

阿里云云计算ACP认证培训

对象存储OSS

课程目标

学习完本课程后，你将能够：

1. 了解对象存储在飞天体系中的位置
2. 了解块存储与对象存储的区别
3. 了解对象处处的基本构成等
4. 掌握如何使用OSS对象存储

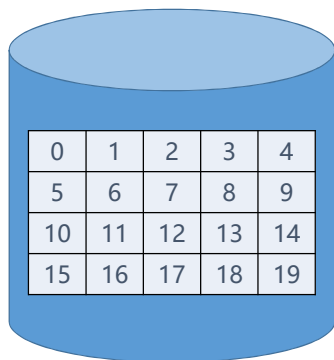
目录

1. 对象存储的基本概念和组成

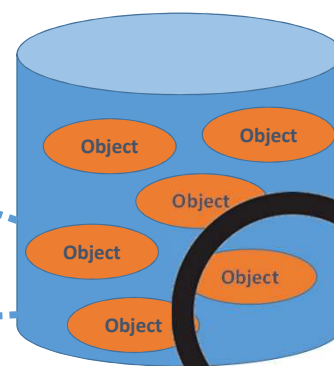
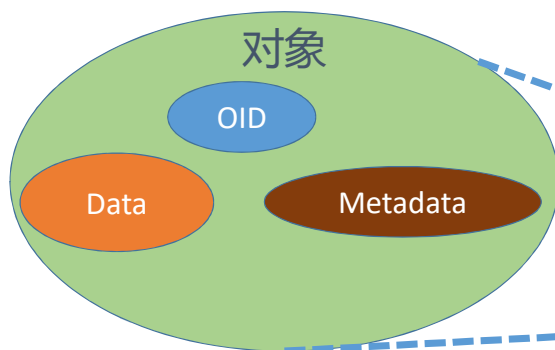
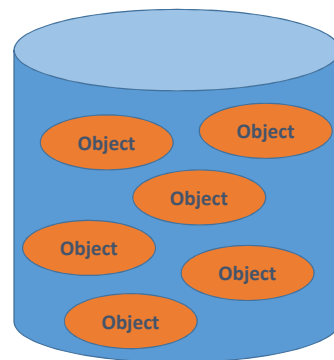
2. 对象存储的应用

对象的构成

基于块的磁盘

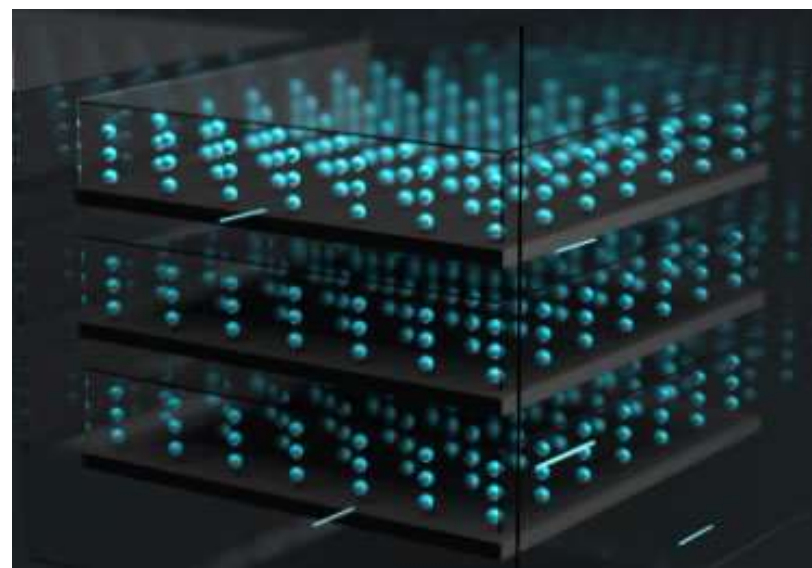


基于对象的磁盘



什么是对象存储

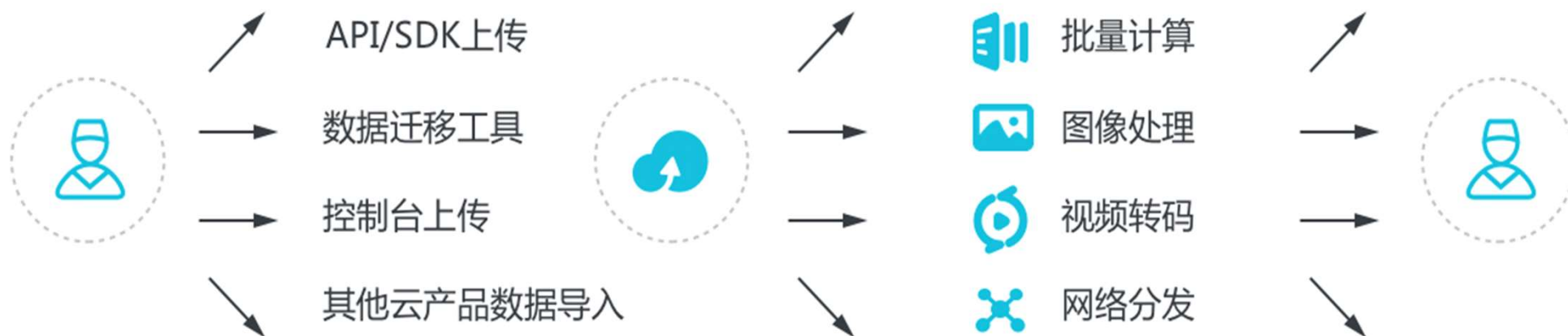
- 阿里云对象存储服务（Object Storage Service，简称OSS），是阿里云提供的海量、安全、低成本、高可靠的云存储服务。
- 它具有与平台无关的RESTful API接口，能够提供99.999999999%（11个9）的数据可靠性和99.99%的服务可用性。
- 您可以在任何应用、任何时间、任何地点存储和访问任意类型的数据。



