ALIBABA CLOUD

阿里云

对象存储 OSS

白皮书

文档版本：20201021

阿里云

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。

2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。

3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。

4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。

5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。

6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	警告 重启操作将导致业务中断，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击**设置**> **网络**> **设置网络类型**。
粗体	表示按键、菜单、页面名称等UI元素。	在**结果确认**页面，单击**确定**。
`Courier字体`	命令或代码。	执行 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *Instance_ID*
[] 或者 [a|b]	表示可选项，至多选择一个。	`ipconfig [-all|-t]`
{} 或者 {a|b}	表示必选项，至多选择一个。	`switch {active|stand}`

目录

1.阿里云存储服务概述

1.1. 介绍

阿里云提供针对各种存储资源（块、文件和对象）的低成本、高可靠、高可用的存储服务，涵盖数据备份、归档、容灾等场景。本文介绍阿里云各类存储服务及特性的适用场景、性能、安全、接口和费用模型等，帮助您选择最适合您业务场景和需求的云存储服务。

有关阿里云存储服务的详细介绍、客户案例、解决方案等，请参见阿里云存储产品家族。

对象存储OSS	对象存储OSS（Object Storage Service）是一款海量、安全、低成本、高可靠的云存储服务，其容量和处理能力弹性扩展，提供多种存储类型供选择，覆盖从热到冷的各种数据存储场景，帮助您全面优化存储成本。
块存储	块存储是阿里云为云服务器ECS提供的块设备，高性能、低时延、随机读写。您可以像使用物理硬盘一样格式化并建立文件系统来使用块存储。
文件存储NAS	阿里云文件存储NAS（Network Attached Storage）是一款面向阿里云ECS实例、E-HPC和容器服务等计算节点的高可靠、高性能的分布式文件系统，可共享访问、弹性扩展。NAS基于POSIX文件接口，天然适配原生操作系统。
文件存储CPFS	文件存储CPFS（Cloud Paralleled File System）是一款并行文件系统，其数据存储在集群中的多个数据节点，多个客户端可以同时访问，满足大型高性能计算机集群的高IOPS、高吞吐、低时延的数据存储需求。
文件存储HDFS	文件存储HDFS（Apsara File Storage for HDFS）是一款面向阿里云ECS实例及容器服务等计算资源的文件存储服务，满足以Hadoop为代表的分布式计算业务类型对分布式存储性能、容量和可靠性的多方面要求。
表格存储	表格存储（Tablestore）是阿里云自研的结构化数据存储，提供海量结构化数据存储以及快速的查询和分析服务，具备PB级存储、千万TPS以及毫秒级延迟的服务能力。
云存储网关	云存储网关（Cloud Storage Gateway）是一款可以部署在用户IDC和阿里云上的网关产品，以阿里云对象存储OSS为后端存储，为云上和云下应用提供业界标准的文件服务（NFS 和 SMB）和块存储服务（iSCSI）。

1.2. 对象存储OSS

对象存储OSS（Object Storage Service）是阿里云提供的海量、安全、低成本、高持久的云存储服务。其数据设计持久性不低于99.9999999999%（12个9），服务设计可用性不低于99.995%。OSS具有与平台无关的RESTful API接口，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提供标准、低频访问、归档和冷归档四种存储类型，全面覆盖从热到冷的各种数据存储场景：

标准存储类型	高持久、高可用、高性能的对象存储服务，支持频繁的数据访问。是各种社交、分享类的图片、音视频应用、大型网站、大数据分析的合适选择。
低频访问存储类型	适合长期保存不经常访问的数据（平均每月访问频率1到2次）。存储单价低于标准类型，适合各类移动应用、智能设备、企业数据的长期备份，支持实时数据访问。

归档存储类型	适合需要长期保存（建议半年以上）的归档数据，在存储周期内极少被访问，数据进入到可读取状态需要1分钟的解冻时间。适合需要长期保存的档案数据、医疗影像、科学资料、影视素材。
冷归档存储类型	适合需要超长时间存放的极冷数据。例如因合规要求需要长期留存的数据、大数据及人工智能领域长期积累的原始数据、影视行业长期留存的媒体资源、在线教育行业的归档视频等。

适用场景

OSS适用于以下场景：

- 静态网站内容和音视频的存储与分发

  每个存储在OSS上的文件（Object）都有唯一的HTTP URL地址，用于内容分发。同时，OSS还可以作为内容分发网络（CDN）的源站。由于无需分区，OSS尤其适用于托管那些数据密集型、用户生产内容的网站，如图片和视频分享网站。各种终端设备、Web网站程序、移动应用可以直接向OSS写入或读取数据。OSS支持流式写入和文件写入两种方式。

- 静态网站托管

  作为低成本、高可用、高扩展性的解决方案，OSS可用于存储静态HTML文件、图片、视频、JavaScript等类型的客户端脚本。

- 计算和分析的数据存储仓库

  OSS的水平扩展性使您可以同时从多个计算节点访问数据而不受单个节点的限制。

- 数据备份和归档

  OSS为重要数据的备份和归档提供高可用、可扩展、安全可靠的解决方案。您可以通过设置生命周期规则将存储在OSS上的冷数据自动转储为低频或者归档存储类型以节约存储成本。您还可以使用跨区域复制功能在不同地域的不同存储空间之间自动异步（近实时）复制数据，实现业务的跨区域容灾。

性能

如果您的云服务器ECS和对象存储OSS在同一个地域，那么通过云服务器ECS访问对象存储OSS中的数据理论上是最快的。OSS的设计也使其服务端延迟相对于网络延迟来讲可以忽略不计。此外，OSS对于存储量、请求数和用户数的扩展特性，使其可以很好的支持大量Web级应用程序。如果您使用多线程、多个应用程序或多个客户端同时访问OSS，总的OSS聚合吞吐量通常会扩展到远超任何单个服务器可以生成或消耗的速率。

为了提升大文件（5 GB以上）的上传性能，阿里云OSS提供分片上传（Multipart Upload）功能，将要上传的Object分成多个数据块（Part）来分别上传，上传完成之后再将这些Part组合成一个Object来达到断点续传的效果。分片上传适用于网络条件不佳的场景，当出现上传失败的时候，可以对失败的Part进行独立的重试，而不需要重新上传整个Object。

为了提升数据访问速度，许多开发者会将OSS和搜索引擎（如开放搜索OpenSearch）或数据库（如表格存储、云数据库RDS）搭配使用。OSS用于存储实际的数据，而搜索引擎或数据库用于存储元信息，如文件名称、大小、关键词等。数据库中存储的元信息很容易被索引和查询。OSS和搜索引擎或数据库结合使用可用于精确定位和检索OSS中的文件。

为了提升远距离大文件的上传下载体验，满足文件动态更新、非热点文件的下载加速需求，OSS还提供传输加速功能，通过智能调度的系统、优化的传输链路、调优的协议栈与传输算法，并深度结合OSS服务端的配套策略，提供端到端的加速方案。

对于静态热点文件的下载加速场景，OSS支持开启阿里云CDN加速服务。阿里云CDN将OSS的Bucket作为源站，将源内容发布到边缘节点。阿里云CDN配合精准的调度系统，将用户的请求分配至最适合的节点，使终端用户以最快的速度读取到所需的内容，有效解决Internet网络拥塞状况，提高用户访问的响应速度。

数据持久性和服务可用性

OSS提供的三种存储类型中，标准类型（Standard）和低频访问类型（Infrequent Access）通过自动同步提供。OSS采用多可用区（AZ）机制，将用户的数据分散存放在同一地域（Region）的3个可用区。当某个可用区不可用时，仍然能够保障数据的正常访问。OSS同城3AZ能够提供99.9999999999%（12个9）的数据持久性以及99.995%的数据可用性。

您还可以针对存储空间启用跨区域复制功能。启用后，不同地域的不同存储空间之间将实现自动异步（近实时）复制数据，实现跨区域容灾需求。源存储空间和目标存储空间均提供99.9999999999%（12个9）的数据持久性以及99.995%的数据可用性。

扩展性和弹性

OSS提供高扩展性和弹性。普通的文件系统如果在同一目录下存放太多文件，经常会出现问题。而OSS总的存储容量以及单个存储空间的容量均无上限。您可以在一个存储空间内存放无限量的文件，OSS自动将您的数据副本存储至同一地域的不同服务器，所有数据副本共享阿里云的高性能基础设施能力。

安全性

阿里云对象存储OSS（Object Storage Service）具有丰富的安全防护能力，支持服务端加密、客户端加密、防盗链白名单、细粒度权限管控、日志审计、合规保留策略（WORM）等特性。OSS是目前中国国内唯一通过Cohasset Associates审计认证的云服务，可满足严格的电子记录保留要求，例如SEC Rule 17a-4（f）、FINRA 4511、CFTC 1.31等合规要求。关于OSS安全能力的详细介绍，请参见OSS安全与合规白皮书。

