阿里云存储架构设计

之 ACE 认证考试辅导版

目录

什么是对象存储

- 阿里云对象存储OSS是阿里云提供的海量、安全、低成本、高可靠的云存储服务。其数据设计持久性不低于99.9999999999%（12个9），服务可用性（或业务连续性）不低于99.995%。
- OSS是一个分布式的对象存储服务，提供的是一个Key-Value对形式的对象存储服务。当您存储文件（Object）时，需要指定此Object的名称（Key），后续您将通过这个Key来获取该Object的内容。

基本概念

- Bucket
- Object
- Endpoint
- AccessKey
- read-after-write

Bucket（存储空间）

- 存储空间是用户用于存储对象（Object）的容器，所有的对象都必须隶属于某个存储空间。存储空间具有各种配置属性，包括地域、访问权限、存储类型等。
- 同一个存储空间的内部是扁平的，没有文件系统的目录等概念，所有的对象都直接隶属于其对应的存储空间。
- 每个用户可以拥有多个存储空间。
- 存储空间的名称在 OSS 范围内必须是全局唯一的，一旦创建之后无法修改名称。
- 存储空间内部的对象数目没有限制。

第6页

Object（对象）

- 对象是OSS存储数据的基本单元，也被称为OSS的文件。对象由元信息（Object Meta），用户数据（Data）和文件名（Key）组成。对象由存储空间内部唯一的 Key 来标识。对象元信息是一组键值对，表示了对象的一些属性，比如最后修改时间、大小等信息，同时用户也可以在元信息中存储一些自定义的信息。
- 对象的生命周期是从上传成功到被删除为止。在整个生命周期内，只有通过追加上传的 Object 可以继续通过追加上传写入数据，其他上传方式上传的 Object 内容无法编辑，您可以通过重复上传同名的对象来覆盖之前的对象。

第7页

Endpoint（访问域名）

- Region 表示 OSS 的数据中心所在物理位置。用户可以根据费用、请求来源等选择合适的地域创建 Bucket。一般来说，距离用户更近的 Region 访问速度更快。Region 是在创建 Bucket 的时候指定的，一旦指定之后就不允许更改。
- Endpoint 表示OSS对外服务的访问域名。OSS以HTTP RESTful API的形式对外提供服务，当访问不同的Region的时候，需要不同的域名。通过内网和外网访问同一个Region所需要的Endpoint也是不同的。
- 例如杭州 Region 的外网 Endpoint 是 oss-cn-hangzhou.aliyuncs.com，内网 Endpoint 是 oss-cn-hangzhou-internal.aliyuncs.com。

第8页

如何选择OSS地域

选择OSS地域时，通常需要考虑以下几个方面：

- 用户所在地
  - 尽量考虑离用户更近的地域。
- 云产品之间的关系
  - 如果您需要将OSS作为其他阿里云产品的数据源，则需要根据其他云产品的地域去选择OSS的地域。
  - 当其他云产品和OSS在同一地域时，可以通过VPC地址访问OSS。访问时不会产生流量费用，且访问速度较外网会更快。
- 资源价格
- 产品功能

第9页

AccessKey（访问密钥）

- AccessKey（简称AK）指的是访问身份验证中用到的AccessKeyId和AccessKeySecret。OSS通过使用AccessKeyId和AccessKeySecret对称加密的方法来验证某个请求的发送者身份。AccessKeyId用于标识用户；AccessKeySecret是用户用于加密签名字符串和OSS用来验证签名字符串的密钥，必须保密。对于OSS来说，AccessKey的来源有：
  - Bucket的拥有者申请的AccessKey。
  - 被Bucket的拥有者通过RAM授权给第三方请求者的AccessKey。
  - 被Bucket的拥有者通过STS授权给第三方请求者的AccessKey。

数据冗余机制

- OSS采用数据冗余存储机制，将每个对象的不同冗余存储在同一个区域内多个设施的多个设备上，确保硬件失效时的数据可靠性和可用性。
  - OSS Object操作具有强一致性，用户一旦收到了上传/复制成功的响应，则该上传的Object就已经立即可读，且数据已经冗余写入到多个设备中。
  - OSS会通过计算网络流量包的校验和，验证数据包在客户端和服务端之间传输中是否出错，保证数据完整传输。
  - OSS的冗余存储机制，可支持两个存储设施并发损坏时，仍维持数据不丢失。
    - 当数据存入OSS后，OSS会检测和修复丢失的冗余，确保数据可靠性和可用性。
    - OSS会周期性地通过校验等方式验证数据的完整性，及时发现因硬件失效等原因造成的数据损坏。当检测到数据有部分损坏或丢失时，OSS会利用冗余的数据，进行重建并修复损坏数据。

