1. 您可通过**查询联动任务详情接口**或者参考**管理SFS Turbo文件系统与OBS桶的存储联动**章节的“任务状态”内容查看导入任务的完成状态。
2. 如果您觉得数据集规模较小或数据集变化不太频繁，不需要通过数据联动来做数据导入导出，您可借助外部工具将数据从OBS迁移到SFS Turbo中，操作指导请参考**OBS和SFS之间的数据迁移**，推荐使用obsutil工具。

上传训练代码

ModelArts Standard开发平台创建训练作业时支持在OBS中配置代码目录，如果代码目录中涉及大量代码文件，建议将代码文件打包成软件包上传到OBS代码目录中，训练作业启动时再将从OBS代码目录下载到本地的软件包进行解压安装，否则大规模训练时可能会存在下载超时导致训练作业启动失败的风险。

10.4.3.2 创建训练任务

基于SFS Turbo共享文件存储创建ModelArts训练任务。

步骤1 登录**ModelArts管理控制台**。

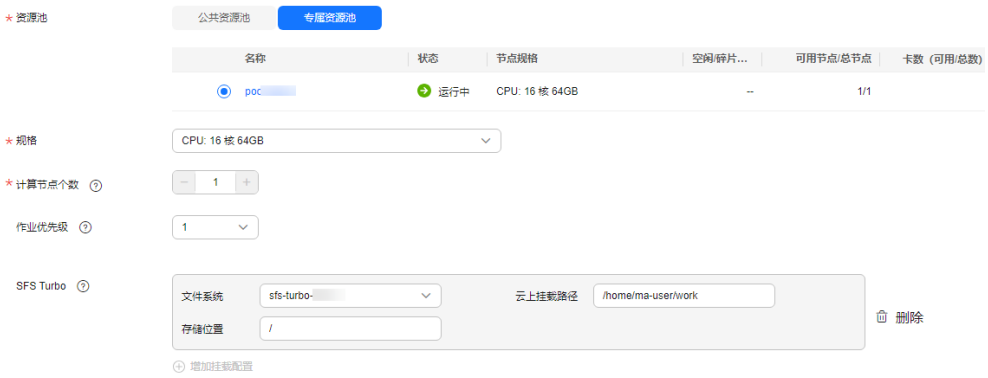
步骤2 在左侧导航栏中选择“训练管理 > 训练作业”，进入“训练作业”列表。

步骤3 单击右上角的“创建训练作业”，进入“创建训练作业”页面，在该页面填写训练作业相关参数信息。

步骤4 填写训练作业相关参数信息，以下配置项请按要求填写，其余参数配置请参考**创建训练作业**根据您的自身情况选择。

- 资源池：专属资源池，选择**创建资源**中创建的ModelArts资源池。
- SFS Turbo：增加挂载配置，选择**创建资源**中创建的SFS Turbo HPC型文件系统。

图 10-7 创建训练作业参数



步骤5 单击“提交”，完成训练作业的创建。

----结束

训练作业创建完成后，后台将自动完成容器镜像下载、代码目录下载、执行启动命令等动作。训练作业一般需要运行一段时间，根据您的训练业务逻辑和选择的资源不同，训练时长将持续几十分钟到几小时不等。要查看训练作业实时情况，您可以前往训练作业列表，查看训练作业的基本情况。

10.4.4 例行维护

SFS Turbo 容量监控及告警

如果SFS Turbo HPC型文件系统存储空间被写满，会影响业务运行，您可以在CES云监控服务上监控SFS Turbo文件系统的容量使用情况，并创建告警规则，当容量使用率超过一定阈值，可以发送邮件、短信等告警到运维人员。当收到容量监控告警时，您需要及时清理SFS Turbo存储空间、或缩短冷数据淘汰时间加速冷数据淘汰、或对SFS Turbo进行空间扩容。详情可参见**SFS Turbo监控指标说明**和**创建告警规则**。

SFS Turbo 性能监控

您可以在CES云监控服务上监控和SFS Turbo文件系统的性能使用情况。当AI算力集群规模变大，大模型参数量变大，导致Checkpoint读加载时间变长时，或训练数据集加载由于存储读写带宽不足导致拖慢AI训练时，您可以对SFS Turbo进行性能扩容，以缩短数据加载时长。详情可参见**SFS Turbo监控指标说明**和**创建告警规则**。

调整 SFS Turbo 数据淘汰策略

操作指导请参考**配置SFS Turbo数据淘汰策略**。

SFS Turbo 容量及性能扩容

当SFS Turbo存储空间不足时，您可以对SFS Turbo存储空间进行容量扩容。

SFS Turbo HPC型是按每TB单位容量来提供一定的带宽吞吐，因此当SFS Turbo HPC性能不足时，需要通过容量扩容来提高性能吞吐。

步骤1 登录**SFS管理控制台**，在左侧导航窗格中选择“SFS Turbo”。

步骤2 在文件系统列表中，单击要扩容的文件系统所在行的“容量调整”或“扩容”，弹出对话框。

图 10-8 SFS Turbo HPC 型容量调整

步骤3 根据业务需要，在“新容量”文本框中重新设置文件文系统的容量。

步骤4 在弹出对话框中确认容量调整信息后，单击“是”。

步骤5 在文件系统列表中查看文件系统调整后的容量信息。

----结束

OBS 性能监控

您可以在CES云监控服务上监控SFS Turbo关联的OBS桶的性能使用情况，SFS Turbo和OBS之间的数据导入导出速度会受OBS服务的读写带宽上限QoS影响，默认是16Gbit/s，如果导入导出速度受到OBS读写带宽上限影响，可**提交工单**联系技术支持人员申请调大OBS服务的读写带宽。

10.5 常见问题

- **可以只使用SFS Turbo HPC型文件系统支撑AI训练吗?**

  当数据规模较小，不存在冷热数据分级降本诉求，又希望能方便快捷的构建AI训练系统时，可以选择只使用SFS Turbo高性能文件存储支撑AI训练。

- **可以基于OBS对象存储支撑AI自动驾驶、大模型训练吗?**

  OBS为容量型存储，在时延、带宽等存储性能上无法满足高性能AI训练，建议使用SFS Turbo HPC型高性能文件系统加速AI训练任务，训练速度加快可以节省AI算力费用。