对象存储OSS概述

易用性

简单易用，便于管理，深度集成数据处理服务



对象存储OSS概述

高可靠

为数据持久存储提供稳定保障

提供跨区域复制功能和灾备方案，支持数据自动备份在不同城市，实现异地容灾能力

异地容灾

多份副本

多份副本保存，有效应对各类硬件故障

基于99.99%可用性设计

冗余架构

OSS全冗余的基础架构，消除单点隐患，保障服务的高可用性

对象存储OSS概述

强安全

多重访问控制细粒度的授权管理



Bucket|Object权限控制



Access ID和请求签名

访问控制



VPC网络链路层访问控制



RAM&STS 主子账号授权

对象存储OSS概述

低成本

数据按照冷热分层提供最具性价比的存储方式

OSS对象存储

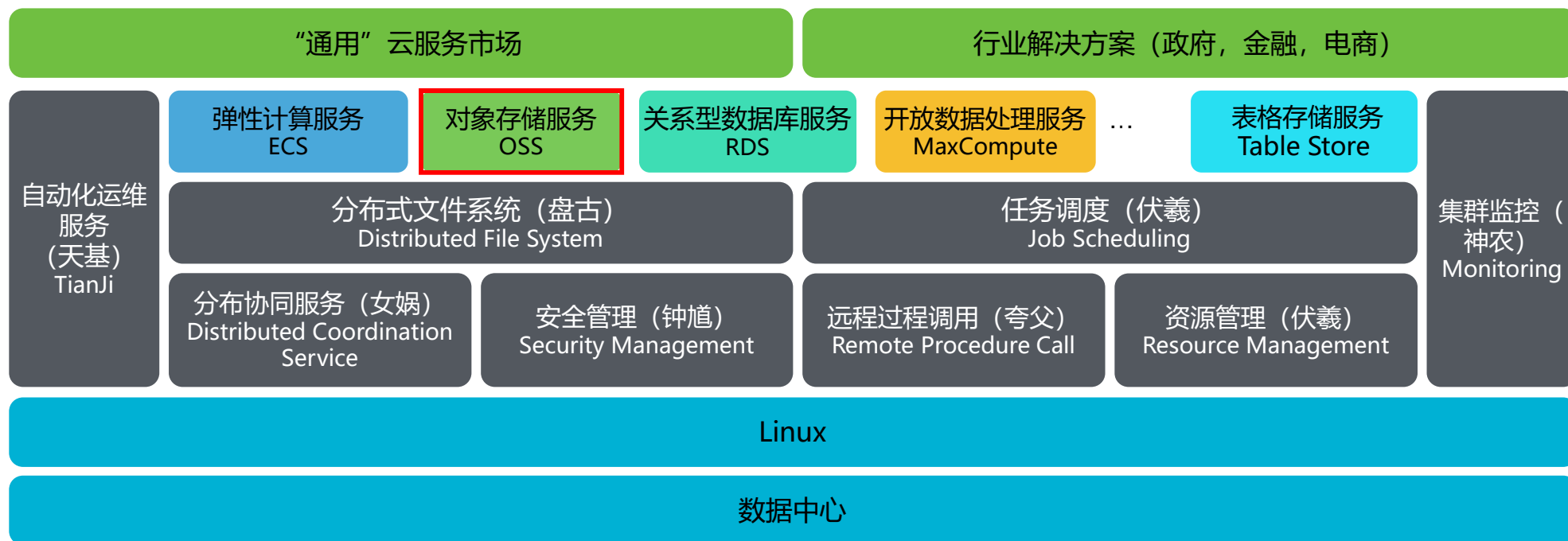
- 用相比自建存储降低25%~75%的成本，提供更加稳定安全可靠的数据保障
- 三种存储类型，不同数据冷热，追求最极致的TCO
- 多线带宽接入，上行流量免费
- 完全托管的存储模式，0成本运维

传统存储

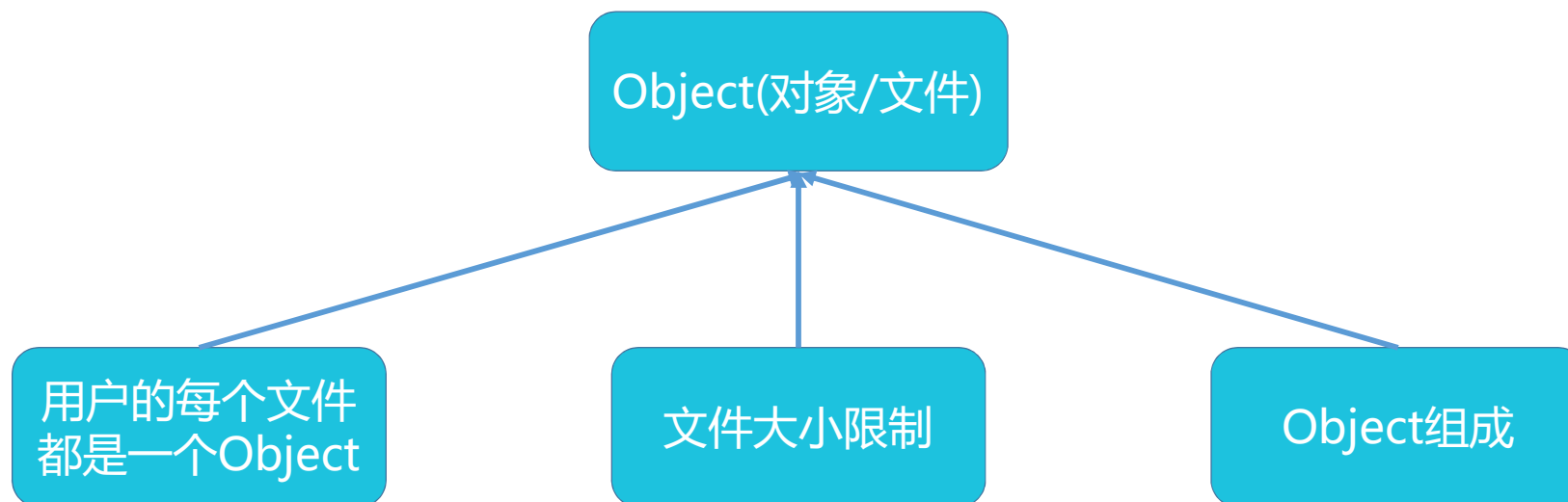
- 一次性投入高，资源利用率很低
- 存储受硬盘容量限制，需人工扩容
- 单线或双线接入速度慢，有带宽限制，峰值时期需人工扩容
- 需专人运维，成本高