接口

OSS提供标准的RESTful API接口，您可以使用API接口将文件（Object）存储在存储空间（Bucket，顶级文件夹）中，存储空间的名称全局唯一。每个文件有一个Object Key（文件名），作为该文件在该存储空间中的唯一标识。OSS没有文件夹的概念，所有元素都是以文件来存储，但是您可以通过创建以正斜线（/）结尾的文件名（如folder1/folder2/file）来模拟文件夹。

开发者一般使用工具或封装了API接口的SDK来开发应用。OSS目前提供包括Java、Python、PHP、Go、Android、iOS在内的10多种开发语言SDK。命令行工具ossutil提供方便、简洁、丰富的Bucket和Object管理命令，如ls、cp、cat、config等，操作性能好，可并发上传，支持Windows、Linux、 Mac平台。您也可以使用图形化管理工具ossbrowser方便直观地进行文件浏览、文件和文件夹（目录）上传下载等基本操作，或者使用图形化的Web应用程序OSS管理控制台轻松、便捷的管理您的OSS资源。

您还可以使用事件通知功能，及时了解您OSS资源上的相关操作。详情请参见事件通知。

费用模型

OSS的服务费用由存储费用、流量费用、请求费用、数据处理费用等组成。OSS开通后默认为按量计费，即按实际使用量*单价的方式计费，每小时统计前一小时的实际用量并从账户余额中扣除实际消费金额。针对部分计费项，您还可以使用包年包月的计费方式，进一步降低费用。包年包月即预先购买指定资源包，之后使用资源时，扣除相应的额度。详情请参见计量项与计费项概述。

1.3. 文件存储NAS

阿里云文件存储NAS（Apsara File Storage）是面向阿里云ECS实例、E-HPC和容器服务等计算节点的文件存储服务。它是一种可共享访问、弹性扩展、高可靠以及高性能的分布式文件系统，支持NFS和SMB协议。

文件存储NAS目前提供极速型、性能型、容量型、低频型四种规格：

极速型	基于阿里云最新一代网络架构和全闪存储打造的高性能共享文件存储。最大容量256 TB，起步带宽150 MB/s，可扩展到1200 MB/s。稳定百微秒级时延。适合海量小文件、时延敏感的业务。
性能型	使用SSD作为存储介质，为应用工作负载提供高吞吐量与IOPS、低时延的存储性能。适用于高并发高吞吐，业务弹性扩展、对读时延有较高要求的文件共享存储服务。对于读写频繁、系统响应要求高的业务，有性能优势。
容量型	使用SATA HDD作为存储介质，以更低的成本提供高性能的存储空间。适用于高并发高吞吐，业务弹性扩展，成本敏感型的文件共享存储服务。对于读写访问不太频繁，时延响应要求不高的业务，有较好的成本优势。
低频型	对于不频繁访问的，长期存储的性能型或容量型数据，可以通过生命周期管理功能将其转移到低频存储空间，采用低频计费方式，从而进一步降低成本。详情请参见生命周期管理功能介绍。

适用场景

NAS适用于以下场景：

- 容器存储

  鉴于容器的可快速预置、容易携带，并可提供进程隔离的特点，容器非常适用于构建微服务。对于每次启动时都需要访问原始数据的容器，它们需要一个共享文件系统，使它们无论在哪个实例上运行，都可以连接到该文件系统。NAS可提供对文件数据的持久共享访问权限，非常适合容器存储。

- 内容管理和Web服务

  NAS可以用作一种持久性强、吞吐量高的文件系统，用于各种内容管理系统和Web服务应用程序，为网站、在线发行和存档等广泛的应用程序存储和提供信息。由于NAS遵循了预期的文件系统语义、文件命名惯例、Web开发人员习惯使用的权限，因此它能够轻松与Web应用程序集成，并且可广泛用于Web站点、在线发行和存档等应用程序。

- 企业应用程序

  NAS具有较高的可扩展性、弹性、可用性和持久性，因而可用作企业应用程序和以服务形式交付的应用程序的文件存储。NAS提供的标准文件系统界面和文件系统语义能够将企业应用程序轻松迁移到阿里云或构建新的应用程序。

- 媒体和娱乐工作流

  视频编辑、影音制作、广播处理、声音设计和渲染等媒体工作流通常依赖于共享存储来操作大型文件。强大的数据一致性模型加上高吞吐量和共享文件访问，可以缩短完成以上工作流所需的时间，并将多个本地文件存储库合并到面向所有用户的单个位置。

- 大数据分析

  NAS提供了大数据应用程序所需的规模和性能，具备计算节点高吞吐量、写和读一致性以及低延迟的文件操作能力。许多分析工作负载通过文件接口与数据进行交互，依赖于文件锁等文件语义，并要求能够写入文件的部分内容。NAS支持文件锁定的文件系统语义，并且能够弹性扩展容量和性能。

性能

单个文件系统的吞吐性能上限（峰值）与文件系统的当前使用容量线性相关，即存储量越大，吞吐性能上限（峰值）越高。支持上千个ECS通过POSIX接口并发访问，随机读写。

规格	容量	时延	IOPS
极速型NAS	256 TB	百微秒级	10000~200000
性能型NAS	1 PB	毫秒级	最大30000（硬盘4k随机IO读写
容量型NAS	10 PB	10毫秒级	最大15000（硬盘4k随机IO读写）

接口

NAS数据层的API，如NAS数据的读写操作，通过POSIX接口实现。您无需修改线下本机的应用程序代码即可直接上云，灵活方便。

NAS控制层的API支持HTTP或者HTTPS网络请求协议，允许GET和POST方法。如果您熟悉网络服务协议和一种以上编程语言，推荐您调用API管理您的文件存储NAS。您可以通过阿里云NAS SDK、阿里云CLI、阿里云API Explorer调用NAS控制层的API，对文件系统、挂载点、权限组、快照、标签等资源执行创建、删除、查询、修改等操作。详情请参见API概览。如果您更习惯使用图形化的Web应用程序，可以使用NAS管理控制台，实现NAS API支持的所有控制层的操作。

扩展性和弹性

传统的存储系统需要耗时又繁琐的规划、购置、分区、监控等操作，使用NAS则无需进行这些复杂的操作。NAS可随着您文件的添加和删除自动进行扩容或缩容，实现存储的按需分配，而不影响您的应用服务。

数据持久性和服务可用性

NAS的数据在后端进行多副本存储，每份数据都有多份拷贝在故障域隔离的不同设备上存放， 提供99.999999999%（11个9）的数据可靠性，能够有效降低数据安全风险。

安全性

- 权限组

  在NAS中，权限组是一个白名单机制，定义了访问文件存储的权限信息，包括授权IP地址、读写权限、用户权限等。您可以添加权限组规则，允许指定的IP地址或网段访问文件系统，并可以给不同的IP地址或网段授予不同级别的访问权限。

- 访问控制RAM

  您可以通过RAM来管理NAS用户身份并控制资源的访问权限。RAM是基于用户的访问控制。您可以在一个云账户（主账户）下创建并管理多个RAM用户，并给RAM用户分配不同的授权策略，从而实现不同RAM用户拥有不同的云资源访问权限。使用RAM还可以让您避免与其他用户共享云账号密钥（AccessKey），按需为用户分配最小权限，从而降低您的企业信息安全风险。详情请参见基于RAM Policy的权限控制。

- 访问控制ACL

  您可以通过ACL管理文件和目录的访问权限。ACL是基于资源的访问控制。企业级用户通过共享文件系统在多个用户和群组之间共享文件时，权限的控制和管理成为了不可缺少的功能。ACL权限控制允许您针对不同目录或文件，给不同的用户和群组设置相应的权限，实现访问隔离。详情请参见NAS NFS ACL和NAS SMB ACL。

- 加密

NAS使用行业标准AES-256加密算法进行静态数据加密，为您的文件系统提供落盘存储加密服务，并使用密钥管理服务（KMS）进行密钥管理。在将数据写入到文件系统之前，自动对其进行加密；在读取数据并将其提供给应用程序之前，自动对其进行解密。这些过程是NAS透明处理的，因此您不必修改您的应用程序。

费用模型

NAS的容量可按照您的业务需求自动配置，您无需事先进行存储分区。相应的，NAS的费用模型也是按量付费。如果文件增加，您也只需支付实际使用的存储空间的费用。如果文件被删除，则会停止相应的计费。您也可以使用包年包月的计费方式，预先购买存储包，之后使用资源时，扣除相应的额度。一般情况下，存储包的价格更优惠。