- **文件系统使用空间不足，可以扩容吗?**

  SFS Turbo文件系统支持在线扩容，扩容过程中挂载文件系统可能失败，建议业务低峰期扩容。

11 结合 EG 事件通知自动处理 OBS 桶中的图片

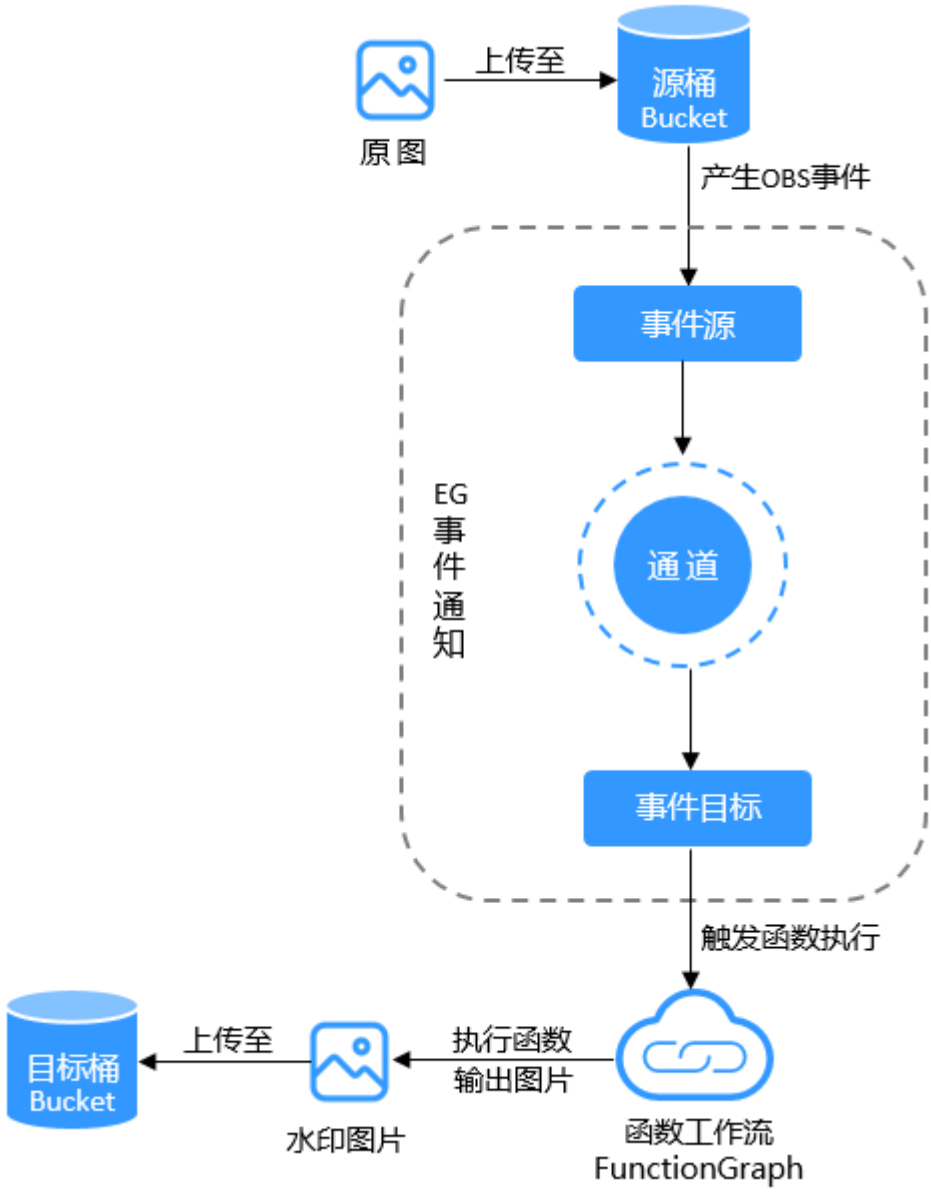
应用场景

根据业务需求，您在OBS桶中执行上传、删除对象等操作后，希望能够自动触发执行后续操作流程，提升效率。

本实践将提供全流程方案，即向源桶中上传图片后，通过EG事件通知功能自动通知下游服务函数工作流FunctionGraph，触发函数为图片添加水印，并将处理后的图片上传至目标桶中。

方案架构

图 11-1 结合 EG 通知自动处理 OBS 桶中图片架构图



结合EG通知自动处理OBS桶中图片的方案如下：

1. 向源桶中上传图片，产生OBS事件作为事件源。
2. EG事件通知（事件网格服务）通过通道将事件源路由至事件目标，从而触发函数执行。
3. 函数工作流（FunctionGraph）执行函数处理图片、输出图片，并将图片上传至目标桶。

方案优势

- 帮助您快速、实时地监控到OBS桶中的对象操作。

- 涉及多流程业务执行时，可通过EG事件通知功能自动触发下游程序执行，节省了人工监控和执行的成本。

约束与限制

- 使用的原图片大小不超过25MB。
- 使用EG事件通知功能，存在一定的延迟，不建议时延敏感类业务场景使用。
- 单桶默认最多同时配置10条EG事件通知策略。
- 新创建的EG事件通知策略将在5分钟之内生效。
- 单桶的多条EG事件通知策略不允许重复，重复的策略会创建失败，即任意对象在发生任意事件时都不能同时匹配两条以上的EG事件通知策略。

  说明

  针对同一事件，如果配置了一条前后缀均为空的EG事件通知策略，则不允许再配置第二条，因为前后缀均为空表示对所有对象生效。

  例如：针对Put事件，已存在一条EG事件通知策略A，定义的前缀是“abcd”，后缀是“.txt”。如果要创建另外一条针对Put事件的EG事件通知策略B，则策略B配置不同前后缀的结果如表11-1所示。

表 11-1 策略 B 前后缀配置场景及结果

策略A前后缀配置	策略B前后缀配置	策略B创建结果	原因
前缀：abcd 后缀：.txt	前缀：abcd 后缀：.txt	失败	前后缀相同
	前缀：abcd 后缀：空	失败	前缀相同，B的后缀包含A的
	前缀：ab 后缀：xt	失败	B的前缀包含A的，B的后缀包含A的
	前缀：abef 后缀：.txt	成功	前缀不同，后缀相同
	前缀：abcd 后缀：.mp4	成功	前缀相同，后缀不同

资源和成本规划

表 11-2 资源规划

资源	资源名称	资源说明	数量	费用
OBS桶	piccomp	上传图片的源桶。 您需要在OBS控制台创建源桶。	1	根据图片占用的存储空间收费，具体请参见存储费用。