强一致性

- 对象操作在OSS上具有原子性，操作要么成功要么失败，不会存在有中间状态的Object。
- 对象操作在OSS上同样具有强一致性，用户一旦收到了一个上传（PUT）成功的响应，该上传的对象就已经立即可读，并且对象的冗余数据已经写成功。不存在一种上传的中间状态，即 read-after-write 却无法读取到数据。对于删除操作也是一样的，用户删除指定的对象成功之后，该对象立即变为不存在。

产品优势

- 不限制存储空间大小。您可以根据所需存储量无限扩展存储空间。
- 支持数据生命周期管理。您可以通过设置生命周期规则，将到期数据批量删除或者转储为更低成本的低频访问、归档存储。
- 灵活的鉴权，授权机制。提供STS和URL鉴权和授权机制、IP黑白名单、防盗链、主子账号等功能。
- OSS采用数据冗余存储机制，将每个对象的不同冗余存储在同一个区域内多个设施的多个设备上，确保硬件失效时的数据可靠性和可用性。
- 提供企业级多层次安全防护，包括服务端加密、客户端加密、防盗链、IP黑白名单、日志审计、WORM特性等。
- 提供多种数据处理能力，如图片处理、视频截帧、文档预览、图片场景识别、人脸识别、SQL就地查询等

存储类型

- OSS提供标准、低频访问、归档三种存储类型，全面覆盖从热到冷的各种数据存储场景。其中
- 标准存储类型提供高可靠、高可用、高性能的对象存储服务，能够支持频繁的数据访问；
- 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；
- 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，在三种存储类型中单价最低。

第14页

标准存储

- 提供高可靠、高可用、高性能的对象存储服务，能够支持频繁的数据访问。适用于各种社交、分享类的图片、音视频应用、大型网站、大数据分析等业务场景。
- **标准存储-本地冗余（LRS）**
  - 采用数据冗余存储机制，将每个对象的不同冗余存储在同一个区域内多个设施的多个设备上，确保硬件失效时的数据可靠性和可用性。
- **标准存储-同城冗余（ZRS）**
  - 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。
  - 对可靠性和可用性有更高要求的业务场景。

第15页

低频访问

- 提供高可靠性、较低存储成本的对象存储服务。有最低存储时间（30天）和最小计量单位（64 KB）要求。支持数据实时访问，访问数据时会产生数据取回费用，适用于较低访问频率（平均每月访问频率1到2次）的业务场景。
- **低频访问-本地冗余（LRS）**
  - 采用数据冗余存储机制，将每个对象的不同冗余存储在同一个区域内多个设施的多个设备上，确保硬件失效时的数据可靠性和可用性。
- **低频访问-同城冗余（ZRS）**
  - 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。
  - 对可靠性和可用性有更高要求的业务场景。

第16页

归档存储

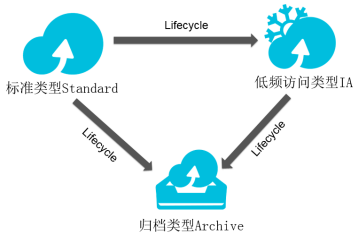
- 提供了高可靠性、极低存储成本的对象存储服务。有最低存储时间（60天）和最小计量单位（64 KB）要求。数据需解冻（约1分钟）后访问，解冻会产生数据取回费用。适用于数据长期保存的业务场景，例如档案数据、医疗影像、科学资料、影视素材等。

第17页

存储类型转换

OSS支持通过以下方式转换对象（Object）的存储类型：

- 方式一：通过生命周期规则自动转换Object的存储类型
- 方式二：通过控制台、OSS工具、SDK手动转换Object的存储类型



生命周期管理

- 生命周期规则可以定期将非热门数据转换为低频访问、归档存储，将不再需要访问的数据删除，让您更高效地管理您存储的数据，节省大量人力及存储成本。例如：
  - 某医疗机构的医疗档案，上传至OSS后半年内需要偶尔访问，半年后基本不再访问。可以通过设置生命周期规则，将已上传180天的医疗档案转为归档存储。
  - 某公司服务热线的录音文件，上传至OSS后2个月内，需要作为数据统计及核查的依据，2个月后偶尔访问，半年后基本不再访问，2年后数据不再需要存储。可以通过设置生命周期规则，设置录音文件上传60天后转为低频访问存储，180天后转为归档存储，730天后删除。
  - 某存储空间内有大量文件需要全部删除，但是手动删除每次仅可以删除最多1000个文件，比较麻烦。此时可以配置一条匹配整个Bucket的生命周期规则，设置一天后删除所有文件。此Bucket内的数据会在第二天被全部删除。

生命周期规则

- 通过生命周期规则可以批量转换存储空间内对象的存储类型，也可以批量删除指定的对象和碎片。
- 生命周期规则配置完成后24小时内会被加载，加载后的24小时内会被执行。
- 删除Object的操作是不可逆的，请根据您的需求合理设置生命周期规则。
- 通过控制台最多可配置100条生命周期规则，如需配置更多条目，请通过ossutil或SDK配置。