OSS在飞天架构中的位置

OSS是阿里云重要的组成部分，基于飞天核心平台构建，是阿里云向外提供的标准云计算存储服务。

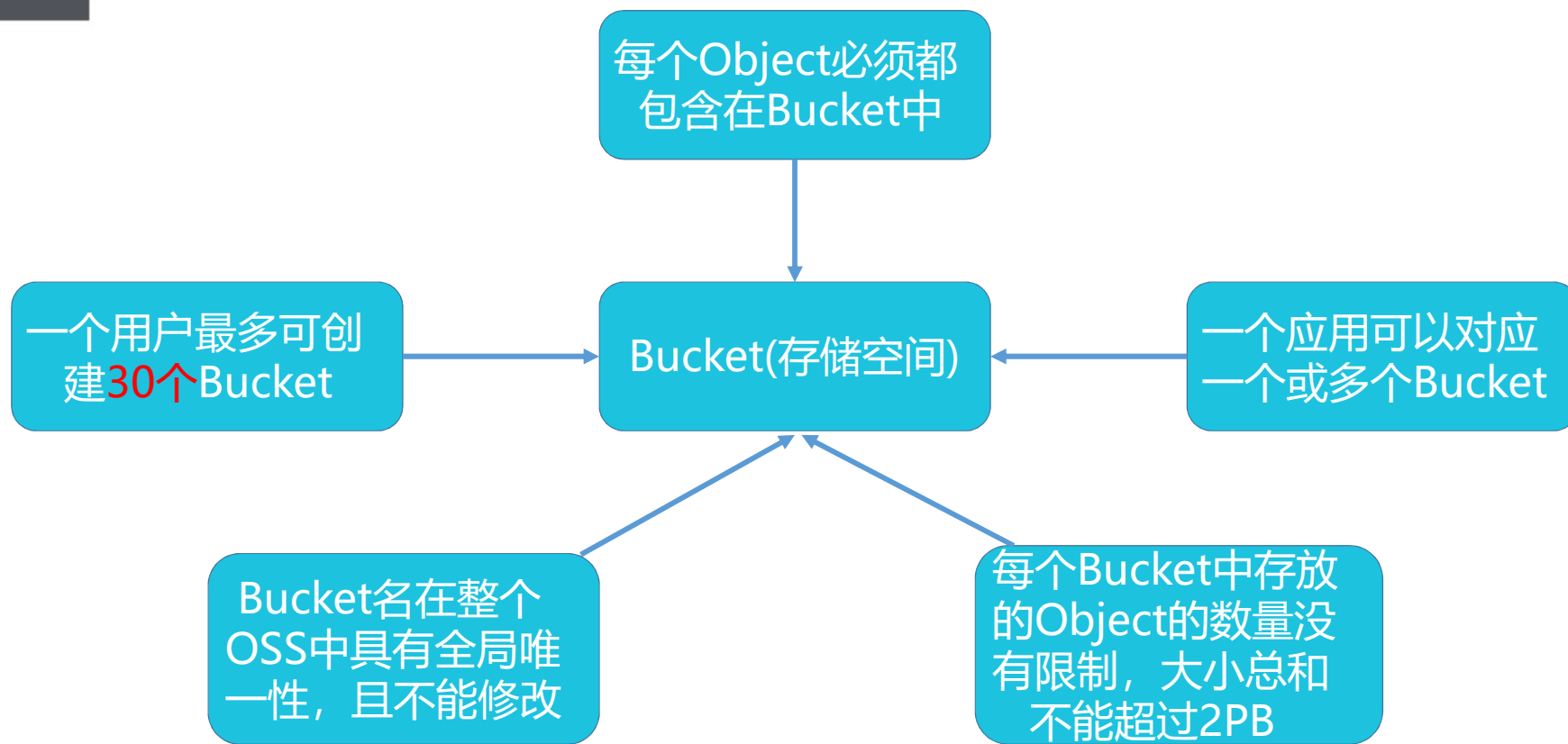


OSS的基本概念



- Put Object方式最大不能超过**5GB**,
- 使用multipart上传方式Object大小不能超过**48.8TB**

OSS的基本概念



OSS的基本概念

Service

提供给用户的**虚拟存储空间**，用户可以在这个存储空间中拥有一个或者多个Bucket

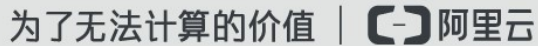
AccessKey ID & Access Key Secret (API密钥)