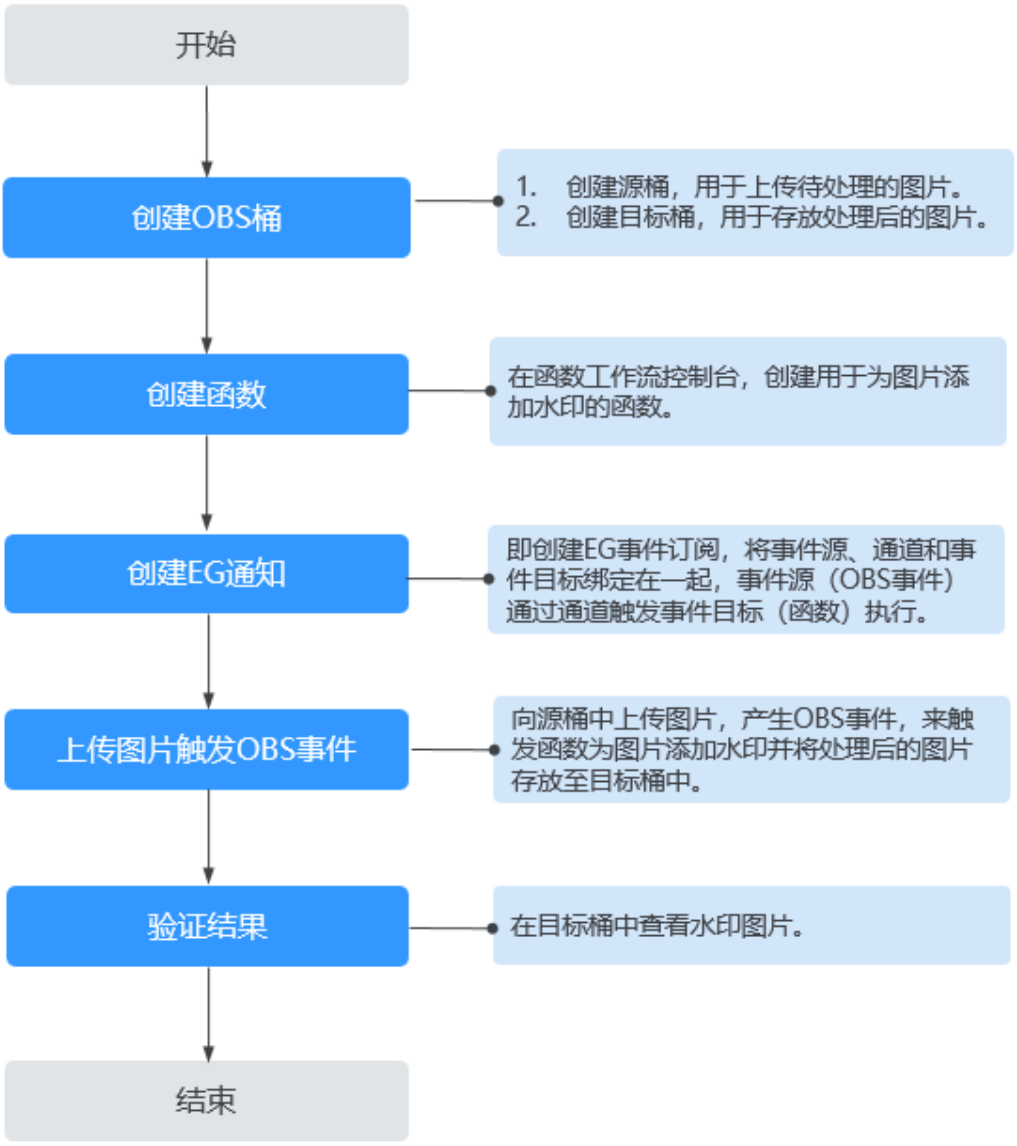
资源	资源名称	资源说明	数量	费用
	piccomp-output	图片处理后存放的目标桶。 您需要在OBS控制台创建目标桶。	1	
图片	example.jpg	用于添加水印的原图片。 您需要提前准备好需要添加水印的图片。	1	-
函数	FG_Test	为图片添加水印的函数。 您需要在函数工作流（FunctionGraph）控制台创建函数。	1	根据请求次数、执行时间、执行次数等收费，具体请参见**函数工作流计费**。
EG事件订阅	subscription-obs	事件订阅将事件源、通道和事件目标绑定在一起，事件源（OBS事件）通过通道触发事件目标（函数）执行。 您需要在OBS控制台的“事件通知”页面创建EG事件订阅。	1	根据请求次数收费，具体请参见**事件网格计费**。

前提条件

账号或IAM用户已具有Tenant Administrator权限。给账号授权请参见**给IAM用户授权**。

操作流程

图 11-2 为图片添加水印流程



实施步骤

步骤一：创建 OBS 源桶和目标桶

桶是OBS中用于存储对象的容器。本示例中，上传的图片存储在源桶，添加水印后的图片存储在目标桶。如果您已有源桶和目标桶，请跳至**步骤二：创建函数**。

说明

由于归档存储和深度归档存储类别的桶，需要先手动恢复才能下载和通过URL访问对象，因此本实践暂不支持使用归档存储和深度归档存储类别的桶。

步骤1 登录控制台，进入**创建桶**页面。

步骤2 在创建桶页面，按照下表说明配置相关参数，其他参数保持默认。表中“示例”仅供参考，您也可以根据业务实际情况自行设置。

关于更多参数配置请参见**创建桶**。

参数	示例	描述
区域	**华北-北京四**	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。 **须知** 目标桶和源桶必须在同一区域。
桶名称	**piccomp**	桶的名称。桶创建成功后，不支持修改名称。 桶名称命名规则如下： ● 全局唯一，不能与已有的任何桶（包含其他账号创建的桶）名称重复。删除桶后，需等待30分钟才能创建同名桶或并行文件系统。 ● 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。
数据冗余存储策略	**多AZ存储**	选择数据存储在多个可用区或单个可用区。 多AZ存储：数据存储至同区域内的多个可用区（AZ），可靠性更高，同时存储成本相对更高。 桶创建成功后，不支持更改数据冗余存储策略。 多AZ存储桶不支持为桶设置归档存储类别和深度归档存储类别。
存储类别	**标准存储**	桶的存储类别。不同的存储类别可以满足客户业务对存储性能、成本的不同诉求。 标准存储：适用于有大量热点文件或小文件，且需要频繁访问（平均一个月多次）并快速获取数据的业务场景。 更多存储类别详情请参见**存储类别**。
桶策略	**私有**	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。
企业项目	**default**	将桶加入到企业项目中统一管理。如无特殊的企业项目划分和管理需求，此处可直接选择默认企业项目“default”。 如果您想要了解更多关于如何通过企业项目管理OBS桶，具体请参见**创建桶**中的“企业项目”参数说明。

步骤3 单击页面右下角的“立即创建”，并确认提示信息。

创建完成后，将会出现创建成功弹窗，确认后在桶列表页即可看到已创建的桶。

步骤4 按照以上步骤再创建目标桶piccomp-output。

----结束

步骤二：创建函数

在OBS源桶中上传图片后，通过EG事件订阅触发函数执行，因此需要创建图片打水印函数。

步骤1 单击页面左上角的  ，选择“计算 > 函数工作流 Function Graph”，进入函数工作流控制台。

步骤2 在左侧导航栏选择“函数 > 函数列表”。

步骤3 单击“创建函数”。

步骤4 在“创建函数”页面，按照如下设置参数，其他参数保持默认。

关于更多参数配置请参见**创建函数**。

表 11-3 函数参数说明

参数	示例	描述
选择创建方式	**创建空白函数**	选择创建函数的方式。 此处选择“创建空白函数”，即从头开始自定义创建函数。
函数类型	**事件函数**	选择触发函数执行的方式。 事件函数，即通过触发器来触发函数执行。
区域	**华北-北京四**	选择要部署函数代码的区域。 此处请选择和源桶、目标桶均相同的区域。
函数名称	**FG_Test**	函数名称，命名规则如下： • 可包含字母、数字、下划线和中划线。 • 以大/小写字母开头，以字母或数字结尾。 • 长度不超过60个字符。
企业项目	**default**	将函数加入到企业项目中统一管理。 如无特殊的企业项目划分和管理需求，此处可直接选择默认企业项目“default”。关于企业项目的使用，具体请参见**使用企业项目**。