功能特点

- **同城容灾**：OSS采用多可用区机制，将用户的数据分散存放在同一地域的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同城冗余存储能够提供99.9999999999%（12个9）的数据设计可靠性以及99.995%的服务可用性。
- **异地容灾**：您可以通过跨区域复制功能将文件的创建、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，实现数据的异地容灾。
- **数据保留合规**：您可以创建保留策略，设置数据的保留时间。在保留时间内，您的数据无法被任何人删除。
- **加密数据**：您可以通过客户端加密和服务端加密功能，将您的数据加密后存储到OSS中。

功能特点

- **托管静态网站**：您可以将您的存储空间配置成静态网站托管模式，并通过存储空间域名访问该静态网页。
- **获取源数据内容**：您可以创建回源规则来定义通过镜像还是重定向获取源数据。回源规则通常用于数据热迁移和重定向特定请求。

数据安全

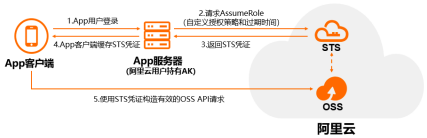
- 访问控制
  - STS临时授权访问OSS
  - 设置防盗链
- 数据容灾
  - 跨区域复制
- 数据加密
  - 服务器端加密
  - 客户端加密
- 签名
  - 在Header中包含签名
  - 在URL中包含签名

RAM 和 STS

在不暴露主账号的AccessKey的情况下安全的授权别人访问

- RAM主要的作用是控制账号系统的权限。
  - 通过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。
  - 通过使用STS来完成对于临时用户的访问授权。

STS临时授权访问OSS



1. App用户登录。App用户和云账号无关，它是App的终端用户，App服务器支持App用户登录。对于每个有效的App用户来说，需要App服务器能定义出每个App用户的最小访问权限。
2. App服务器请求STS服务获取一个安全令牌（SecurityToken）。在调用STS之前，App服务器需要确定App用户的最小访问权限（用RAM Policy来自定义授权策略）以及凭证的过期时间。然后通过扮演角色（AssumeRole）来获取一个代表角色身份的安全令牌（SecurityToken）。
3. STS返回给App服务器一个临时访问凭证，包括一个安全令牌（SecurityToken）、临时访问密钥（AccessKeyId和AccessKeySecret）以及过期时间。
4. App服务器将临时访问凭证返回给App客户端，App客户端可以缓存这个凭证。当凭证失效时，App客户端需要向App服务器申请新的临时访问凭证。例如，临时访问凭证有效期为1小时，那么App客户端可以每30分钟向App服务器请求更新临时访问凭证。
5. App客户端使用本地缓存的临时访问凭证去请求OSS API。OSS收到访问请求后，会通过STS服务来验证访问凭证，正确响应用户请求。

设置防盗链

- 防盗链功能通过设置Referer白名单以及是否允许空Referer，限制仅白名单中的域名可以访问您Bucket内的资源。OSS支持基于HTTP和HTTPS header中表头字段Referer的方法设置防盗链。
- 是否进行防盗链验证的具体场景如下：
  - 仅当通过签名URL或者匿名访问Object时，进行防盗链验证。
  - 当请求的Header中包含Authorization字段，不进行防盗链验证。

第26页

跨区域复制

- 跨区域复制（Bucket Cross-Region Replication）是跨不同OSS数据中心（地域）的Bucket自动、异步复制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。该功能能够很好的提供Bucket跨区域容灾或满足用户数据复制的需求。目标Bucket中的文件是源Bucket中文件的精确副本，它们具有相同的文件名、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、文件内容等。

第27页

服务器端加密

- 服务器端加密是将数据保存到数据中心的磁盘之前进行加密，并且在下载文件时自动进行解密。OSS提供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，可以使用指定的CMK ID或者默认KMS托管的CMK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，这是一种低成本的加解密方式。
- **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AES256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，它将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。

第28页

客户端加密

- 客户端加密：客户端加密是指将数据发送到OSS之前在用户本地进行加密，对于数据加密密钥的使用，目前支持如下两种方式：
- **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）。
- **使用用户自主管理密钥**使用用户自主管理密钥，需要用户自主生成并保管加密密钥。当用户本地客户端加密时，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。

第29页

客户端加密

- 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meta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。

签名

对OSS的HTTP请求可以根据是否携带身份验证信息分为匿名请求和带身份验证的请求。

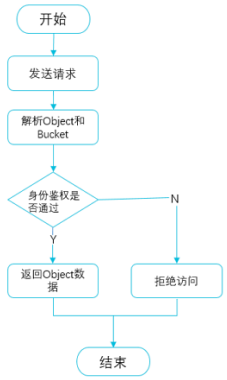
- 匿名请求指的是请求中没有携带任何和身份相关的信息；
- 带身份验证的请求指的是按照OSS API文档中规定的在请求头部或者在请求URL中携带签名的相关信息。