1.4. 块存储

块存储是阿里云为云服务器ECS提供的块设备类型产品，具备高性能、低时延等特性。您可以像使用物理硬盘一样格式化并建立文件系统来使用块存储，可满足绝大部分通用业务场景下的数据存储需求。

适用场景

阿里云为您的云服务器ECS提供了丰富的块存储产品类型，包括基于分布式存储架构的云盘以及基于物理机本地硬盘的本地盘产品。其中：

- 云盘是阿里云为云服务器ECS提供的数据块级别的块存储产品，采用多副本的分布式机制，具有低时延、高性能、持久性、高可靠等性能，可以随时创建、扩容以及释放。
- 本地盘是基于云服务器ECS所在物理机（宿主机）上的本地硬盘设备，为ECS实例提供本地存储访问能力。本地盘适用于对存储I/O性能和海量存储性价比有极高要求的业务场景。具有低时延、高随机IOPS、高吞吐量、高性价比等优势。

性能

衡量块存储产品的性能指标主要包括IOPS、吞吐量和访问时延。部分块存储产品对容量也有要求，例如不同性能等级的ESSD云盘对应的容量范围不同。详细的性能指标请参见块存储性能。

数据持久性和服务可用性

在同一可用区中，您的业务数据以多副本的形式分布存储在块存储集群中，保证读写过程中的数据稳定性，为ECS实例实现99.9999999%（9个9）的数据可靠性保证。

为进一步提升块存储的可靠性，建议您定期创建快照，为云盘提供数据备份能力，确保日志和客户交易等信息有备份可查询。详情请参见快照概述。

扩展性和弹性

您可以对云盘进行快速分区或释放，根据您的业务需求对存储容量进行实时的调整。随着业务发展和应用数据增长，您可以选择多种方式来扩展云盘，增加单台实例的存储容量：

- 扩容已有云盘，您需要自行扩展已有分区或者扩展新建分区。
- 创建一块新云盘，作为数据盘挂载到实例上，并需要自行分区格式化。
- 更换系统盘的同时指定更高的系统盘容量。

安全性

您可以通过访问控制RAM授权其他用户访问您云盘的权限。

对于数据敏感型应用，建议您加密存储设备。ECS云盘加密采用行业标准的AES-256算法，利用密钥加密云盘以及云盘快照。从ECS实例传输到云盘的数据会被自动加密，并在读取数据时自动解密。详情请参见加密概述。

接口

块存储API支持HTTP或者HTTPS网络请求协议，允许GET和POST方法。如果您熟悉网络服务协议和一种以上编程语言，推荐您调用API管理您的块存储。您可以通过阿里云ECS SDK、阿里云CLI、阿里云API Explorer调用块存储 API，对ECS实例上的云盘进行创建、删除、查询、挂载、卸载、扩容等操作，对存储在OSS上的云盘快照进行创建、删除、查询等操作。

如果您更习惯使用图形化的Web应用程序，可以使用ECS管理控制台，实现块存储API支持的所有操作。

费用模型

和其他阿里云服务一样，块存储有按量计费和包年包月两种计费方式。按量计费方式下，您按需开通和释放块存储资源，无需提前购买大量资源，成本比传统主机降低30%~80%；如果您使用包年包月的方式，即先付费再使用，成本将进一步降低。

通过不同方式创建云盘时，支持的计费方式不同：

- 随ECS实例创建云盘，计费方式和ECS实例相同。
- 为已有包年包月ECS实例创建包年包月云盘，计费方式为包年包月。
- 在云盘页面创建云盘，计费方式仅支持按量付费。
- 使用快照创建云盘，计费方式仅支持按量付费。

云盘支持转换计费方式，方便您灵活管理云盘，详情请参见转换云盘计费方式。存储容量单位包SCU可以抵扣部分云盘类型的按量付费账单，详情请参见存储容量单位包概述。

1.5. 文件存储CPFS

文件存储CPFS（Cloud Paralleled File System）是一种并行文件系统。CPFS的数据存储在集群中的多个数据节点，并可由多个客户端同时访问，从而能够为大型高性能计算机集群提供高IOPS、高吞吐、低时延的数据存储服务。

适用场景

文件存储CPFS针对高性能计算场景的性能要求进行了深度优化，提供对数据毫秒级的访问和高聚合IO、高IOPS的数据读写请求，可以用于AI深度训练、自动驾驶、基因计算、EDA仿真、石油勘探，气象分析、机器学习、大数据分析以及影视渲染等业务场景中。

性能

文件存储CPFS可以提供数百GB的带宽，数百万的IOPS以及亚毫秒级的延时。具体的带宽和IOPS与您购买的文件系统规模有关。

容量	带宽	标准型（写IOPS）	标准型（读IOPS）	高级型（写IOPS）	高级型（读IOPS）
2 TB	1 GB/s	20 k	40 k	50 k	100 k
5 TB	1 GB/s	20 k	40 k	50 k	100 k
	2.5 GB/s	60 k	150 k	100 k	350 k

容量	带宽	标准型（写IOPS）	标准型（读IOPS）	高级型（写IOPS）	高级型（读IOPS）
10 TB	1.5 GB/s	40 k	100 k	80 k	200 k
	2.5 GB/s	60 k	150 k	100 k	350 k
30 TB	2.5 GB/s	60 k	150 k	100 k	350 k
	5 GB/s	80 k	200 k	140 k	500 k
50 TB	2.5 GB/s	60 k	150 k	100 k	350 k
	7.5GB/s	100 k	300 k	200 k	600 k

您可以使用FIO工具进行吞吐和IOPS的性能测试，并通过分片配置提高聚合带宽和IOPS，详情请参见性能测试和性能调优。

数据持久性和服务可用性

文件存储CPFS的数据持久化存储于阿里云自研的盘古分布式存储系统，支持多份数据拷贝，可以提供99.999999999%（11个9）的数据可靠性。

文件存储CPFS的所有节点均为高可用设计。实现集群内秒级别的故障检测，并由CPFS集群调度器自动将服务切换到其他节点，同时兼顾负载均衡。整个切换过程用户不感知，提供远高于传统两节点的高可用性。

扩展性和弹性

文件存储CPFS支持在线扩容。由于所有数据均以条带化的方式存储并且支持扩容以后的自动负载平衡，可满足性能的线性增长，并且即时利用扩容节点的吞吐和存储能力，满足业务增长需要的更多容量与性能诉求。

安全性

文件存储CPFS支持配置企业自建的LDAP（Lightweight Directory Access Protocol）服务，来控制CPFS文件系统的用户访问。不接入LDAP时，CPFS只允许root用户访问文件系统，其他用户访问时将返回permission denied错误。接入LDAP时，您需要提供LDAP服务器并确保LDAP服务的连通性。

接口

CPFS API支持HTTP或HTTPS协议进行请求通信，支持GET方法发送请求。如果您熟悉网络服务协议和一种以上编程语言，推荐您调用API管理您的文件存储CPFS，对文件系统进行创建、挂载、管理等操作，以及LDAP用户管理。

如果您更习惯使用图形化的Web应用程序，可以使用管理控制台来管理CPFS文件系统。

费用模型

文件存储CPFS的计费项包括存储容量和带宽。开通产品时默认按照实际使用量按小时计费（按量付费），同时也支持购买资源包（包年包月）的方式提前购买资源的使用额度和时长，获取更多的优惠。详情请参见计量项和计费项。

1.6. 文件存储HDFS

阿里云文件存储HDFS（Apsara File Storage for HDFS）是面向阿里云ECS实例及容器服务等计算资源的文件存储服务。您可以像在Hadoop分布式文件系统 (Hadoop Distributed File System) 中管理和访问数据那样使用文件存储HDFS。您无需对现有大数据分析应用做任何修改，即可使用具备无限容量及性能扩展、单一命名空间、多共享、高可靠和高可用等特性的分布式文件系统。

适用场景

文件存储HDFS适用于对吞吐要求较高的大数据分析与机器学习业务场景。文件存储HDFS能够提供高吞吐量和低延迟的访问能力，无需将数据迁移到计算资源本地。

您将数据存入文件存储HDFS后 ，ECS实例或其他计算资源即可直接访问这些数据。将Hadoop或其他机器学习应用部署在多个计算资源上，应用可以直接通过Hadoopfs接口访问数据进行离线或在线计算，也可以直接将计算结果输出到文件存储HDFS做永久保存。

性能

衡量文件存储HDFS的性能指标主要是吞吐能力。吞吐最大不会超过ECS带宽。如果您的ECS带宽只有1.5Gbps，则吞吐最高可达到187.5MB/s。吞吐能力和购买的存储空间相关。更多信息请参见集群吞吐性能测试。

数据持久性和服务可用性

和文件存储NAS一样，文件存储HDFS的数据在后端进行多副本存储，每份数据都有多份拷贝在故障域隔离的不同设备上存放， 提供 99.999999999%（11个9） 的数据可靠性，能够有效降低数据安全风险。