参数	示例	描述
委托名称	**OBS_Agency**	用于委托函数工作流服务去访问其他其他云服务。 此处需要为函数工作流服务授予OBS的管理员权限（OBS Administrator），授权范围选择“所有资源”。 创建委托请参见**委托其他云服务管理资源**。
运行时	**Python 3.9**	选择用来编写函数的语言。

图 11-3 创建函数

步骤5 单击“创建函数”，完成函数的创建。

步骤6 在函数列表中，单击函数名称，进入函数详情页。

步骤7 上传代码文件。本示例中使用的样例代码文件请参见**使用函数为图片添加水印**。

1. 单击“代码”页签右侧的“上传自”，选择“Zip文件”。
2. 在“上传Zip文件”弹窗，单击“添加文件”，选择下载的样例代码文件“watermark.zip”，并单击“确定”。

   在代码区域产生了一个index.py文件，index.py为函数执行的入口文件。文件中的关键参数说明如下：

   - obs_output_bucket：添加水印后的图片存放的OBS桶（本示例中的目标桶）。

- obs_region：目标桶所在的区域编号。

步骤8 添加代码依赖包。样例代码依赖pillow包，需要通过依赖包的形式进行引入。

1. 在“代码”页签底部，单击“添加依赖包”。
2. 在右侧的“选择依赖包”弹窗，添加公共依赖包“pillow-7.1.2”，并单击“确定”。

步骤9 设置环境变量。用来配置图片添加水印后存放的目标桶信息。

1. 切换至“设置”页签，单击左侧导航列表的“环境变量”。
2. 单击“编辑环境变量”，在右侧弹窗单击“添加环境变量”。
3. 添加以下环境变量，并单击右下角的“确定”。

表 11-4 环境变量

键	值	说明
obs_output_bucket	piccomp-output	添加水印后的图片存放的OBS目标桶。 值为**步骤一：创建OBS源桶和目标桶**中创建的目标桶名称。
obs_region	cn-north-4	目标桶所在的区域编号。 更多区域编号请参见**地区和终端节点**。

说明

键“obs_output_bucket”和“obs_region”为**7**中样例代码里面目标桶的关键参数。

图 11-4 设置环境变量

----结束

步骤三：创建 EG 通知

使用EG通知来作为事件触发器，触发函数执行。即创建EG事件订阅，将事件源、通道和事件目标绑定在一起，事件源（OBS事件）通过通道触发事件目标（函数）执行。

步骤1 单击页面左上角的，选择“存储 > 对象存储服务 OBS”，进入桶列表页面。

步骤2 单击源桶名称，进入对象列表页。

步骤3 在左侧导航栏选择“数据管理 > 事件通知”。

步骤4 在“EG通知”页签，单击“创建”，进入EG事件订阅详情页。

步骤5 修改订阅名称。

单击上方订阅名称旁的，在“修改订阅”弹窗，修改订阅名称后单击“确定”。本示例中订阅名称修改为“subscription-obs”。

步骤6 配置事件源。

1. 单击“事件源”，按照如下设置参数，其他参数保持默认。
   关于更多参数配置请参见**创建事件订阅**。

表 11-5 事件源参数说明

参数	示例	描述
选择提供方	**云服务**	选择事件源提供方。 云服务，即华为云服务作为事件源提供方。
事件源	**OBS应用事件源**	选择云服务事件源。 OBS应用事件源，即通过操作OBS桶内对象的特定行为来产生事件源。
桶	**piccomp**	选择产生事件源的OBS桶，即本示例中的源桶。
事件类型	- **OBS:DWR:ObjectCreated:PUT** - **OBS:DWR:ObjectCreated:POST** - **OBS:DWR:ObjectCreated:COPY** - **OBS:DWR:ObjectCreated:CompleteMultipartUpload**	选择产生事件源的OBS操作。 - **OBS:DWR:ObjectCreated:PUT**：通过页面或Put请求创建或覆盖桶对象。 - **OBS:DWR:ObjectCreated:POST**：使用Post请求创建或覆盖桶对象。 - **OBS:DWR:ObjectCreated:COPY**：使用Copy请求创建或覆盖桶对象。 - **OBS:DWR:ObjectCreated:CompleteMultipartUpload**：通过页面或API请求合并分段任务。

图 11-5 设置事件源

2. 单击“确定”，完成事件源配置。

步骤7 配置事件目标。

1. 单击“事件目标”，按照如下设置参数，其他参数保持默认。
   关于更多参数配置请参见**创建事件订阅**。

表 11-6 事件目标参数说明

参数	示例	描述
选择提供方	**云服务**	选择事件目标提供方。 云服务，即华为云服务作为事件目标提供方。
事件目标	**FunctionGraph（函数计算）**	选择云服务事件目标。 FunctionGraph（函数计算），即由函数工作流服务执行特定操作。
函数	**FG-Test**	选择要执行的函数。 本示例中选择已创建的为图片添加水印的函数FG-Test。
委托	**EG_TARGET_AGENCY**	用于委托事件网格服务EG去访问其他云服务。 本示例中需要委托EG去访问函数工作流服务。如无委托，可单击旁边的“创建委托”，将会自动创建名为“EG_TARGET_AGENCY”的委托。

参数	示例	描述
类型	**透传**	事件网格EG对事件参数进行转换，通过JSONPath从事件中提取参数，然后把这些参数路由到事件目标。
参数	**如下所示。**	需要转换的参数。
模板	**如下所示。**	自定义一个包含所需变量的模板，事件网格EG按照模板定义的形式进行转换。