签名

- 对OSS的HTTP请求可以根据是否携带身份验证信息分为匿名请求和带身份验证的请求。
  - **匿名请求**指的是请求中没有携带任何和身份相关的信息；
  - **带身份验证的请求**指的是按照OSS API文档中规定的在请求头部或者在请求URL中携带签名的相关信息。

带身份验证的请求流程

1. 用户的请求被发送到OSS的HTTP服务器上。
2. OSS根据URL解析出Bucket和Object。
3. OSS根据请求的OSS的AccessKeyId获取请求者的相关身份信息，进行身份鉴权。
   - 如果未获取成功，则拒绝访问，请求结束。
   - 如果获取成功，但请求者不被允许访问此资源，则拒绝访问请求结束。
   - 如果获取成功，但OSS端根据请求的HTTP参数计算的签名和请求发送的签名字符串不匹配，则返回，请求结束。
   - 如果身份鉴权成功，则返回Object的内容给用户。



AccessKey类型

- 目前访问OSS使用的 AccessKey（AK）有三种类型。
- **阿里云账号AK**阿里云账号AK特指阿里云主账号的AK，每个阿里云账号提供的AccessKey对拥有的资源有完全控制的权限。
- **RAM子账号AK**子账号是从属于主账号的，并且这些账号下不能拥有实际的任何资源，所有资源都属于主账号。
- **STS账号AK**STS（Security Token Service）是阿里云提供的临时访问凭证服务。STS账号AK指的是通过STS颁发的AK。这组AK只能按照STS定义的规则去访问Bucket里的资源。

第34页

实现过程

- 当用户以个人身份向OSS发送请求时，其身份验证的实现如下：

1. 用户将发送的请求按照OSS指定的格式生成签名字符串。
2. 用户使用AccessKeySecret对签名字符串进行加密产生验证码。
3. OSS收到请求以后，通过AccessKeyId找到对应的AccessKeySecret，以同样的方法提取签名字符串和验证码。
   - 如果计算出来的验证码和提供的一样即认为该请求是有效的。
   - 否则，OSS将拒绝处理这次请求，并返回HTTP 403错误。

第35页

三种带身份验证的访问方法

- 使用控制台访问OSS：控制台中对用户隐藏了身份验证的细节，使用控制台访问OSS的用户无需关注细节。
- 使用SDK访问OSS：OSS提供了多种开发语言的SDK，SDK中实现了签名算法，只需要将AccessKey信息作为参数输入即可。
- 使用API访问OSS：如果您想用自己喜欢的语言来封装调用RESTful API接口，您需要实现签名算法来计算签名。包括：
  - 在Header中包含签名：您可以在HTTP请求中增加 Authorization 的Header来包含签名（Signature）信息，表明这个消息已被授权。
  - 在URL中包含签名：您可以在URL中加入签名信息，以便将该URL转给第三方实现授权访问。

第36页

回源

- 对象存储OSS提供回源功能，配置回源规则后，当您向OSS请求的数据不存在时，可以通过回源规则从设定的源地址获取到正确的数据，满足您对于数据热迁移、特定请求重定向等需求。回源方式分为镜像和重定向。
- 如果配置了**镜像回源**，当用户对该存储空间内一个不存在的文件进行GET操作时，OSS会向回源地址请求这个文件，返回给用户，同时会将该文件存入OSS。
- **重定向**功能的作用是根据设置的回源条件，以及相应的跳转的配置，向用户返回一个3xx跳转。用户可以利用这种跳转的功能对文件做重定向以及在此基础之上的各种业务。

第37页

镜像回源

- 镜像回源主要用于数据无缝迁移到OSS的场景。例如某服务已经在自己建立的源站或者在其他云产品上运行。现因业务发展，需要将数据迁移到OSS上，但是又不能停止服务，此时可以在迁移数据的同时，使用镜像回源功能保证业务的正常进行。

第38页

重定向回源

- 其他数据源向OSS的无缝迁移
  - 用户异步的从自己的数据源向OSS迁移数据，在此过程中未迁移到OSS的数据通过URL rewrite的方式返回给用户一个302重定向请求，用户的客户端根据302中的Location从自己的数据源读回数据。
- 配置页面跳转功能
  - 例如用户希望隐藏自己的某些前缀开头的object，给访问者返回一个特殊的页面。
- 配置发生404或500错误时的跳转页面
  - 发生以上错误的时候用户可以看到一个预先设定的页面，不至于系统发生错误的时候向用户完全暴露OSS的错误。