用于标识用户，为访问OSS做签名验证

访问域名 (Endpoint)

Endpoint 表示OSS对外服务的访问域名。

© 2006 The Authors
Journal compilation © 2006 Blackwell Publishing Ltd



OSS的优势

OSS与自建存储对比的优势

对比项	对象存储OSS	自建服务器存储
可靠性	<ul style="list-style-type: none">•服务设计可用性不低于99.99%。•规模自动扩展，不影响对外服务。•数据设计持久性不低于99.999999999%。•数据自动多重冗余备份。	<ul style="list-style-type: none">•受限于硬件可靠性，易出问题，一旦出现磁盘坏道，容易出现不可逆转的数据丢失。•人工数据恢复困难、耗时、耗力。
安全	<ul style="list-style-type: none">•提供企业级多层次安全防护。•多用户资源隔离机制，支持异地容灾机制。•提供多种鉴权和授权机制及白名单、防盗链、主子账号功能。	<ul style="list-style-type: none">•需要另外购买清洗和黑洞设备。•需要单独实现安全机制。
成本	<ul style="list-style-type: none">•多线BGP骨干网络，无带宽限制，上行流量免费。•无需运维人员与托管费用，0成本运维。	<ul style="list-style-type: none">•存储受硬盘容量限制，需人工扩容。•单线或双线接入速度慢，有带宽限制，峰值时期需人工扩容。•需专人运维，成本高。
数据处理能力	提供图片处理、音视频转码、内容加速分发、鉴黄服务、归档服务等多种数据增值服务，并不断丰富中。	需要额外采购，单独部署。

OSS存储类型

标准类型

高性能、高可靠、高可用的对象存储服务

- 吞吐量大，热点文件、需要频繁访问的业务场景
- 持久性：99.999999999%
- 最低存储时间：无

- 移动应用 ➢ 图片分享
- 大型网站 ➢ 热点音视频

低频访问类型

较低存储成本和实时访问特性的对象存储服务

- 数据访问实时，读取频率较低的业务场景
- 持久性：99.999999999%
- 最低存储时间：30天

- 移动设备 ➢ 网盘应用
- 监控数据
- 应用与企业数据备份

归档类型

归档数据的长期存储，存储单价最低

- 数据恢复有等待时间，数据有存储时长要求
- 持久性：99.999999999%
- 最低存储时间：60天

- 各种长期保存的档案数据
- 医疗影像
- 影视素材

目录

1. 对象存储的基本概念和组成

2.对象存储的应用

2.1 如何使用OSS

2.2 如何用好OSS

OSS使用快速入门：创建Bucket

1. 用户创建一个 Bucket 时，可以根据费用单价、请求来源分布、响应延迟等方面的考虑，**为该 bucket 选择所在的数据中心**
阿里云所有数据中心都提供OSS公众服务：

Region中文名称	Region英文表示	外网Endpoint	ECS访问的内网Endpoint
华东 1	oss-cn-hangzhou	oss-cn-hangzhou.aliyuncs.com	oss-cn-hangzhou-internal.aliyuncs.com
华东 2	oss-cn-shanghai	oss-cn-shanghai.aliyuncs.com	oss-cn-shanghai-internal.aliyuncs.com
华北 1	oss-cn-qingdao	oss-cn-qingdao.aliyuncs.com	oss-cn-qingdao-internal.aliyuncs.com
华北 2	oss-cn-beijing	oss-cn-beijing.aliyuncs.com	oss-cn-beijing-internal.aliyuncs.com
华南 1	oss-cn-shenzhen	oss-cn-shenzhen.aliyuncs.com	oss-cn-shenzhen-internal.aliyuncs.com
香港	oss-cn-hongkong	oss-cn-hongkong.aliyuncs.com	oss-cn-hongkong-internal.aliyuncs.com

- Bucket 一旦创建完成后，就不可以修改所属的数据中心。**
2. OSS 只支持 Bucket 级别的数据中心设置，**不支持针对 Object 设置数据中心**
 3. Bucket 所在的数据中心确定后，该 Bucket 下的所有 Object 将一直存放在该数据中心，除非用户自己将它们搬迁到其它数据中心

安全控制：Bucket权限控制

OSS 提供 Bucket级别的权限访问控制

OSS提供ACL（Access Control List）权限控制方法，OSS ACL提供Bucket级别的权限访问控制，Bucket目前有三种访问权限：

Public-read-write

Public-read

Private

- 创建Bucket时默认为private权限。
- 可以通过OSS的Put Bucket Acl接口修改该Bucket的权限。

OSS使用快速入门：创建Bucket

新建 Bucket

[创建存储空间](#) ×

① 注意：Bucket 创建成功后，您所选择的**存储类型**、**区域**不支持变更。

Bucket 名称 0/63

区域

相同区域内的产品内网可以互通；订购后不支持更换区域，请谨慎选择

您在该区域下没有可用的 **存储包**、**流量包**。建议您购买资源包享受更多优惠，点击 [购买](#)。

Endpoint oss-cn-beijing.aliyuncs.com

存储类型

标准存储

低频访问

归档存储

标准：高可靠、高可用、高性能，数据会经常被访问到。

[如何选择适合您的存储类型？](#)