扩展性和弹性

文件存储HDFS能够为应用负载提供高吞吐量、高IOPS及低时延的存储性能。同时，其性能与容量成线性关系，可满足业务增长时对更高容量与存储性能的需求。

安全性

文件存储HDFS具有文件系统标准权限控制、权限组访问控制和RAM主子账号授权等多种安全机制，从而保证文件系统数据安全万无一失。

接口

文件存储HDFS的SDK包含文件系统SDK和管控系统SDK。目前公测期间只提供文件系统SDK，管控操作则通过控制台进行。文件存储HDFS SDK实现了Hadoop FileSystem 接口，提供一种Hadoop兼容的文件系统，对外输出为一个单独的JAR文件，即aliyun-sdk-dfs-x.y.z.jar。借助该SDK，Apache Hadoop的计算分析应用（如MapReduce、Hive、Spark、Flink等）可以无需修改代码和编译，直接使用文件存储HDFS作为defaultFS，从而获得超越原始HDFS的功能和性能优势 。

如果您更习惯使用图形化的Web应用程序，可以使用管理控制台来管理HDFS文件系统。

费用模型

文件存储HDFS的计费项包括存储容量和预置吞吐。开通产品时默认按照实际使用量按小时计费（按量付费），同时也支持购买资源包（包年包月）的方式提前购买资源的使用额度和时长，获取更多的优惠。详情请参见云产品定价。

1.7. 表格存储

表格存储（Tablestore）是阿里云自研的结构化数据存储，提供海量结构化数据存储以及快速的查询和分析服务。表格存储提供兼容HBase的WideColumn模型、消息模型Timeline以及时空模型Timestream，实现PB级存储、千万TPS以及毫秒级延迟的服务能力。

适用场景

表格存储单表支持PB级存储、千万QPS，以及多种索引方式（全局二级索引、全文索引、倒排索引以及时空索引），被广泛用于社交互联网、物联网、人工智能、元数据和大数据等领域结构化数据业务场景。

- 元数据

  用户存储海量的文档、媒体文件等数据的同时，对文件元数据的存储和分析不可或缺。此外，电商的订单、银行流水、运营商话费账单也需要存储及分析大量的元数据。表格存储可以帮助您实现高效的元数据管理。

- 消息数据

  表格存储自研的Timeline模型主要用于消息数据，能够抽象出支撑海量Topic的轻量级消息队列，可以存储大量社交信息，包括IM聊天，以及评论、跟帖和点赞等Feed流信息。目前表格存储Timeline模型已被应用在众多IM系统中，例如支撑钉钉海量消息同步等。

- 轨迹溯源

  表格存储提供了面向轨迹类场景的Timestream模型，帮助您管理和分析跑步、骑行、健走、外卖等轨迹数据。

- 科学大数据

  多维网格数据是一种科学大数据，在地球科学领域（气象、海洋、地质、地形等）应用非常广泛，且数据规模也越来越大。相关的科学工作者有快速浏览数据的需求以及在线查询的需求，查询种类丰富、延迟要求高。表格存储可以解决科学大数据的海量存储规模和查询性能问题。

- 互联网大数据

  互联网各类电商平台以及咨讯平台的产品设计者需要汇总统计和分析各类平台的数据做为依据，决定后续的产品发展，公司的公关和市场部门也需要根据舆情作出相应的及时处理。表格存储可以帮助您实现百亿级互联网舆情存储及分析。

- 物联网

  表格存储可以满足IoT设备、监控系统等时序数据的存储需求，大数据分析SQL直读以及高效的增量流式读接口让数据完成离线分析与实时流计算。

性能

表格存储单表提供10 PB级数据量、万亿条记录数、千万级别的TPS以及毫秒级延迟的服务能力，支持自动负载均衡及热点迁移，无需人工运维，提供高吞吐写入能力以及稳定可预期的读写性能。详情请参见表格存储性能白皮书。

数据持久性和服务可用性

表格存储将数据的多个备份存储在不同机架的不同机器上，并会在备份失效时进行快速恢复，根据99.99%的高可用以及99.999999999（11个9）的可靠性标准设计。

扩展性和弹性

表格存储通过数据分片和负载均衡技术，实现了存储无缝扩展。随着表数据量的不断增大，表格存储会进行数据分区的调整从而为该表配置更多的存储。表格存储可支持不少于10 PB数据存储量，单表可支持不少于1 PB数据存储量或1万亿条记录。

安全性

表格存储提供表级别和API级别的鉴权和授权机制，支持STS临时授权和自定义权限认证及主子账号功能，实现用户级别资源隔离。详情请参见RAM和STS介绍。表格存储支持互联网、ECS内网及VPC私有网络访问，提供网络访问控制功能。

接口

表格存储提供标准的RESTful API接口，开发者一般使用工具或封装了API接口的SDK来开发应用。表格存储目前提供包括Java、Python、PHP、Go在内的多种开发语言SDK。命令行工具Tablestore CLI提供简洁、方便的管理命令，包括表操作、单行数据操作、简单压测操作、数据备份操作，支持Windows、Linux、Mac平台。客户端工具提供图形化的操作界面，支持创建、更新和删除数据表，写入、更新、读取和删除数据。

表格存储管理控制台提供实例、数据表、多元索引的创建，基本的数据读写操作，以及实例和表级别的访问监控数据（QPS、延时、请求数等）。

费用模型

使用表格存储，您可以按实际使用量付费，先使用，后付费，以较低的成本满足访问波动明显大并发低延时的需要。您也可以通过包年包月的方式，预先购买资源包，之后使用资源时，扣除相应的额度。表格存储是按使用量计费的服务，计费项包括数据存储量、读吞吐量、写吞吐量、外网下行流量，如果使用多元索引和全局二级索引，也会产生相应的费用。详情请参见计费概述。

1.8. 云存储网关

云存储网关CSG（Cloud Storage Gateway）是一款可以部署在用户本地数据中心和阿里云上的网关产品。它以阿里云对象存储OSS为后端存储，为云上和云下应用提供业界标准的文件服务（NFS和SMB）和块存储服务（iSCSI）。

云存储网关目前提供两种形态：

- 文件网关

  文件网关将OSS Bucket的对象结构与NAS文件系统的目录和文件建立映射关系，您通过标准的NFS和SMB协议即可读写指定OSS Bucket里的对象。同时，文件网关利用本地存储空间作为热数据缓存，在提供OSS Bucket海量空间的同时，保障了数据访问的高性能。文件网关还高度兼容POSIX和第三方备份软件。如果是小文件的备份和共享读写场景，推荐使用标准型或基础型文件网关；如果对性能有一定要求或者有多个客户端同时访问数据，推荐使用增强型或性能型文件网关。

- 块网关

  块网关在OSS中创建存储卷，提供Internet小型计算机系统接口（iSCSI）协议访问。本地应用程序可将这些卷作为iSCSI目标进行访问。块网关提供两种模式：透传模式和缓存模式。透传模式可以将块卷数据切片同步上云，适用于专线等高速链路客户；缓存模式提供本地缓存盘进行读写加速，缓存数据异步上云，适用于期望本地快速访问但是上云链路慢的客户。

适用场景

云存储网关适用于以下场景：

- 云存储扩容和迁移

  集成智能缓存算法，自动识别冷热数据，将热数据保留在本地缓存，保证数据访问体验，无感知的将海量云存储数据接入本地数据中心，拓展存储空间。同时在云端保留全量数据，保证数据的一致性。

- 云容灾

  随着云计算的普及，越来越多的用户把自己的业务放到了云上。但是随着业务的发展，如何提高业务的可靠性和连续性，跨云容灾是一个比较热门的话题。借助云存储网关对虚拟化的全面支持，可以轻松应对各种第三方云厂商对接阿里云的数据容灾。

- 多地数据共享和分发

  通过多个异地部署的文件网关实例，对接同一个阿里云OSS Bucket，可以实现快速的异地文件共享和分发，非常适合多个分支机构之间互相同步和共享数据。

- 适配传统应用

  有很多用户在云上的业务是新老业务的结合，老业务是从数据中心迁移过来的，使用的是标准的存储协议，例如：NFS/SMB/iSCSI。新的应用往往采用比较新的技术，支持对象访问的协议。如何沟通两种业务之间的数据是一个比较麻烦的事情，云存储网关可以起到一个桥梁的作用，便捷的沟通新旧业务，进行数据交换。

- 替代ossfs和ossftp

  ossfs和ossftp都是基于文件协议的开源工具，您可以通过它们直接上传文件到OSS。但是这两个开源文件都不支持在生产环境使用（POSIX兼容度低），同时挂载在用户的客户端需要额外的配置和缓存资源，在多个客户端的情况下安装配置繁琐。通过文件网关的服务可以替代ossfs和ossftp。通过创建文件网关，您只需要执行简单的挂载（NFS）和映射（Windows SMB）就可以像使用本地文件系统一样使用OSS。