第39页

迁移案例

- 客户 A 为某互联网服务公司，主要业务架设于某云计算服务提供商 B 处，为其用户提供图片、视频等在线编辑服务。客户 A 存储在 B 处的历史数据约有1亿个文件，共320TB 左右大小，每天新增约20GB 数据，B 处的数据存储服务和 OSS 的访问带宽均为250MByte/s，业务所需带宽最高为50MByte/s。
- 现因公司发展需要，考虑将业务切换至 OSS 上。切换时需将原始数据及新增的数据迁移至 OSS，因历史数据较多，为保证公司业务正常进行，此次业务切换需做到如下要求。
  - 迁移中，需保证业务的正常进行，不能影响其用户正常读取数据。
  - 迁移完成后，需保证数据完整，业务可无缝切换。

第40页

迁移方案

- 根据客户需求及背景信息，制定了如下迁移方案。
  - 通过阿里云在线迁移服务将客户的存量数据从云服务迁移到 OSS，迁移完成前，客户业务不做变动。
  - 存量数据迁移完成后，通过 OSS 的镜像回源功能让用户可以访问到暂时未迁移至 OSS 的增量数据。
  - 客户将业务切换至 OSS。
  - 业务切换完成后，通过在线迁移服务将用户的增量数据也迁移至 OSS。
  - 数据全部迁移完成并检查无误后，删除源端数据。

第41页

思考题

1. 某视频网站采用移动端直接上传短视频，设计一个这样的上传服务的机构，应该按照什么顺序进行呢？
   ① 移动端向应用申请 STS 凭证
   ② 向应用服务返回 STS 凭证
   ③ OSS 向移动端返回上传结果
   ④ 移动端使用缓存的 STS 凭证上传视频文件
   ⑤ 应用服务向 RAM 请求 AssumeRole
   ⑥ 应用服务向移动端返回 STS 凭证

目录

什么是离线迁移

- 离线迁移（闪电立方）是阿里云提供的安全、高效、便捷的数据迁移服务。通过定制化的迁移设备（闪电立方），实现 TB 到 PB 级别的本地数据迁移上云。致力于解决大规模数据传输效率、安全问题等难题。
- 当本地机房带宽较小或无公网时，可通过离线迁移服务将数据迁移至阿里云 OSS。
- 单台设备可支持 36TB\100TB\480TB 的迁移数据能力，可多套同时使用，提升迁移效率。
- 支持多种的数据源类型：本地文件系统、NAS、HDFS、FastDFS等。
- 相比传统Internet或者专线接入的方式，成本下降 60%，迁移速度提升 20 倍。

产品优势

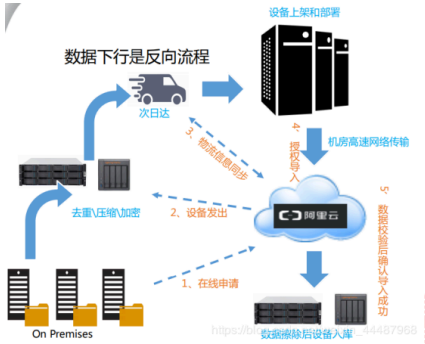
- 扩展灵活，低成本
  - 单台设备可支持 36TB\100TB\480TB 的迁移数据能力，可多套同时使用，提升迁移效率。
  - 相比传统Internet或者专线接入的方式，成本下降 60%，迁移速度提升 20 倍。
- 部署方便
  - 采用专业的数据迁移设备，标准机架和电源，可多套同时部署提升迁移效率。
  - 支持多种的数据源类型：本地文件系统、NAS、HDFS、FastDFS等。
- 安全可靠
  - 保证数据一致性：采用 CRC 技术进行读写双向校验。
  - 数据加密：提供端到端的加密机制，并通过 RAM 授权的方式运输并上传数据。
  - 数据擦除：数据迁移完毕后，通过阿里云官方数据擦除机制，确保数据不会被第三方获取。

设备类型

- 闪电立方提供三种类型的设备，分别适用不同数据量的迁移场景，可多套设备叠加使用。
- **闪电立方Mini**为塔式设备，单台支持40TB，存储计算一体，已经预装闪电立方Agent。可开机直接使用，提供图形化控制界面。
- **闪电立方-II型**：单台支持100TB，全HDD-SAS
- **闪电立方-III型**：单台支持480TB，全HDD-SAS
- 闪电立方II和闪电立方III为存储节点，需要额外的服务器部署闪电立方Agent（需要单独准备虚机或者物理机用于部署闪电立方Agent）。
- 闪电立方所有系列都有两个万兆的光口和电口，推荐提供两个10GE的交换机接口。

迁移流程

1. 创建订单创建订单并完成支付。
2. 创建OSS Bucket。
3. 收到闪电立方Mini设备并检查无误后，安装硬件。
4. 创建源数据地址。
5. 创建并执行迁移任务，完成数据到闪电立方Mini设备的迁移。
6. 关闭设备。
7. 通知阿里云取回设备。
8. 迁移完成后，请检查数据，确保无误后，申请退还押金。