读写权限

私有

公共读

公共读写

私有：对文件的所有访问操作需要进行身份验证。

确定

取消

存储空间



OSS使用快速入门：上传文件



上传文件

文件目录

当前目录

指定目录

目录地址

/

文件 ACL

继承 Bucket

私有

公共读

公共读写

继承 Bucket: 单个文件的读写权限按 Bucket 的读写权限为准。

上传文件



将目录或多个文件（最多支持 100 个文件同时上传）拖曳到此，或 [直接上传](#)。

文件的命名规范如下：

1. 使用 UTF-8 编码
2. 长度必须在 1-1023 字节之间
3. 不能以「/」或者「\」字符开头

注意：对象名称需要区分大小写。如无特殊说明，本文档中的对象、文件称谓等同于 Object。

注：如果上传的文件与存储空间中已有的文件重名，则会覆盖已有文件。

通过OSS控制台上传小于5GB的文件

通过SDK或API使用Multipart Upload方法上传大于5GB的文件。

Object外链地址的构成规则

- 如果Bucket的权限为公共读或者公共读写时，Object的访问规则如下：

`http://<你的bucket名字>.<数据中心服务域名>/<你的object名字>`

- 示意图：

`http://oss-example.oss-cn-hangzhou.aliyuncs.com/aliyun-logo.png`

The diagram illustrates the structure of the URL by highlighting different components with colored bars and labels below them:

- bucket**: `oss-example` (highlighted in yellow)
- host**: `.oss-cn-hangzhou.aliyuncs.com` (highlighted in red)
- object**: `/aliyun-logo.png` (highlighted in green)

访问Object

- 用户可以直接将该上述URL 链接放入 HTML 中使用:

```
<img src= "http://oss-example.oss-cn-Hangzhou.aliyuncs.com/aliyun-logo.png" />
```

- 假设 oss-example 这个 bucket 在青岛数据中心, 这个 object 的外链 URL 为:

```
http://oss-example.oss-cn-qingdao.aliyuncs.com/aliyun-logo.png
```

- 在使用 OSS 时, 请一直使用 OSS 服务域名, 而不要使用固定的 IP 地址。

请求路由规则

1. OSS 使用域名系统 (DNS, Domain Name System) 将请求发往正确的服务器
2. 从 URL 中通过三级域名提取 bucket 名称, 然后将请求路由到 Bucket 所在的数据中心, 即所谓的三级域名访问方式
3. 当一个数据中心的 OSS 服务器收到属于其他数据中心 bucket 的请求时, OSS服务器会返回 HTTP 403 (禁止访问) 错误码, 并在 HTTP 消息体内提示正确的数据中心服务域名

OSS使用快速入门：下载文件

OSS提供三种下载方式：

简单下载

简单下载即下载已经上传的文件（Object），Object下载是使用HTTP的GET请求来完成的。

断线续传下载


OSS提供了从Object指定的位置开始下载的功能，在下载大的Object的时候，可以分多次下载。如果下载中断，重启的时候也可以从上次完成的位置开始继续下载。

授权给第三方下载

将私有Bucket内部的Object授权给第三方下载的时候，不应该直接将AccessKey提供给下载者，而应该使用URL签名和临时访问凭证两种方法。

OSS使用快速入门：删除文件

上传文件 新建目录 删除 设置 HTTP 头 碎片管理 授权 刷新 已选择: 1 / 1

<input checked="" type="checkbox"/>	文件名 (Object Name)	文件大小	存储类型
<input checked="" type="checkbox"/>	 1528445740260.jpg	90.574KB	标准存储