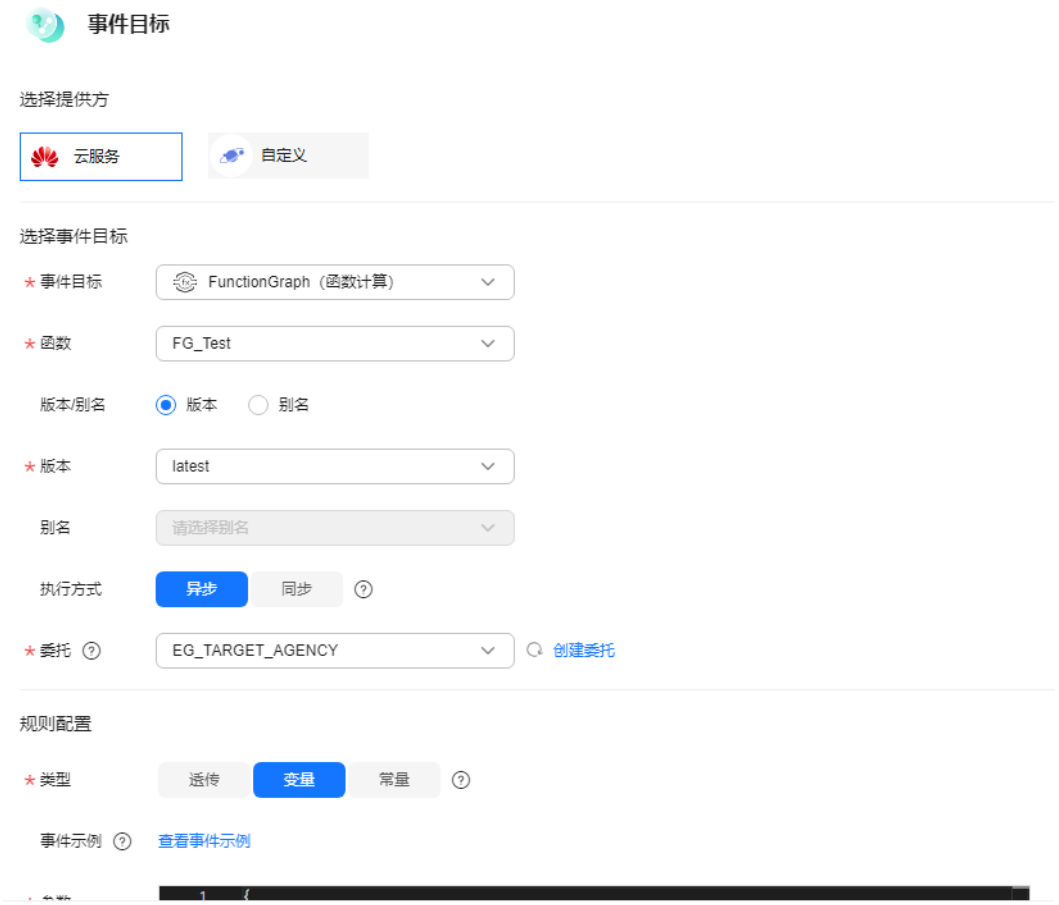
本示例中，“参数”请填写如下内容：

```
{
  "eventVersion": "$.data.eventVersion",
  "eventTime": "$.data.eventTime",
  "requestParameters": "$.data.requestParameters.sourceIPAddress",
  "configurationId": "$.data.obs.configurationId",
  "eTag": "$.data.obs.object.eTag",
  "sequencer": "$.data.obs.object.sequencer",
  "key": "$.data.obs.object.key",
  "size": "$.data.obs.object.size",
  "arn": "$.data.obs.bucket.arn",
  "name": "$.data.obs.bucket.name",
  "ownerIdentity": "$.data.obs.bucket.ownerIdentity.ID",
  "eventRegion": "$.data.eventRegion",
  "eventName": "$.type",
  "userIdentity": "$.data.userIdentity.ID"
}
```

本示例中，“模板”请填写如下内容：

```
{
   "Records": [
      {
         "eventVersion": "${eventVersion}",
         "eventTime": "${eventTime}",
         "requestParameters": {
            "sourceIPAddress": "${requestParameters}"
         },
         "b1": {
            "configurationId": "${configurationId}",
            "object": {
               "eTag": "${eTag}",
               "sequencer": "${sequencer}",
               "key": "${key}",
               "size": "${size}"
            },
            "bucket": {
               "arn": "${arn}",
               "name": "${name}",
               "ownerIdentity": {
                  "PrincipalId": "${ownerIdentity}"
               }
            }
         },
         "eventRegion": "${eventRegion}",
         "eventName": "${eventName}",
         "userIdentity": {
            "principalId": "${userIdentity}"
         }
      }
   ]
}
```

图 11-6 设置事件目标



2. 单击“确定”，完成事件目标配置。

步骤8 单击页面右上角的“保存”。

----结束

步骤四：上传图片触发 OBS 事件

向已创建的OBS源桶中上传一张图片，产生OBS事件，使得EG通知去触发函数执行：为上传的图片添加水印，并将处理后的图片存储至已创建的目标桶中。

步骤1 单击页面左上角的，选择“存储 > 对象存储服务 OBS”，进入桶列表页面。

步骤2 单击源桶名称，进入对象列表页。

步骤3 单击搜索框上方的“上传对象”。

步骤4 在“上传对象”弹窗，单击“添加文件”，选择要上传的图片，其他参数保持默认即可。

关于更多参数配置请参见**上传对象**。

步骤5 单击“上传”。

在对象列表页可以看到已上传对象，表示上传成功。

图 11-7 上传对象成功

----结束

步骤五：验证结果

在目标桶中查看图片是否已添加水印。

步骤1 在桶列表页，单击目标桶名称。

步骤2 在对象列表页，单击添加水印后的图片名称。

步骤3 切换至“图片预览”页签，查看图片已添加水印。

图 11-8 查看水印图片

----结束

12 基于全站加速 WSA 的 OBS 传输加速最佳实践

应用场景

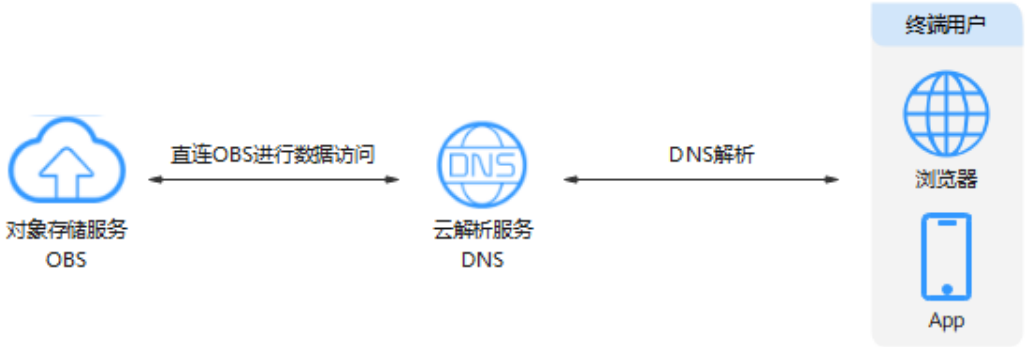
- 远距离数据传输：

  如果客户端所在区域与数据存储区域相距较远，那么当客户端访问数据时，可能会因为传输距离远引发访问延时长、不稳定等问题，例如全球性的论坛网站、在线协同办公平台等，远距离传输造成的长时延会影响客户上传下载数据的体验。基于全站加速（Whole Site Acceleration，WSA）的传输加速方案可以让全球各地的客户极大地提升上传和下载速度，让不同地域的用户都能有很好的访问体验。
- 动态文件下载：