源数据

- 源数据包括本地文件、远程文件系统和HDFS三种类型，您可以根据数据类型创建合适的源数据地址。
- **本地文件**：如果您的数据保存在带USB接口的移动硬盘中，请将数据所在的移动硬盘直连到闪电立方Mini设备的USB接口上，并创建本地文件的数据地址进行数据迁移。
- **远程文件系统**：如果您的数据保存在远程文件系统，例如：远程Windows文件系统、远程Linux文件系统和NAS服务器中，请将数据所在的设备，通过网线直连方式或交换机方式，连接到闪电立方Mini设备的网口或光口上，并创建远程文件系统的数据地址进行数据迁移。
- **HDFS**：如果您的数据保存在HDFS中，请您提供计算节点，将HDFS和闪电立方Mini设备都挂载至计算节点上进行数据迁移。

常见问题

- 支持哪些数据源？
  - 源端数据源：本地存储文件、本地共享存储NAS、Wos、FastDFS、HDFS等。
  - 目的端数据源：阿里云OSS、阿里云NAS。
- 是否加密数据？
  - 闪电立方离线数据迁移服务使用AES-256位加密算法加密您所有的数据。您可以自己保管加密的密码。
- 是否支持压缩？
  - 闪电立方离线数据迁移服务支持压缩，具体压缩比取决于上传的数据资料，最大可达到40:1的压缩比。

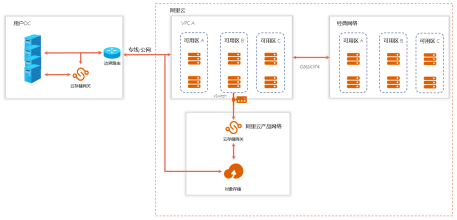
常见问题

- 使用闪电立方离线数据迁移服务可以传输多少数据？
  - 可以迁移任意数量的数据。我们已经成功为多位客户迁移几十PB的数据。您可以根据需要迁移的数据量，选择合适的闪电立方类型。我们提供闪电立方Mini（40TB），闪电立方II（100TB），闪电立方III（480TB）三种规格的设备，您也可以选择多台闪电立方设备搭配使用，实现更多数据量的迁移。
- 使用闪电立方设备迁移数据需要多长时间？
  - 数据迁移使用两个 10Gbps 的网络接口，理论上最大可支持 20Gbps 的数据传输速度。实际的传输速度同数据源的读吞吐，交换机的带宽，文件数和文件大小都有关系。

目录

什么是云存储网关

- 云存储网关（Cloud Storage Gateway：简称CSG）是一款可以部署在用户本地数据中心和阿里云上的软网关。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）。



产品形态

- **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/文件建立映射关系。用户通过标准的NFS和SMB协议即可读写指定OSS Bucket里的对象。并且利用本地存储空间作为热数据缓存，使用户在享受OSS Bucket海量空间的同时，保障数据访问的高性能。
- **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。

文件网关

- **归档支持**
  - 选择**是**，开启归档支持功能。在已归档的文件上发起读操作请求时同步发起解冻请求，请求不会报错，但存在一定的时间延迟。
  - 选择**否**，关闭归档支持功能。在已归档的文件上发起读操作请求时，需先手动解冻文件，否则请求会报错。
- **模式**
  - **复制模式**：所有数据都会保存两份拷贝，一份保存在本地缓存，另一份保存在OSS。
  - **缓存模式**：本地缓存全量元数据和经常访问的用户数据。OSS侧保持全量数据。
- **反向同步**
  - 将OSS上的元数据同步回本地。适用于网关容灾和数据恢复/共享场景。

第54页

归档管理

- 支持文件网关中的文件自动归档存储到OSS Bucket。
- 对于标准类型或者低频访问类型OSS Bucket内的文件，文件网关提供了文件系统端配置自动归档文件，解冻归档文件，查询文件归档状态的功能，不需要跳转到OSS控制台针对某个文件进行生命周期管理。
- 步骤一：设置生命周期规则
  - 您可以通过生命周期规则来批量转换OSS Bucket内对象（Object）的存储类型。
- 步骤二：归档管理配置
  - 使用网关归档管理工具sgw_archive_util进行归档，解冻和查询的操作。

第55页

本地缓存

- 本地客户端通过文件网关向OSS上传文件时，数据会先写入文件网关的缓存。当文件完全写入缓存并关闭后，文件网关会将缓存中的文件上传至OSS。如果在上传过程中有新的文件写入缓存，上传过程将会中断，等待文件完全写入缓存并关闭后，上传才会再次开始。这是因为OSS的数据更新需要原子性的全量数据，这就要求文件网关需要缓存文件的全部数据才能上传，保证客户端和OSS之间的数据一致性。
- 缓存中的文件上传完成后，文件网关会根据数据访问的热度自动淘汰已上传文件的缓存，以便接收新写入的文件。缓存淘汰机制只针对已上传的文件内容数据，对文件的元数据（文件名、目录结构、权限等）不做淘汰。