性能

作为应用与OSS之间的云存储网关，其性能取决于多个因素，包括您本地磁盘的速度和配置、iSCSI启动器与网关之间的网络带宽、分配给网关虚拟机的本地存储量、网关虚拟机与OSS之间的带宽等。对于网关缓存，要提供对本地应用的低延迟读取访问，必须提供足够的本地缓存容量来存储最近访问的数据。文件共享的缓存区估算公式为：本地建议缓存容量=（应用带宽（MB/s）-网关后端带宽（MB/s））×写入时长（s）×1.2。如果您需要获得较好的本地访问性能，可以先预估总的热数据容量，取总的热数据容量和本地建议缓存容量的最大值为本地缓存盘容量。网关同步带宽根据OSS带宽限制制定，目前OSS为每个用户提供的最大访问带宽为10 Gbps。各区域的集群略有差异，请向各区域OSS客户支持人员查询。

云存储网关支持传输加速，充分利用网关的公网带宽，提高跨域情况下的数据传输速度。您可以在创建共享时或者共享创建之后开启传输加速。

数据持久性和服务可用性

网关缓存模式采用同步IO（Sync IO）落盘，确保掉电不丢失数据。云上网关依托于阿里云云盘的高可靠性，确保了缓存盘的数据持久可靠。本地部署的网关依赖于您虚拟环境后端存储的可靠性，建议您使用RAID存储或高可靠分布式存储作为缓存盘。网关将缓存盘的新数据刷新上传到OSS Bucket，依托OSS数据不低于99.9999999999%（12个9）的设计持久性，保证了数据的安全可靠，进而确保了数据从进入网关到上传云端整条链路的高可靠性。

扩展性和弹性

云存储网关以阿里云对象存储OSS为后端存储，因此具备OSS的高扩展性和弹性。普通的文件系统如果在同一目录下存放太多文件，经常会出现问题。而OSS总的存储容量以及单个存储空间的容量均无上限。您可以在一个存储空间内存放无限量的文件，OSS自动将您的数据副本存储至同一地域的不同服务器，所有数据副本共享阿里云的高性能基础设施能力。

安全性

云存储网关支持通过RAM管理用户身份与资源访问控制。RAM是基于用户的访问控制。您可以在一个云账户（主账户）下创建并管理多个RAM用户，并给RAM用户分配不同的授权策略，从而实现不同RAM用户拥有不同的云资源访问权限。使用RAM还可以让您避免与其他用户共享云账号密钥（AccessKey），按需为RAM用户分配最小权限，从而降低您的企业信息安全风险。详情请参见账号访问控制。

云存储网关还提供数据从网关传输至OSS的上云传输加密。您还可以选择开启OSS服务端加密并设置密钥，则通过共享目录上云的文件会在OSS端自动利用KMS密钥进行加密。

接口

您可以通过云存储网关控制台部署网关虚拟机到本地或ECS实例，然后配置文件网关或块网关，创建缓存和共享。您也可以通过API管理您的云存储网关。云存储网关API支持HTTP或者HTTPS网络请求协议，支持GET方法发送请求。

费用模型

云存储网关是按使用量收费的服务，包括线上网关和线下网关，对应的计费项不同。线上网关根据网关规格和缓存类型、数据公网带宽进行计费，支持按量计费和包年包月两种计费方式。线下网关由客户提供虚拟机和缓存资源，阿里云只收取网关软件许可证费用。详情请参见计量项和计费项。

2.阿里云存储服务优化

2.1. 概述

本文介绍如何选择和优化阿里云存储服务，帮助您在满足数据存储需求的同时节省成本。

企业和组织一般将数据存储视为辅助服务，在数据上云后不会优化存储，也不会清理未使用的存储，从而使这些服务以巨额成本长期运行。根据RightScale的博客文章，大约有7%的云上支出浪费在未使用的存储卷和旧快照（存储卷的副本）上。

阿里云提供了涵盖各种存储资源（块、文件和对象）的广泛而灵活的数据存储方案，可以让您随时在不同的存储类型之间转换。本文讨论了如何选择最适合您的阿里云存储服务，以最低成本满足您的数据存储需求，同时还讨论了如何优化这些服务，从而达到性能、可用性和持久性之间的平衡。

2.2. 数据存储需求评估

在优化存储之前，需要了解每个业务负载的性能配置文件，测量IOPS、吞吐量等性能数据。

阿里云存储服务为不同的存储场景提供存储优化方案，并没有一个通用的方案能够适用于所有的存储场景。因此，当您在评估存储需求时，请考虑对不同的业务负载分别选择不同的存储方案。

您在每个业务负载中划分数据并确定存储需求时，需要考虑以下几点：

- 数据量

  了解数据量的总大小有助于您估算存储容量和成本。

- 数据访问的频率和响应时间要求

  阿里云针对不同的访问频率和响应时间要求提供不同的存储方案，对应不同的存储价格。

- IOPS和吞吐量要求

  阿里云针对IOPS和吞吐量的不同要求提供不同的存储类型。了解IOPS和吞吐量要求将有助于您选择合适的存储类型，避免不必要的成本支出。

- 数据的重要性

  关键或受监管的数据，必须确保绝对的安全，且长时间的存储。

- 数据的敏感性

  对于高度敏感的数据，不仅要确保其不丢失和损坏，还要保护其免受意外和恶意更改。数据的持久性、安全性和成本同样重要。

2.3. 阿里云存储服务

为您的数据选择合适的阿里云存储服务，也就是在数据的可用性、持久性和性能方面找到最匹配的产品。

> **说明** 可用性是指存储产品根据请求提供数据的能力。持久性是指年平均预期数据丢失。性能是指存储产品可以提供的IOPS或吞吐量。

阿里云提供三类存储服务：对象存储、块存储和文件存储，分别满足不同的存储需求。您可以根据需要选择最适合您的存储解决方案。

对象存储

对象存储OSS（Object Storage Service）是阿里云提供的海量、安全、低成本、高可靠的云存储服务，尤其适合非结构化数据（如图片、音视频）的存储。OSS在阿里云上提供最高级别的数据持久性和可用性。其存储分为三类：标准、低频访问、归档，分别对应热数据、温数据、冷数据。就价格而言，数据越冷，存储成本越低，需要时的访问成本越高。您可以轻松地在这些存储类型之间转换以优化存储成本：

标准存储类型	高持久、高可用、高性能的对象存储服务，支持频繁的数据访问。是各种社交、分享类的图片、音视频应用、大型网站、大数据分析的合适选择。
低频访问存储类型	适合长期保存不经常访问的数据（平均每月访问频率1到2次）。存储单价低于标准类型，适合各类移动应用、智能设备、企业数据的长期备份，支持实时数据访问。
归档存储类型	适合需要长期保存（建议半年以上）的归档数据，在存储周期内极少被访问，数据进入到可读取状态需要1分钟的解冻时间。适合需要长期保存的档案数据、医疗影像、科学资料、影视素材。
冷归档存储类型	适合需要超长时间存放的极冷数据。例如因合规要求需要长期留存的数据、大数据及人工智能领域长期积累的原始数据、影视行业长期留存的媒体资源、在线教育行业的归档视频等。

OSS不同存储类型对应的存储单价如下：

OSS存储类型	存储单价（本地冗余，元/GB/月）	存储单价（同城冗余，元/GB/月）
标准	0.12	0.15
低频访问	0.08（不含数据取回费用0.0325）	0.10（不含数据取回费用0.0325）
归档	0.033（不含数据取回费用0.06）	不涉及

块存储

块存储是阿里云为云服务器ECS提供的块设备类型产品，具备高性能、低时延等特性。您可以像使用物理硬盘一样格式化并建立文件系统来使用块存储。

阿里云为您的云服务器ECS提供了丰富的块存储产品类型，包括基于分布式存储架构的云盘以及基于物理机本地硬盘的本地盘产品。其中：

- 云盘是阿里云为云服务器ECS提供的数据块级别的块存储产品，采用多副本的分布式机制，具有低时延、高性能、持久性、高可靠等性能，可以随时创建、扩容以及释放。
- 本地盘是基于云服务器ECS所在物理机（宿主机）上的本地硬盘设备，为ECS实例提供本地存储访问能力。本地盘适用于对存储I/O性能和海量存储性价比有极高要求的业务场景。具有低时延、高随机IOPS、高吞吐量、高性价比等优势。

价格上，云盘收取云盘容量费用，可以用作系统盘和数据盘。本地盘收取本地盘容量费用，只能用作数据盘。本地盘指与特定ECS实例规格绑定的本地盘，不支持单独购买，且费用计入实例规格。详细的产品类型和对应的价格信息，请参见块存储产品价格页面。