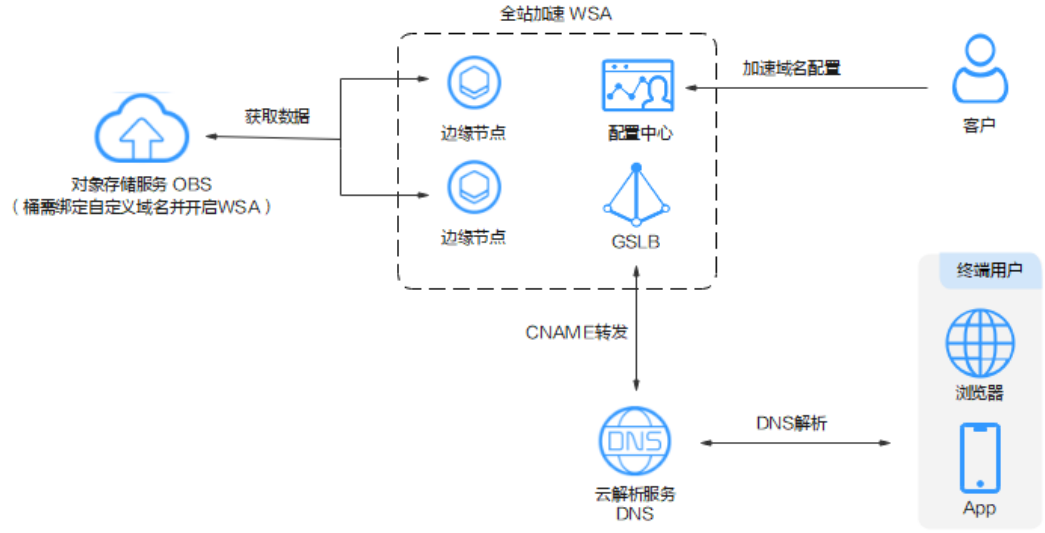
  与其他加速技术相比，WSA不仅加速静态资源，还适用于加速各行业动静态内容混合、含较多动态资源请求（如asp、jsp、php等格式的文件）的源站应用服务。除了常见的网站页面加速，WSA 还能为各种应用类型提供加速服务，包括但不限于Web应用、移动应用、API接口、WebSocket应用等。

方案架构

开启WSA前，客户端请求经过DNS解析后，通过直连网络上传下载OBS。



开启WSA后，客户端请求经过DNS解析后，DNS服务器会通过CNAME方式将域名请求重定向到WSA服务。WSA通过一组预先定义好的策略（如内容类型、地理区域、网络负载状况等），静态内容从当时能够最快响应用户的边缘节点就近获取，动态内容通过动态加速技术避开网络拥堵路由，智能选择较优路由回源获取，使用户可以以最快的速度获得网站内容。



方案优势

加速范围全面：

- 动静态内容一体化加速：传统的CDN技术大多只能加速静态资源，如图片、样式表、脚本等。而WSA不仅可以对静态资源进行高效缓存和分发，还能针对动态内容，如动态网页、API接口、实时数据等进行加速。
- 多类型应用加速支持：除了常见的网站页面加速，WSA还能为各种应用类型提供加速服务，包括但不限于Web应用、移动应用、API接口、WebSocket应用等。

智能优化能力强：

- 智能路由选择：WSA能够根据用户的地理位置、网络运营商、网络质量、节点负载等多种因素，实时动态地计算出到源站的最优访问路径。相比传统的基于DNS的就近访问原则，WSA的智能路由可以更精准地避开网络拥堵、故障等问题，提高数据传输效率。
- 协议优化：通过自研的协议优化算法，WSA可以降低网络传输中的延迟和卡顿率，尤其在端侧弱网接入场景下，能够有效改善丢包、时延等问题，提升用户在各种网络环境下的访问体验。

资源和成本规划

表 12-1 资源和成本规划

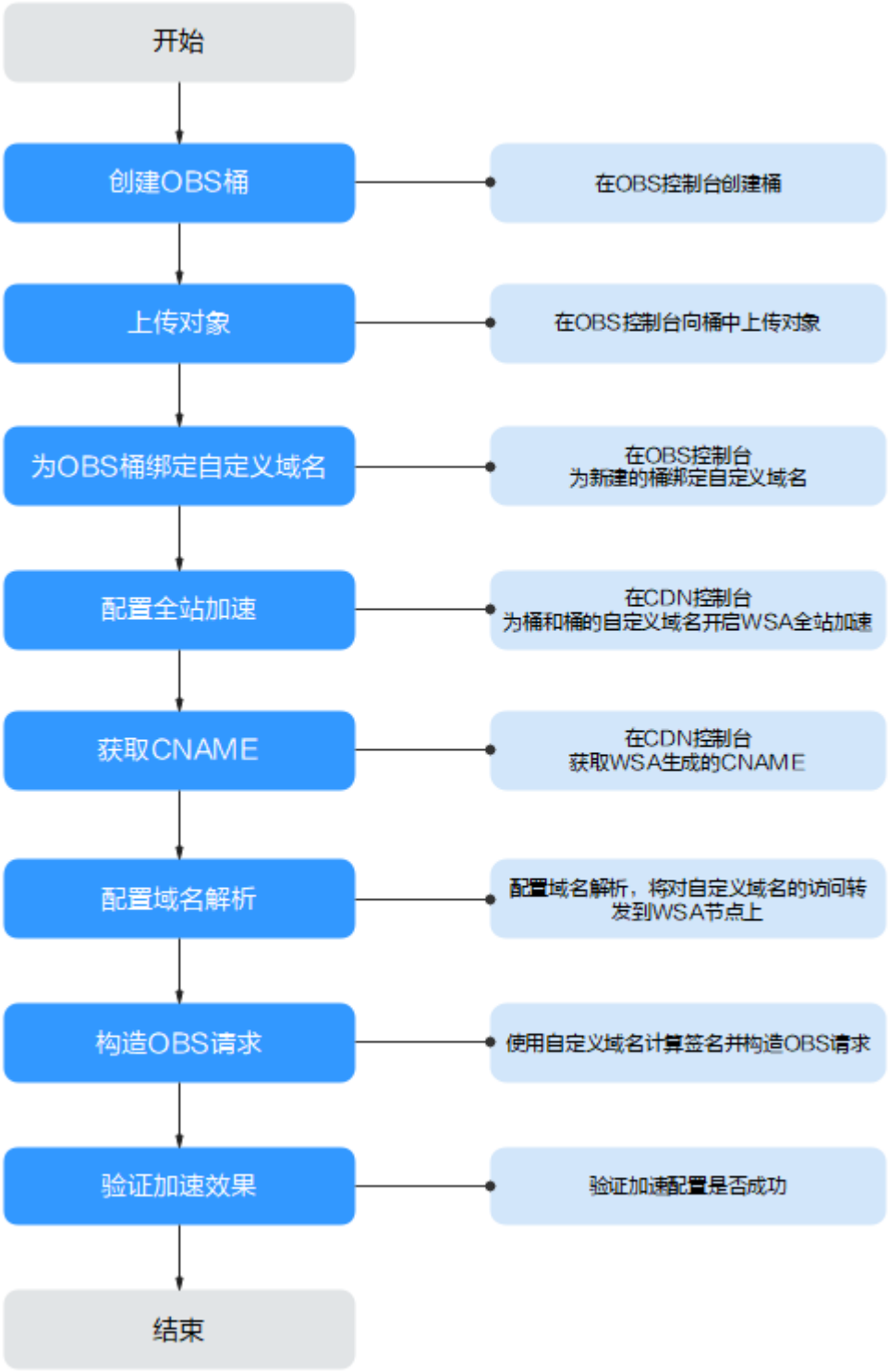
资源	资源说明	数量	费用
全站加速WSA	提供全站加速功能，加速数据上传下载。	NA	基础服务计费：流量或带宽费用，该最佳实践默认按流量阶梯计费，您也可以在WSA服务中购买预付费流量包，更多计费详情请参见**价格详情**。 增值服务计费：全站加速请求数费用，详情请参见**价格详情**。
OBS桶	OBS桶用于存放用户上传和下载的数据，桶存储类别为“标准存储”。	1	存储费用：按照OBS存储数据所占用的存储空间容量大小收费。 流量费用：WSA回源OBS时会产生公网流出费用，按需计费，版本为3.0以上的桶且以“OBS桶域名”形式接入WSA可购买OBS回源流量包抵扣。
网站域名	绑定在对象桶上的自定义域名，用户通过访问该域名来访问桶。	1	域名注册和管理相关费用，不同厂商的收费标准不同。