如果您不再需要存储所上传的文件，请将其删除以免进一步产生费用。

目录

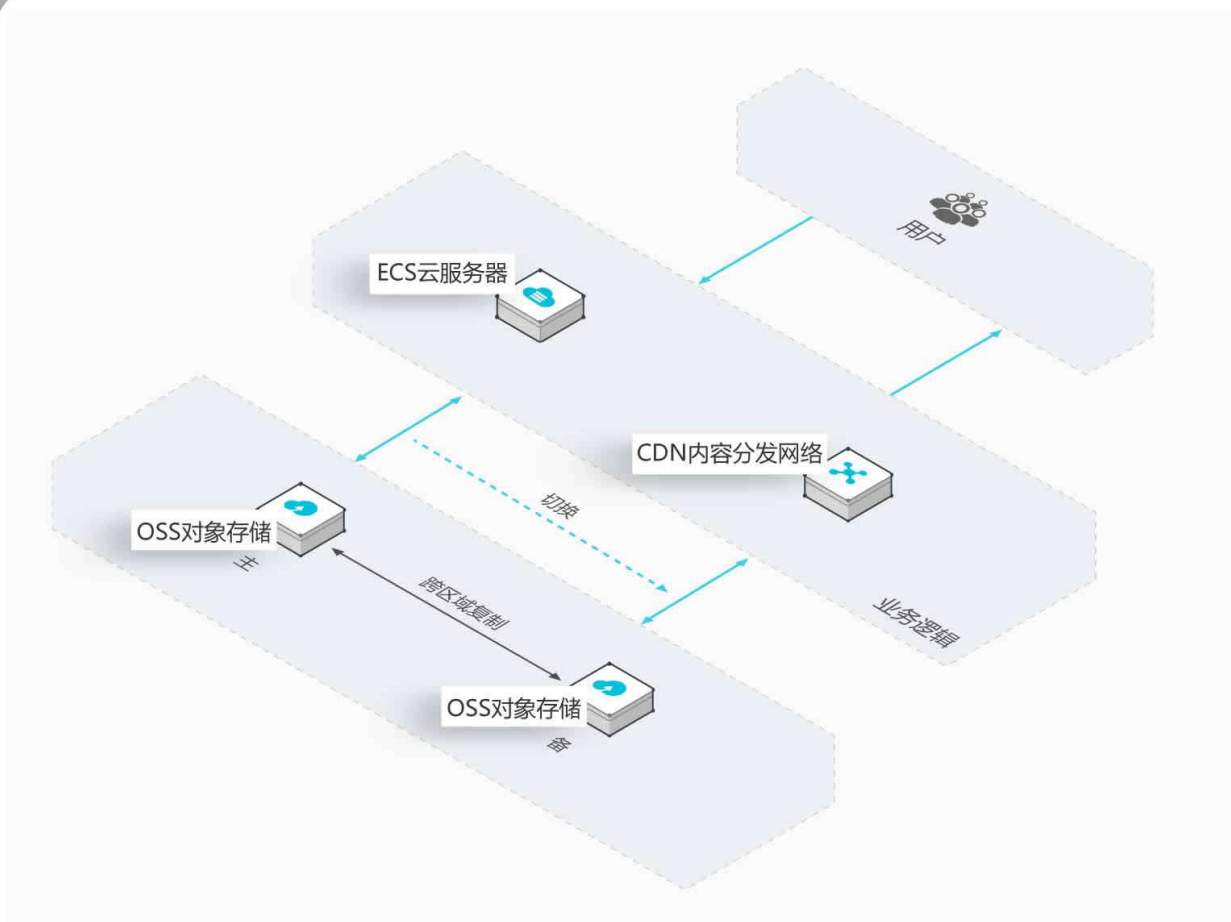
1. 对象存储的基本概念和组成

2.对象存储的应用

2.1 如何使用OSS

2.2 如何用好OSS

OSS实践1：数据备份与跨域复制



能够提供

- **异地容灾**：通过跨区域复制功能可在另一数据中心维护副本，实现异地容灾
- **数据合规**：在远距离的OSS数据中心之间复制数据以满足数据合规性要求

典型案例



OSS实践1：数据备份与跨域复制

使用场景

- 合规性要求
- 最大限度减少延迟
- 数据备份与容灾
- 数据复制
- 操作原因

开启跨区域复制

同步目标Location :

华北 2 (北京) ▼

同步目标Bucket :

test-1-005 ▼

是否同步历史数据 :

☒ 同步

确定

取消

OSS实践2：安全防护与管理

OSS适用于存储各种类型的静态资源，为防止OSS的资源被恶意盗用，OSS提供了几种安全防护功能，还可以集成安全类产品进行安全防护。

防盗链

目前OSS提供的防盗链方法主要有以下两种：

- 设置Referer。该操作通过控制台和SDK均可进行，用户可根据自身需求进行选择。
- 签名URL，适合习惯开发的用户。

权限控制

Bucket私有的情况下，需要通过签名URL访问object。

由于签名URL存在一个过期时间，所以签名URL会定期过期，增加了一直恶意下载的成本，同时用户需要集成OSS签名URL的API，有一定的开发成本。

OSS实践2：安全防护与管理

跨域设置

设置跨域访问，用户就可以直接上传到OSS而无需中转。

异常流量排查

可以通过OSS 管理控制台->Bucket名称->热点统计，查看哪些IP发起的请求，是否存在异常IP发起了请求。

除了上述OSS本身提供的安全防护功能，还可以结合安全产品进行安全防护如：高防防护OSS，WAF结合OSS使用等。

OSS实践3：云端数据处理

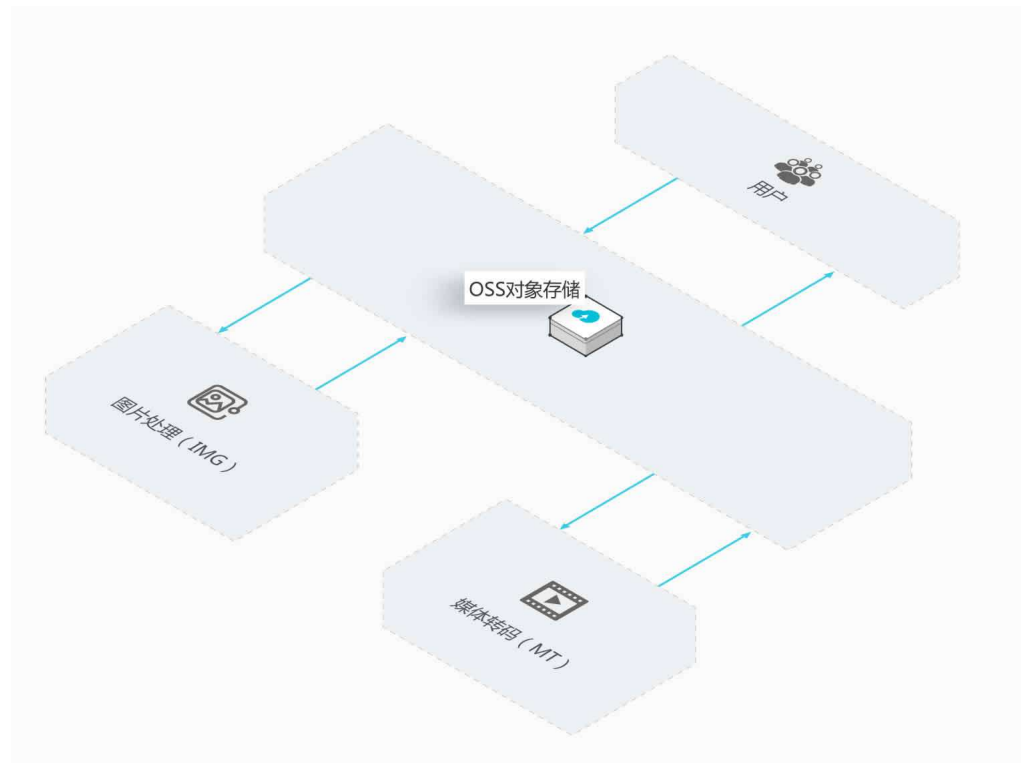
数据增值服务，为您的存储数据挖掘价值

上传文件到OSS后，您可以配合媒体转码服务(MTS)，图片处理服务（IMG），批量计算服务、离线数据处理服务（ODPS）充分挖掘您数据的价值，引领从IT到DT的变革。