文件存储

阿里云文件存储NAS（Apsara File Storage）是面向阿里云ECS实例、E-HPC和容器服务等计算节点的文件存储服务。它是一种可共享访问、弹性扩展、高可靠以及高性能的分布式文件系统，支持NFS和SMB协议。

NAS目前提供极速型、性能型、容量型、低频型四种规格：

极速型	基于阿里云最新一代网络架构和全闪存储打造的高性能共享文件存储。最大容量256 TB，起步带宽150 MB/s，可扩展到1200 MB/s。稳定百微秒级时延。适合海量小文件、时延敏感的业务。
性能型	使用SSD作为存储介质，为应用工作负载提供高吞吐量与IOPS、低时延的存储性能。适用于高并发高吞吐，业务弹性扩展、对读时延有较高要求的文件共享存储服务。对于读写频繁、系统响应要求高的业务，有性能优势。
容量型	使用SATA HDD作为存储介质，以更低的成本提供高性能的存储空间。适用于高并发高吞吐，业务弹性扩展，成本敏感型的文件共享存储服务。对于读写访问不太频繁，时延响应要求不高的业务，有较好的成本优势。
低频型	对于不频繁访问的，长期存储的性能型或容量型数据，可以通过生命周期管理功能将其转移到低频存储空间，采用低频计费方式，从而进一步降低成本。详情请参见生命周期管理功能介绍。

NAS不同产品规格对应的存储单价如下：

NAS产品规格	存储单价（元/GB/月）
极速型	1.8
性能型	1.85
容量型	0.35
低频型	0.15

总结

对象存储OSS和文件存储NAS根据您的使用情况分配存储资源，您只需为使用量付费。但是对于块存储，无论您是否使用预分配的存储资源都需要付费。因此，在满足一定的功能需求的同时，保持较低存储成本的关键在于最大限度地使用OSS，而仅在应用程序需要时才使用带有预配置I/O的更昂贵的块存储。

2.4. 对象存储优化

对象存储OSS提供存储管理功能，帮助您优化存储性能和成本。

您可以分析数据访问模式并配置生命周期规则，自动将访问频率较低的数据转换为成本更低的存储类型，或者在到期日之后自动删除数据。为了更有效地管理存储数据，您还可以使用标签对OSS对象进行分类，并在生命周期规则中对这些标签进行过滤。

存储空间清单可以帮助您更好地了解对象的状态，简化并加速工作流和大数据作业任务等。存储空间清单功能以周为单位，对您存储空间内的对象进行扫描，扫描完成后会生成CSV格式的清单报告，并存储到您指定的存储空间内。在清单报告中，您可以有选择地导出指定对象的元数据信息，如文件大小、加密状态等。

OSS监控服务为您提供系统基本运行状态、性能以及计量等方面的监控数据指标，并且提供自定义报警服务，帮助您跟踪请求、分析使用情况、统计业务趋势，及时发现以及诊断系统的相关问题。

借助这些存储管理功能提供的信息，您可以创建策略，将访问频率较低的数据转换为成本更低的存储类型，从而节省大量费用。例如，通过将数据从标准存储转换为低频访问存储，您可以节省高达40%的OSS存储费用；而将生命周期结束后的数据转换为归档存储，您可以节省高达70%的OSS存储费用。

下表比较了OSS标准存储类型与低频访问存储类型存储1 PB数据的每月成本（包括数据取回费用）。从表中可以看出，如果每月访问10%的数据，那么使用低频访问存储可以节省31%的费用；如果每月访问50%的数据，将节省20%的费用；即使每月访问100%的数据，使用低频访问存储仍可节省6%的费用。

数据总量	数据访问量	标准存储费用（元）	低频访问存储费用（元）	节省费用
1 PB	10%	125,829	87,294	31%
1 PB	50%	125,829	100,925	20%
1 PB	100%	125,829	117,965	6%

为了进一步优化存储和数据取回的成本，OSS还推出了选取内容（SelectObject）功能。一般情况下，对象存储中的数据无论大小都必须作为一个整体进行访问。OSS SelectObject允许您使用简单的SQL语句检索对象，这意味着您的应用程序无需使用计算资源来扫描和过滤对象中的数据。使用OSS SelectObject可以将查询性能提升4倍，并将查询成本降低80%。OSS还支持对低频访问和归档存储的数据进行检索，您无需执行数据取回操作即可找到分析所需的数据。通过OSS SelectObject，您可以降低成本，获取更多数据洞察。

2.5. 块存储优化

使用块存储，您需要为预配置的容量付费，即使云盘未挂载或只有极少量的写入操作。因此，要优化块存储的性能和成本，请定期监控和识别未挂载的，以及未充分使用或过度使用的云盘，并调整配置以匹配实际的使用情况。

删除未挂载和未使用的云盘

降低成本的最简单方法是查找和删除未挂载的云盘。如果云盘没有设置为随实例自动释放，当ECS实例停止或终止时，云盘不会自动删除，费用将会继续累计，你需要执行手工删除。您还可以查看过去几周内是否有任何云盘的读写操作。如果云盘处于非生产环境，连续几周未使用，或者一个月没有挂载，建议您及时删除。

调整云盘容量

对于过度使用的云盘，您可以进行在线或离线扩容，增加单个实例的存储容量。对于ESSD云盘，您也可以选择在线升级其性能级别，从而满足性能和容量要求。

对于按量付费的ESSD云盘，您也可以选择在线降低其性能级别，从而达到降低容量和成本的目的。

当业务发生变动，当前类型的性能和价格不能满足需求时，您可以快速变更云盘类型，例如从SSD变更为ESSD。如果需要，您可以对云盘重新初始化，将其恢复到创建时的状态。

删除旧的快照

如果您创建了每天或每周获取快照的自动快照策略，快照将会大量积累。您需要定期清理不需要的快照以降低存储成本。您可以手动清理过期的快照，也可以在自动快照策略中设置快照的保留时间，自动删除超过一定时间的快照。删除快照对块存储没有影响。

使用存储容量单位包SCU

如果您的业务量固定，建议使用包年包月的云盘，时间越长，获得优惠越大。但如果您的业务量波动较大，建议使用按量付费的云盘，搭配存储容量单位包SCU，按需使用的同时享受价格优惠。SCU可以提高创建云盘的灵活性并且节约存储成本。

2.6. 持续的存储优化

维护一个规模适中且价格合理的存储架构是一个持续的过程。为了更有效地利用存储支出，您每个月都应该进行存储优化工作。您可以通过以下方式简化这项工作：

- 建立用于优化存储和设置存储策略的持续机制。
- 通过监控服务和账单密切监控存储成本。
- 使用对象标签和生命周期策略，在整个数据生命周期中持续优化数据存储。

总之，存储优化是评估数据存储需求的变化并选择最具成本效益的存储方案的持续过程。对于对象存储，使用生命周期策略自动将访问频率较低的数据转换为更低成本的存储类型。对于块存储，监控存储使用情况并调整未充分使用或过度使用的云盘容量，同时删除未挂载云盘和过期的快照，避免为未使用的存储资源付费。您可以为存储优化任务设置月度计划，使用OSS提供的各种存储管理功能来监控存储成本并评估资源使用情况，从而简化存储优化工作。

3.安全与合规

3.1. 概述

阿里云对象存储OSS（Object Storage Service）具有丰富的安全防护能力，支持服务器端加密、客户端加密、防盗链白名单、细粒度权限管控、日志审计、合规保留策略（WORM）等特性。OSS为您的云端数据安全进行全方位的保驾护航，并满足您企业数据的安全与合规要求。

OSS是目前中国国内唯一通过Cohasset Associates审计认证的云服务，可满足严格的电子记录保留要求，例如SEC Rule 17a-4（f）、FINRA 4511、CFTC 1.31等合规要求。此外，OSS已获得以下合规认证：

- ISO9001、ISO20000、ISO22301、ISO27001、ISO27017、ISO27018、ISO29151、ISO27701
- BS10012
- CSA STAR
- PCI DSS
- C5
- MTCS
- GxP
- TPN
- 可信云服务认证
- SOC 1/2/3 报告

本文对于OSS的安全能力做一个全面的介绍，包含以下内容：

访问控制	OSS提供读写权限ACL、授权策略、防盗链白名单等功能，实现存储资源访问的控制和管理。
数据加密	OSS提供服务器端加密和客户端加密，并支持基于SSL/TLS的HTTPS加密传输，有效防止数据在云端的潜在安全风险。
监控审计	OSS提供访问日志的存储和查询功能，可满足您对企业数据的监控审计需求。
数据容灾	OSS提供同城冗余存储和跨区域复制特性，实现同地域和跨地域级别的机房容灾能力。
数据保留合规	OSS支持WORM（Write once read many）特性，允许用户以“不可删除、不可篡改”方式保存和使用数据，符合美国证券交易委员会（SEC）和金融业监管局（FINRA）的合规要求。
其他特性	OSS提供版本控制功能，防止数据的误删除和覆盖。如果您的OSS Bucket遭受攻击或者分享了非法内容，OSS会自动将该Bucket切入沙箱，防止影响您其他Bucket的服务。