第56页

淘汰机制

- 文件网关会根据缓存的当前使用率确定是否进行淘汰，具体情况如下：
  - 当前缓存使用率低于60%时，不会触发缓存淘汰机制。
  - 当前缓存使用率为60%~80%时，文件网关会触发缓存淘汰机制，对缓存中的内容进行淘汰，直至使用率降至60%以下。
  - 当前缓存使用率超过80%时，文件网关会全速淘汰缓存中的内容，并限制前端的数据写入，避免出现缓存不足。

第57页

块网关

- **模式：**
  - **写透模式**：在写透模式下，文件会透传到阿里云OSS Bucket，直接从云端读取。
  - **缓存模式**：在缓存模式下，文件读写优先访问本地的缓存。通常在缓存模式下iSCSI网关的读写性能更好。

第58页

使用场景

- 文件网关
  - 在本地存储有限的情况下搭建一个海量文件系统的文件存储服务。
  - 将数据以对象形式存储在云端，但希望应用仍然以文件系统的方式访问文件而不需修改代码。
  - 在多个数据中心，通过文件存储服务的方式访问共享文件夹。
- 块网关
  - 通过备份软件备份数据到云上且备份软件支持iSCSI高效传输。
  - 将视频流数据通过iSCSI访问方式导入存储卷上，实现云上存储。

第59页

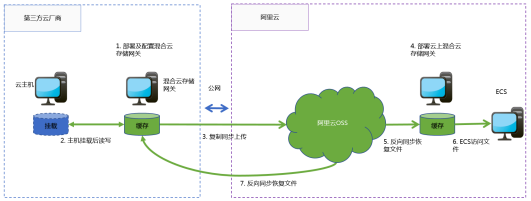
云存储扩容和迁移

- 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（冷+热）保证数据的一致性。具体的使用场景如下所示。
  - **共享文件池**：在不同计算集群之间共享文件和数据。
  - **数据备份**：通过类似Veaam，NBU等备份软件，将一些应用数据按一定策略通过云存储网关将数据备份到阿里云OSS。
  - **冷数据归档**：可以通过云存储网关将冷数据从本地或者ECS实例中通过云存储网关写入OSS的低频和归档库中，释放本地空间，提高存储的效费比。

第60页

云容灾

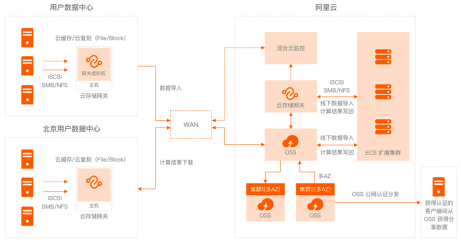
- 随着云计算的普及，越来越多的用户把自己的业务放到了云上。但是随着业务的发展，如何提高业务的可靠性和连续性，跨云容灾是一个比较热门的话题。借助云存储网关对虚拟化的全面支持，可以轻松应对各种第三方云厂商对接阿里云的数据容灾。



第61页

多地数据共享和分发

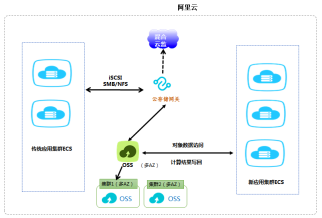
- 通过多个异地部署的文件网关实例，对接同一个阿里云OSS Bucket，可以实现快速的异地文件共享和分发，非常适合多个分支机构之间互相同步和共享数据。



第62页

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，云存储网关正好起到一个桥梁的作用，可以便捷的沟通新旧业务，进行数据交换。



第63页

目录

第64页

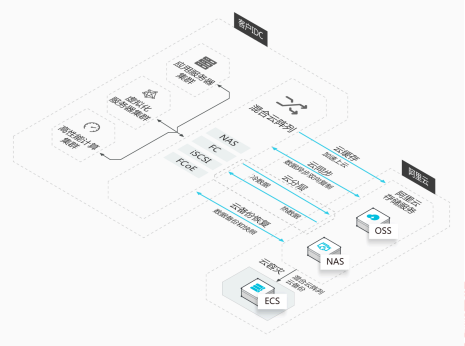
什么是混合云存储阵列

- 存储阵列
  - 硬件存储设备
  - 提供
    - 本地文件/块存储服务
    - 数据迁移上云
- 混合云存储
  - 像使用本地存储一样使用阿里云存储
- 特别适合于那些
  - 系统对传统存储阵列依赖较高
  - 对敏感数据的物理存放有特殊要求