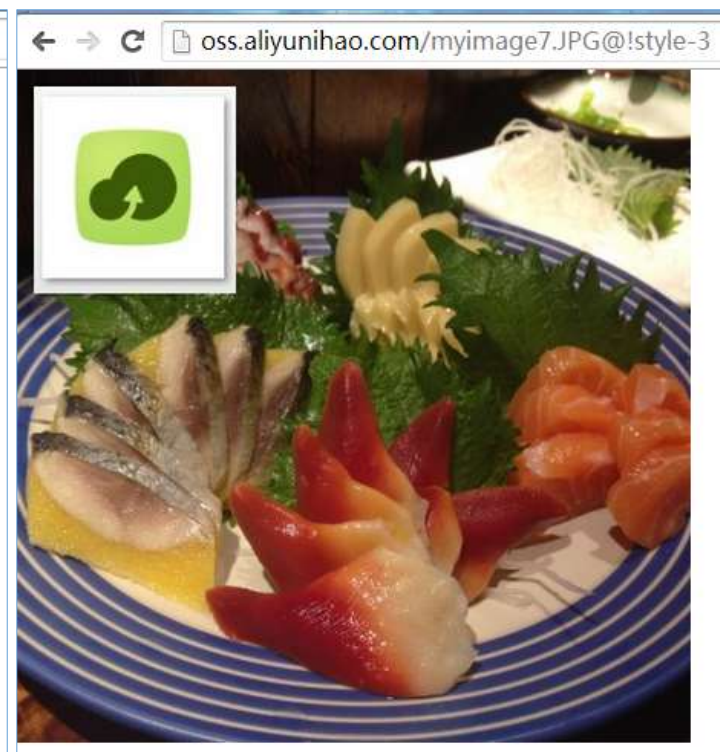
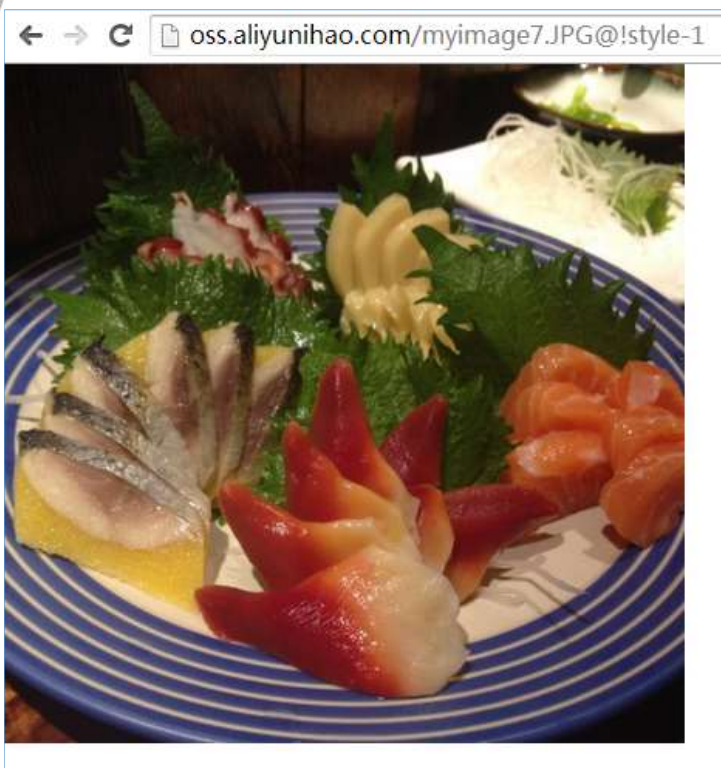
能够提供

- **富媒体数据处理**：自带图片处理/自定义函数等增值服务，配合MTS实现视频转码/截帧
- **存储+计算**：与阿里云数据计算产品打通，可直接调用计算服务挖掘您的数据价值