3.2. 访问控制

阿里云对象存储OSS提供读写权限ACL、授权策略、防盗链白名单等功能，实现存储资源访问的控制和管理。

读写权限

OSS为权限控制提供访问控制列表（ACL）。ACL是授予Bucket和Object访问权限的访问策略。 您可以在创建存储空间（Bucket）或上传对象（Object）时配置ACL，也可以在创建Bucket或上传Object后的任意时间内修改ACL。

- Bucket ACL

  Bucket ACL是Bucket级别的权限访问控制。目前有三种访问权限，含义如下：

权限值	中文名称	权限对访问者的限制
public-read-write	公共读写	任何人（包括匿名访问）都可以对该Bucket中的Object进行读/写/删除操作；所有这些操作产生的费用由该Bucket的Owner承担，请慎用该权限。
public-read	公共读	只有该Bucket的Owner或者授权对象可以对存放在其中的Object进行写/删除操作；任何人（包括匿名访问）可以对Object进行读操作。
private	私有	只有该Bucket的Owner或者授权对象可以对存放在其中的Object进行读/写/删除操作；其他人在未经授权的情况下无法访问该Bucket内的Object。

- Object ACL

  Object ACL是Object级别的权限访问控制。目前有四种访问权限，含义如下：

权限值	中文名称	权限对访问者的限制
public-read-write	公共读写	所有用户拥有对该Object的读写权限。
public-read	公共读	非Object Owner只有该Object的读权限，而Object Owner拥有该Object的读写权限。
private	私有	只有该Object的Owner拥有该Object的读写权限，其他的用户没有权限操作该Object。
default	继承Bucket	Object遵循Bucket的读写权限，即Bucket是什么权限，Object就是什么权限。

> **说明** Object的读写权限默认为继承Bucket。Object的权限大于Bucket权限。例如，设置了Object的权限是public-read，则无论Bucket是什么权限，该Object都可以被身份验证访问和匿名访问。

更多信息，请参见OSS开发指南中的读写权限ACL。

基于用户的授权策略RAM Policy

RAM（Resource Access Management）是阿里云提供的资源访问控制服务，RAM Policy是基于用户的授权策略。通过设置RAM Policy，您可以集中管理您的用户（例如员工、系统或应用程序），以及控制用户可以访问您名下哪些资源的权限，例如限制您的用户只拥有对某个Bucket里的某些对象的读权限。

RAM Policy为JSON格式，您可以通过其中的Statement描述授权语义，每条语义包含对Action、Effect、Resource和Condition的描述。您可以根据业务场景设置多条语义，实现灵活的授权策略。详情请参见OSS开发指南中的基于RAM Policy的权限控制。

STS临时授权

相对于RAM提供的长效控制机制，STS（Security Token Service）提供的是一种临时访问授权。通过STS可以返回临时的AccessKey和Token，这些信息可以直接发给临时用户用来访问OSS。一般来说，从STS获取的权限会受到更加严格的限制，并且拥有时间限制，因此这些信息泄露之后对于系统的影响也很小。

OSS可以通过阿里云STS进行临时授权访问。通过STS，您可以为第三方应用或子用户（即用户身份由您自己管理的用户）颁发一个自定义时效和权限的访问凭证。更多信息请参见OSS开发指南中的STS临时授权访问OSS。

基于资源的授权策略Bucket Policy

Bucket Policy是基于资源的授权策略。相比于RAM Policy，Bucket Policy支持在控制台直接进行图形化配置操作，并且Bucket拥有者直接可以进行访问授权。

使用Bucket Policy，您可以授予其他账号的RAM用户访问您的OSS资源的权限，也可以向匿名用户授予带特定IP条件限制的访问权限。详情请参见添加Bucket授权策略（Bucket Policy）。

防盗链白名单

对象存储OSS是按使用量收费的服务。为了减少您存储于OSS的数据被其他人盗链而产生额外费用，OSS支持设置基于HTTP和HTTPS header中表头字段Referer的防盗链方法。

您可以设置防盗链白名单，仅允许指定的域名访问OSS资源，或者仅允许HTTP或HTTPS header中包含Referer字段的请求才能访问OSS资源。对于公共读或公共读写的Bucket，防盗链白名单可以有效防止盗链，保护您的合法权益。详情请参见OSS开发指南中的防盗链。

3.3. 数据加密

对象存储OSS提供服务器端加密和客户端加密，并支持基于SSL/TLS的HTTPS加密传输，有效防止数据在云端的潜在安全风险。

服务器端加密

OSS支持在服务器端对上传的数据进行加密（Server-Side Encryption）。上传数据时，OSS对收到的用户数据进行加密，然后再将得到的加密数据持久化保存下来；下载数据时，OSS自动对保存的加密数据进行解密并把原始数据返回给用户，并在返回的HTTP请求Header中，声明该数据进行了服务器端加密。

OSS通过服务器端加密机制，提供静态数据保护。适合于对于文件存储有高安全性或者合规性要求的应用场景。例如，深度学习样本文件的存储、在线协作类文档数据的存储。针对不同的应用场景，OSS有以下两种服务器端加密方式：

- 使用KMS托管密钥进行加解密（SSE-KMS）

  上传文件时，可以使用默认KMS（Key Management Service）托管的CMK（Customer Master Key）或者指定的CMK ID进行加解密操作。这种场景适合于大量的数据加解密。数据无需通过网络发送到KMS服务端进行加解密，是一种低成本的加解密方式。

  KMS是阿里云提供的一款安全、易用的管理类服务。用户无需花费大量成本来保护密钥的保密性、完整性和可用性。借助密钥管理服务，用户可以安全、便捷的使用密钥，专注于开发加解密功能场景。用户可以通过KMS控制台中查看和管理KMS密钥。

  除了采用AES-256加密算法外，KMS负责保管用户主密钥CMK（对数据密钥进行加密的密钥），以及生成数据加密的密钥，通过信封加密机制，进一步防止未经授权的数据访问。CMK可通过使用OSS默认托管的KMS密钥的方式或者通过BYOK的方式生成，其中使用的BYOK材料可以由阿里云提供，也可以由用户自主提供。

SSE-KMS服务器端加密的逻辑示意图如下。

- 使用OSS完全托管加密（SSE-OSS）

  基于OSS完全托管的加密方式，是Object的一种属性。OSS服务器端加密使用行业标准的强加密算法AES-256（即256位高级加密标准）加密每个对象，并为每个对象使用不同的密钥进行加密。作为额外的保护，它使用定期轮转的主密钥对加密密钥本身进行加密。该方式适合于批量数据的加解密。

  该加密方式下，数据加密密钥的生成和管理由OSS负责。您可以将Bucket默认的服务器端加密方式设置为AES-256，也可以在上传Object或修改Object的元信息时，在请求中携带 `X-OSS-server-side-encryption` 并指定其值为 `AES256` ，即可实现该Object的服务器端加密存储。

更多信息请参见OSS开发指南中的服务器端加密。

客户端加密

客户端加密是指将文件（Object）发送到对象存储OSS之前在本地进行加密。使用客户端加密功能时，您需要对主密钥的完整性和正确性负责。在对加密数据进行复制或者迁移时，您需要对加密元信息的完整性和正确性负责。

使用客户端加密时，会为每个Object生成一个随机数据加密密钥，用该随机数据加密密钥明文对Object的数据进行对称加密。主密钥用于生成随机的数据加密密钥，加密后的内容会当作Object的元信息保存在服务端。解密时先用主密钥将加密后的随机密钥解密出来，再用解密出来的随机数据加密密钥明文解密Object的数据。主密钥只参与客户端本地计算，不会在网络上进行传输或保存在服务端，以保证主密钥的数据安全。

对于主密钥的使用，目前支持以下两种方式：

- 使用KMS托管用户主密钥

  当使用KMS托管用户主密钥用于客户端数据加密时，无需向OSS加密客户端提供任何加密密钥，只需要在上传对象时指定KMS用户主密钥ID（也就是CMK ID）。具体工作原理如下图所示。

- 使用用户自主管理密钥

  使用用户自主管理密钥时，需要您自主生成并保管加密密钥。当本地客户端加密Object时，由用户自主上传加密密钥（对称加密密钥或者非对称加密密钥）至本地加密客户端。其具体加密过程如下图所示。