约束限制

- 对于使用中国大陆节点服务器提供互联网信息服务的用户，绑定服务器的域名需要在取得备案号后才能进行访问。
- 您必须是桶拥有者或拥有设置桶的自定义域名的权限，才能设置桶的自定义域名信息。建议使用IAM或桶策略进行授权，如果使用IAM则需授予obs:bucket:PutBucketCustomDomainConfiguration权限，如果使用桶策略则需授予PutBucketCustomDomainConfiguration权限。相关授权方式介绍可参见**OBS权限控制概述**，配置方式详见**使用IAM自定义策略**、**自定义创建桶策略**。

操作流程

图 12-1 基于全站加速 WSA 的 OBS 传输加速最佳实践操作流程

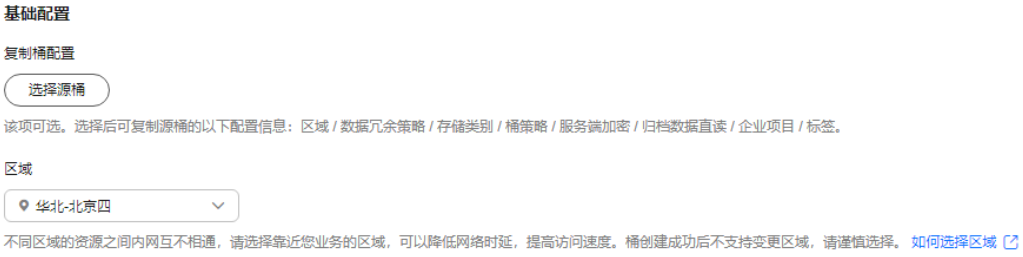


实施步骤

步骤一：在 OBS 控制台创建 OBS 桶

步骤1 登录控制台，进入**创建桶**页面。

步骤2 设置“基础配置”。



参数	示例	说明
区域	**华北-北京四**	桶所属区域。桶创建成功后，不支持变更区域，请谨慎选择。

步骤3 设置“桶配置”。其他参数保持默认，可在桶创建后修改。

参数	示例	说明
桶名称	**wsa-example-bucket**	桶的名称。桶创建成功后，不支持修改名称。 桶名称命名规则如下： ● 全局唯一，不能与已有的任何桶（包含其他账号创建的桶）名称重复。删除桶后，需等待30分钟才能创建同名桶或并行文件系统。 ● 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。
数据冗余存储策略	**多AZ存储**	● 多AZ存储：数据存储至同区域内的多个可用区（AZ），可靠性更高，同时存储成本相对更高。 ● 单AZ存储：数据仅存储在单个可用区（AZ），成本更低。 桶创建成功后，不支持更改数据冗余存储策略。
存储类型	**标准存储**	桶的存储类别。不同的存储类别可以满足客户业务对存储性能、成本的不同诉求。 ● 标准存储：适用于有大量热点文件或小文件，且需要频繁访问（平均一个月多次）并快速获取数据的业务场景。 ● 低频访问存储：适用于不频繁访问（平均一年少于12次），但需要快速获取数据的业务场景。 **说明** 归档与深度归档存储不支持配置WSA全站加速。 更多详情请参见**存储类别**。
桶策略	**私有**	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。 ● 复制桶策略：复制源桶的桶策略。当且仅当您选择了源桶时，该选项处于可选状态。

参数	示例	说明
企业项目	**default**	将桶加入到企业项目中统一管理。如无特殊的企业项目划分和管理需求，此处可直接选择默认企业项目“default”。 如果您想要了解更多关于如何通过企业项目管理OBS桶，具体请参见**创建桶**中的“企业项目”参数说明。

步骤4 单击页面右下角的“立即创建”，并确认提示信息。

创建完成后，将会出现创建成功弹窗，确认后在桶列表页即可看到已创建的桶。

----结束

步骤二：在 OBS 控制台向桶中上传对象

步骤1 在桶列表页面，单击已创建好的桶名称，进入“对象”页面。

步骤2 单击搜索框上方的“上传对象”。

步骤3 将本地文件拖拽至“上传对象”区域框内来添加对象。

也可以通过单击区域框内的“添加文件”，选择本地文件进行添加。

步骤4 其他参数保持默认，单击“上传”。

右侧自动弹出任务中心页面，可在任务中心查看对象上传状态。上传成功的对象将在对象列表中展示。

----结束

步骤三：在 OBS 控制台为桶绑定自定义域名

步骤1 在左侧导航栏选择“域名管理”，进入“域名管理”界面。

图 12-2 域名管理界面

步骤2 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（此处以“**testwsa.com**”为例），然后单击“确定”。域名后缀目前支持的范围为2~6个英文大小写字母。如：.com、.cn。

配置自定义域名

说明

在配置自定义域名后，配置WSA之前，OBS会暂时将桶域名作为自定义域名的CNAME，配置WSA后CNAME会变更为WSA生成的CNAME，最终在DNS上配置的CNAME为WSA生成的CNAME。