典型案例

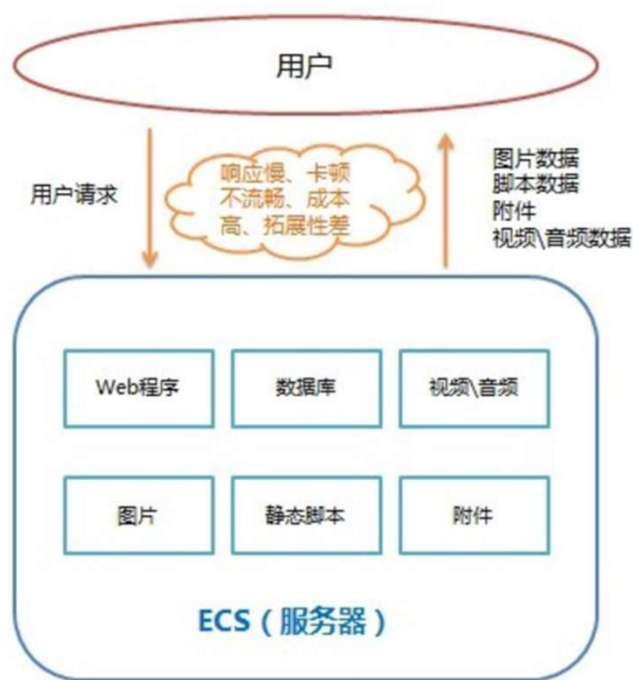


OSS实践3：云端数据处理



OSS实践4：CDN加速与动静分离

传统动静不分离的产品架构，其性能会随着系统访问量的增长而受到限制甚至遭遇瓶颈。



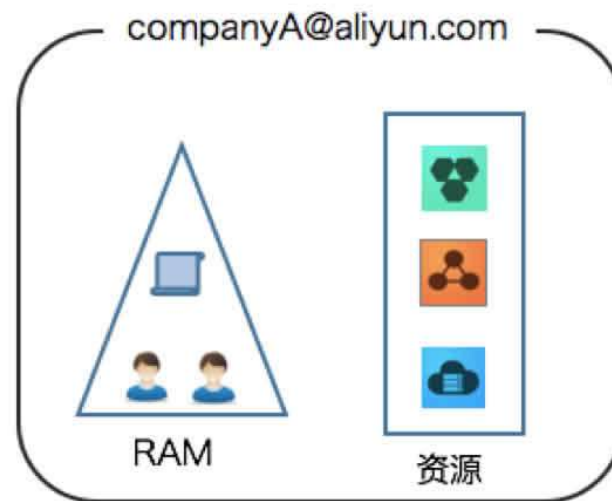
传统网站架构示意



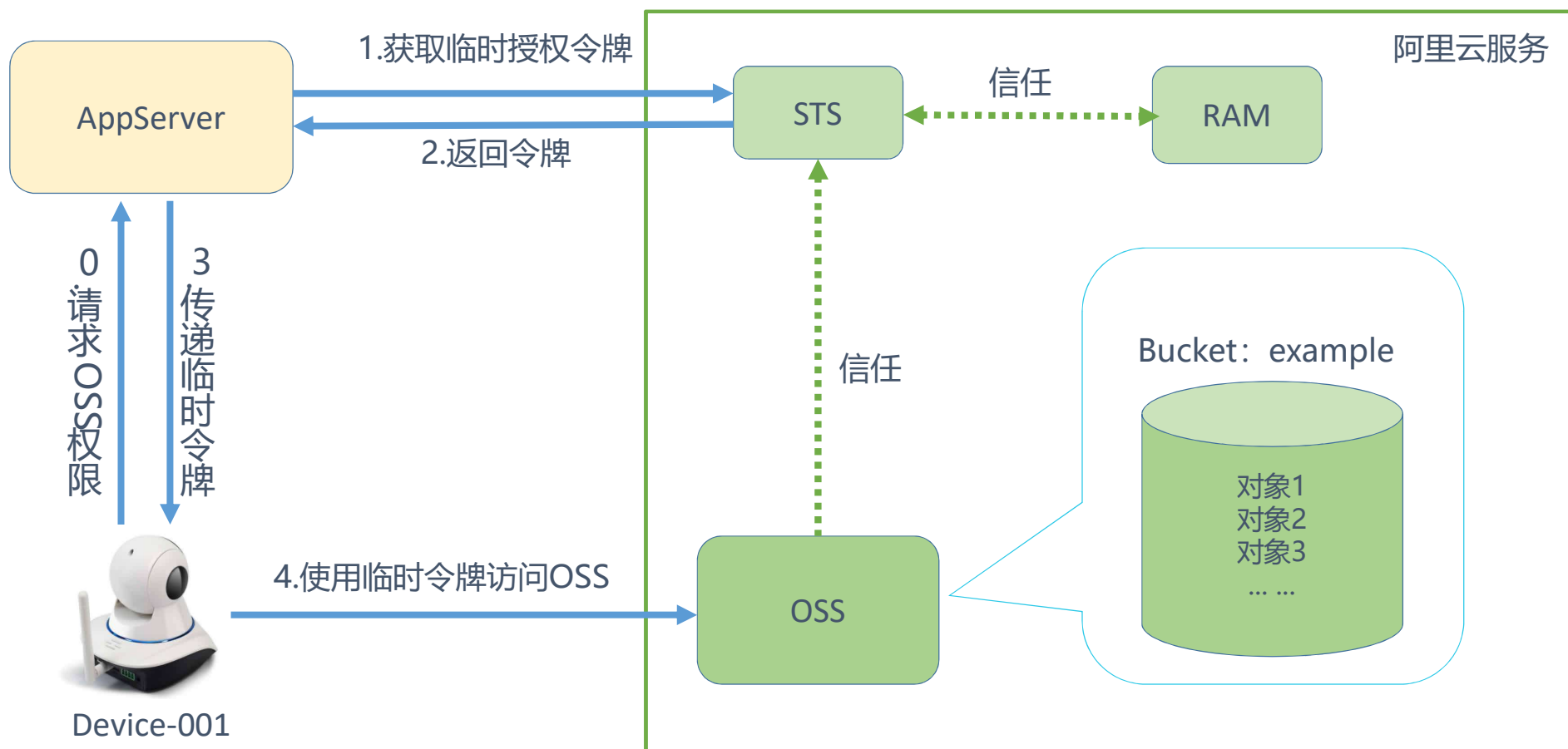
网站动静分离架构示意

OSS实践5：RAM与STS

- RAM和STS是阿里云提供的权限管理系统。
- RAM主要的作用是控制账号系统的权限。通过使用RAM可以将在主账号的权限范围内创建子用户，给不同的子用户分配不同的权限从而达到授权管理的目的。
- STS是一个安全凭证（Token）的管理系统，用来授予临时的访问权限，这样就可以通过STS来完成对于临时用户的访问授权。



OSS实践5：RAM与STS



小结

1. 什么是对象存储OSS?
2. 什么是Object, 什么是Bucket?
3. OSS有几种存储类型, 分别是什么?
4. OSS提供的安全防护有哪些?
5. RAM与STS 的作用是什么?

为了无法计算的价值 |  阿里云