更多信息请参见OSS开发指南中的客户端加密。

基于SSL/TLS的HTTPS加密传输

OSS支持通过HTTP或HTTPS的方式访问。您也可以在Bucket Policy中设置仅允许通过HTTPS（TLS）来访问OSS资源，实现更加安全的数据传输。安全传输层协议（TLS）用于在两个通信应用程序之间提供保密性和数据完整性。详情请参见添加Bucket授权策略（Bucket Policy）。

3.4. 监控审计

对象存储OSS提供访问日志的存储和查询功能，并支持Bucket操作日志透明化，满足您对企业数据的监控审计需求。

访问日志存储

用户在访问OSS的过程中，会产生大量的访问日志。OSS的日志存储功能可将OSS的访问日志以小时为单位，按照固定的命名规则，生成一个Object写入您指定的Bucket。您可以配置目标Bucket的生命周期管理规则，将这些日志文件转成归档存储，长期归档保存。详情请参见OSS开发指南中的访问日志存储。

实时日志查询

通过与日志服务SLS相结合，OSS还支持实时日志查询功能。您可以在OSS控制台直接查询OSS访问日志，完成OSS访问的操作审计、访问统计、异常事件回溯和问题定位等工作。实时日志查询功能能够有效提升您的工作效率，并帮助您基于数据进行决策。详情请参见OSS开发指南中的实时日志查询。

操作日志透明化

阿里云操作审计（ActionTrail）提供平台操作日志（Inner-ActionTrail）近实时投递到日志服务，进行相关分析审计服务。ActionTrail可以近实时地记录并存储阿里云OSS平台操作日志，并基于日志服务，输出查询分析、报表、报警、下游计算对接与投递等能力，满足您平台操作日志相关的分析与审计需求。详情请参见平台操作日志简介。

监控服务

OSS监控服务为您提供系统基本运行状态、性能以及计量等方面的监控数据指标，并且提供自定义报警服务，帮助您跟踪请求、分析使用情况、统计业务趋势，及时发现以及诊断系统的相关问题。有关监控服务的更多信息，请参见OSS开发指南中的监控服务。

敏感数据检测与审计

您在OSS上存储的数据可能包括一些敏感信息，例如个人隐私信息、密码/密钥、敏感图片等。如果您希望更好的针对敏感数据进行识别、分类、分级和保护，可以将OSS与敏感数据保护SDDP结合使用。SDDP可在您完成数据源识别授权后，从您的海量数据中快速发现和定位敏感数据，对敏感数据分类分级并统一展示，同时追踪敏感数据的使用情况，并根据预先定义的安全策略，对数据进行保护和审计，以便您随时了解数据资产的安全状态。详情请参见敏感数据安全防护方案。

3.5. 数据容灾

OSS提供同城冗余存储和跨区域复制特性，实现同地域和跨地域级别的机房容灾能力。

同城冗余存储

OSS采用多可用区（AZ）机制，将用户的数据分散存放在同一地域（Region）的三个可用区。当某个可用区不可用时，仍然能够保障数据的正常访问。OSS同城冗余存储提供99.9999999999%（12个9）的数据设计持久性以及99.995%的服务可用性。

OSS的同城冗余存储能够提供机房级容灾能力。当断网、断电或者发生灾难事件导致某个机房不可用时，仍然能够确保继续提供强一致性的服务能力，整个故障切换过程用户无感知，业务不中断、数据不丢失，可以满足关键业务系统对于“恢复时间目标（RTO）”以及“恢复点目标（RPO）”等于0的强需求。

目前OSS的同城冗余存储支持标准存储类型、低频访问存储类型。这两种存储类型的各项对比指标详情如下：

对比指标	标准存储类型	低频访问存储类型
数据设计持久性	99.9999999999%（12个9）	99.9999999999%（12个9）
服务可用性	99.995%	无
服务设计可用性	无	99.995%

对比指标	标准存储类型	低频访问存储类型
对象最小计量大小	按照对象实际大小计算	64 KB
最短存储时间	无最短存储时间要求	30天
数据取回费用	无	按实际获取的数据收取，单位GB
数据访问	实时访问，毫秒延迟	实时访问，毫秒延迟
图片处理	支持	支持

更多信息请参见OSS开发指南中的同城冗余存储。

跨区域复制

跨区域复制（Cross-Region Replication）是跨不同OSS数据中心（地域）的存储空间（Bucket）自动、异步（近实时）复制对象（Object），它会将Object的创建、更新和删除等操作从源存储空间复制到不同区域的目标存储空间。

跨区域复制可满足您的以下业务需求：

- 合规性要求：虽然OSS默认对每个存储的对象在物理盘上有多份副本，但合规性要求所规定的数据需要跨一定距离保存一份副本。通过跨区域复制，可以在远距离的OSS数据中心之间复制数据以满足这些合规性要求。
- 最大限度减少延迟：客户处于两个地理位置。为了最大限度缩短访问对象时的延迟，可以在地理位置与用户较近的OSS数据中心中维护对象副本。
- 数据备份与容灾：您对数据的安全性和可用性有极高的要求，对所有写入的数据，都希望在另一个数据中心显式地维护一份副本，以备发生特大灾难，如地震、海啸等导致一个OSS数据中心损毁时，还能启用另一个OSS数据中心的备份数据。
- 数据复制：由于业务原因，需要将数据从OSS的一个数据中心迁移到另一个数据中心。
- 操作原因：您在两个不同数据中心拥有分析同一组对象的计算集群，可以选择在两个不同区域中维护对象副本。

跨区域复制功能满足Bucket跨区域容灾或用户数据复制的需求。目标Bucket中的对象是源Bucket中对象的精确副本，它们具有相同的对象名、版本信息、元数据以及内容，例如创建时间、拥有者、用户定义的元数据、Object ACL、对象内容等。支持复制未加密的对象和使用SSE-KMS、SSE-OSS方式进行服务器端加密的对象。

更多信息请参见OSS开发指南中的跨区域复制介绍。

3.6. 数据保留合规

OSS支持WORM（Write once read many）特性，允许用户以“不可删除、不可篡改”方式保存和使用数据，符合美国证券交易委员会（SEC）和金融业监管局（FINRA）的合规要求。

OSS是目前中国国内唯一通过Cohasset Associates审计认证的云服务，可满足严格的电子记录保留要求，例如SEC Rule 17a-4（f）、FINRA 4511、CFTC 1.31等合规要求。详情请参见 OSS Cohasset Assessment Report。

OSS提供强合规策略，您可以针对Bucket设置基于时间的合规保留策略。当策略锁定后，用户可以在Bucket中上传和读取Object，但是在Object的保留时间到期之前，任何用户都无法删除Object和策略。Object的保留时间到期后，才可以删除Object。OSS支持的WORM特性适用于金融、保险、医疗、证券等行业。您可以基于OSS搭建“云上数据合规存储空间”。

更多信息请参见OSS开发指南中的合规保留策略。

3.7. 其他特性

OSS还提供版本控制功能，防止数据的误删除和覆盖。如果您的OSS Bucket遭受攻击或者分享了非法内容，OSS会自动将该Bucket切入沙箱，防止影响您其他Bucket的服务。

版本控制

为了防止您存储在OSS上的数据被误删除，OSS提供了针对Bucket的版本控制功能。开启了版本控制以后，针对数据的覆盖和删除操作将会以历史版本的形式保存下来。用户在错误覆盖或者删除Object后，OSS能够将Bucket中存储的Object恢复至任意时刻的历史版本。

版本控制应用于Bucket内的所有Object。当第一次针对Bucket开启版本控制后，该Bucket中所有的Object将在之后一直受到版本控制，并且每个版本都具有唯一的版本ID。您可以在开启了版本控制的Bucket中进行上传、列举、下载、删除、恢复对象等操作。您也可以暂停版本控制以停止在Bucket中继续累积同一Object的新版本。暂停版本控制后，您仍可以通过指定versionId对历史版本Object进行下载、拷贝、删除等操作。OSS会针对每个版本进行收费，您可以通过生命周期规则自动删除过期版本。

更多信息请参见OSS开发指南中的版本控制介绍。

OSS沙箱

当您的OSS Bucket遭受攻击，或者有其他用户通过您的Bucket分享违法内容，OSS会自动将Bucket切入沙箱。沙箱中的Bucket仍可以正常响应请求，但服务质量将被降级，您的应用可能会有明显感知。若您的Bucket遭受攻击，您需要自行承担因攻击而产生的全额费用。

为防止您的Bucket因攻击原因被切入沙箱，建议您使用高防IP来抵御DDoS攻击和CC攻击。为防止您的Bucket因分享涉黄、涉政、涉恐等违法内容被切入沙箱，建议您开通内容安全服务，定期针对您选中的Bucket进行检测。

更多信息请参见OSS开发指南中的OSS沙箱。