----结束

步骤四：在 CDN 控制台配置全站加速

步骤1 登录CDN控制台，单击左侧“域名管理”，进入域名管理页面。

步骤2 在域名管理页面单击“添加域名”，进入添加域名页面。

步骤3 在添加域名页面，配置域名参数，其他参数保持默认：

参数	示例	说明
服务范围	**中国大陆**	• 全球：全球各地用户的访问都会调度到用户附近最优的CDN节点，加速域名需要到工信部备案，详见**备案流程**。 • 中国大陆：所有用户的访问都会调度到中国大陆的节点，加速域名需要到工信部备案，详见**备案流程**。 • 中国大陆境外：所有用户的访问都会调度到中国大陆境外的节点，此时不需要到工信部备案。
加速域名	**testwsa.com**	需要加速的域名，请填写可以正常使用的域名。 • 域名长度不能超过200个字符，支持大小写字母、数字、“-”、“.”“*”，“*”必须是首字符，首字符不能是“-”或“.”。 • 域名单节点长度不超过63个字符，即：***.***.com中，***的字符数最多63个。
企业项目	**default**	将加速域名加入到企业项目中统一管理。如无特殊的企业项目划分和管理需求，此处可直接选择默认企业项目“default”。
业务类型	**全站加速**	适用于各行业动静态内容混合，含较多动态资源请求（如asp、jsp、php等格式的文件）的网站。 **说明** 如果您未开通全站加速服务，界面将提示您开通WSA服务： 1. 单击“前往开通”。 2. 选择计费方式，勾选服务声明，单击“立即开通”即可开通WSA服务。
回源方式	**HTTP**	配置CDN节点回源时采用的协议，可选： • HTTP：CDN采用HTTP协议回源。 • HTTPS：CDN采用HTTPS协议回源（请确保源站支持HTTPS访问），如需使用请**提交工单**联系技术人员开通。 • 协议跟随：回源协议跟客户端访问协议一致，例：客户端以HTTPS协议访问CDN，CDN也将采用HTTPS协议回源，如需使用请**提交工单**联系技术人员开通。

步骤4 在源站配置模块单击“添加源站”，为域名添加源站：

参数	示例	说明
源站类型	**源站域名**	• 源站IP：使用IP作为源站地址时，CDN节点回源时直接访问该IP地址。支持配置IPv4，暂不支持IPv6。 • 源站域名：支持配置域名作为源站，CDN节点回源时直接访问该域名。 **说明** – 域名首字符为字母或数字，支持大小写字母、数字、“-”、“.”，长度不能超过255个字符。 – 域名单节点长度不超过63个字符，即：***.***.com中，***的字符数最多63个。
源站地址	**wsa-example-bucket.obs.cn-north-4.myhuaweicloud.com**	CDN节点回源时访问的地址，此处填写桶域名。
回源HOST	**testwsa.com**	回源HOST是CDN回源过程中，在源站访问的站点域名，即HTTP请求头中的HOST信息。配置回源HOST后，CDN在回源过程中会根据HOST信息去对应站点获取资源，此处填写加速域名。

步骤5 单击“确定”，完成源站添加。

步骤6 源站添加完成后，单击页面左下方“确定”按钮，完成域名添加。

----结束

步骤五：在 CDN 控制台获取 WSA 生成的 CNAME

步骤1 在**CDN控制台域名管理页面**，单击**步骤四**中添加的域名，进入域名详情页。

步骤2 在“基本配置”页签，复制WSA生成的CNAME，这个CNAME将会在**步骤六**中用到。

----结束

步骤六：在 DNS 控制台配置域名解析

如果您已成功添加加速域名，系统会自动为您的加速域名分配对应的CNAME域名。加速域名在WSA服务中获得的CNAME域名不能直接访问，必须在加速域名的域名服务商处配置CNAME记录，将加速域名指向CNAME域名，访问加速域名的请求才能转发到WSA节点上，达到加速效果。

不同DNS服务商的CNAME配置方式不同，此处以华为云云解析服务为例。其他DNS服务商的CNAME配置方法可参考**配置CNAME域名解析**。

步骤1 登录**DNS控制台**。

步骤2 在左侧菜单栏中，选择“公网域名”，进入公网域名列表页面。

步骤3 单击“域名”列的域名名称。本实践中对应的域名为“testwsa.com”。

步骤4 单击“添加记录集”，进入“添加记录集”页面。

步骤5 根据界面提示填写参数配置，参数信息如**表12-2**所示，下表中未提到的参数可保持默认值：

表 12-2 参数说明

参数	示例	说明
记录类型	**CNAME-将域名指向另外一个域名**	记录集的类型，此处为CNAME类型。

参数	示例	说明
主机记录	*	解析域名的前缀。 例如创建的域名为“example.com”，其“主机记录”设置包括： ● www：用于网站解析，表示解析的域名为“www.example.com”。 ● 空：用于网站解析，表示解析的域名为“example.com”。 ● 主机记录置为空，还可用于为空头域名“@”添加解析。 ● abc：用于子域名解析，表示解析的域名为“example.com”的子域名“abc.example.com”。 ● mail：用于邮箱解析，表示解析的域名为“mail.example.com”。 ● *：用于泛解析，表示解析的域名为“*.example.com”，匹配“example.com”的所有子域名。
值	**testwsa.com.xxxxxxxx.c.cdnhwc1.com**	需指向的域名。开启WSA加速后，该值为**步骤五**中获取的WSA分配的CNAME域名。

步骤6 单击“确定”，完成添加。

步骤7 验证CNAME配置是否生效。

打开Windows操作系统中的cmd程序，输入如下指令：

```
nslookup -qt=cname 桶绑定的自定义域名
```

本实践中桶绑定的自定义域名为“testwsa.com”。如果回显CDN分配的CNAME域名，则表示CNAME配置已经生效。

----结束

步骤七：构造 OBS 请求

公开桶直接获取对象URL即可访问桶内资源，详情参见**匿名用户通过URL访问对象**。私有桶请使用自定义域名计算签名或初始化SDK客户端：

- 如果您直接调用OBS API访问桶中资源，那么在计算API签名时，请将CanonicalizedResource中的桶名替换为自定义域名，详情参见**OBS签名机制**。
- 如果您使用OBS SDK访问桶中的资源，那么在初始化SDK客户端时，请将endpoint设置为自定义域名的endpoint，例如“http://testwsa.com”，并为SDK客户端配置自定义域名相关参数，如**表3**所示。

表 12-3 SDK 客户端自定义域名相关参数

语言	Java	Python	C	Go	BrowserJS	Android	iOS	PHP	Node.js
需要设置的参数	cname	is_cname	useCname host_name	cname	is_cname	cname	OBSDomainMode Custom	is_cname	is_cname

步骤八：验证加速效果

配置完成后，访问桶内文件，如果文件能成功访问，则表示加速配置成功。