第65页

什么是混合云存储阵列

- 数据能按照策略自动同步到云端，实现数据的云端备份容灾
- 支持自动云分层和云缓存功能，保证数据的高速访问和存储空间的有效利用
- 提供多版本快照，复制等丰富的企业数据服务
- 全冗余设计，安全可靠，支持数据中心机架部署



第66页

产品定位

- 很多企业客户希望利用公共云的易于扩展以及低成本的优势，快速上云，同时对存储有很高的性能和稳定性要求，希望敏感数据本地物理存放，满足公司政策或监管的需求，阿里云混合云存储阵列就是专门为这些客户设计的。阿里云混合云存储阵列将公共云存储的高性价比和可扩展性与本地数据中心架构相结合，能帮助客户轻松实现数据在本地数据中心和阿里云之间的无缝流动。
- 混合云存储阵列除了提供所有传统存储阵列的功能外，还集成了阿里云的云存储服务，客户在不改变现有IT架构的情况下，就能受益于公共云存储快速部署，海量扩展，按需付费的灵活性。

第67页

硬件规格

产品型号	SA2600	SA3600	SA5600
控制器	2~8控	2~16控	
控制器形态	2U12/2U25/3U48	2U12/2U25/3U48	4U
处理器（每双控）	2*Intel 6核 V4	2*Intel 10核 V4	4*Intel 10核 V4
缓存（每双控）	32/64/128GB	128/256/512GB	256/512/1024GB
缓存（每集群）	32GB~512GB	128GB~4TB	256GB~8TB
磁盘通道接口（每双控）	4*SAS 3.0	4*SAS 3.0	8*SAS 3.0
主机通道接口（每双控）	28	40	80
端口选项	16Gb FC，8Gb FC，1 / 10GbE / iSCSI，10Gb FCoE		
RAID 类型	RAID 0，1，10，5，6，50，60，分布式 RAID		
支持硬盘类型	SSD，SAS，NL-SAS		
最大硬盘数	600	1600	2800
前端协议支持	FC，FCoE，iSCSI，NFS，CIFS，OSS，FTP		
企业软件特性	快照，克隆，镜像，远程复制，智能双活，异构虚拟化，在线压缩，数据重删，加密		
混合云模式	云缓存，云分层，云复制，云快照		
云存储支持	阿里云		

第68页

常见操作

- 建立存储池
- 建立卷及LUN映射
- 卷复制
- 文件夹同步
- 建立云端整合卷
- 云端灾难恢复

第69页

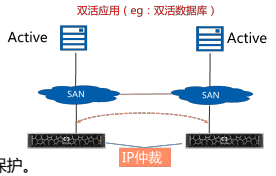
应用场景

- 双活容灾
- 异构虚拟化

第70页

双活容灾

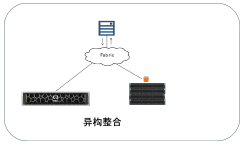
- Apsara系列提供了丰富的数据保护服务，满足最严苛应用双活需求，在前端应用到配合下可以实现本地的应用双活容灾，为企业关键业务的保驾护航。
- 镜像-卷镜像
  - 集群内单节点无后端单点存储故障。
- 本地复制-快照，克隆，备份
  - 集群内近距离站点（<10Km, 时延<1ms）
- 同步远程复制
  - 集群间（<300KM, 时延>15ms），满足对RPO=0的站点级数据保护。
- 异步远程复制
  - 集群间（>300KM），允许RPO>0的站点级数据保护，通常适用于两地三中心标准容灾架构中的远程异地中心。



第71页

异构虚拟化

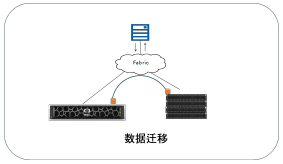
- **异构整合**
  - Apsara SA阵列可以直接接管异构阵列，并对外实行透明接管，对前端业务架构实现透明切换。
    - 依靠SA系列的透明接管，可以实现旧存储的无缝接入，支持业界95%以上品牌和型号的光纤存储（和部分IP SAN）；
    - 可实现异构存储数据迁移，迁移过程无需停机，省时省力，支持回退安全可靠；
    - 数据100%同步后可以撤走旧存储或者继续保持镜像关系运行。



第72页

异构虚拟化

- **数据迁移**
  - 对于老旧和性能比较差的阵列，Apsara可以实现对旧数据的热迁移，并且可以通过无中断迁移功能，实现卓越的效率和业务价值。
    - 帮助客户实现老旧存储的利旧整合和存储空间再利用，节约用户成本，降低管理运维复杂度
    - 可实现异构存储的在线数据迁移，降低数据迁移复杂度和业务中断时间风险
    - 同云卷功能结合，实现旧设备的快照上云备份



第73页

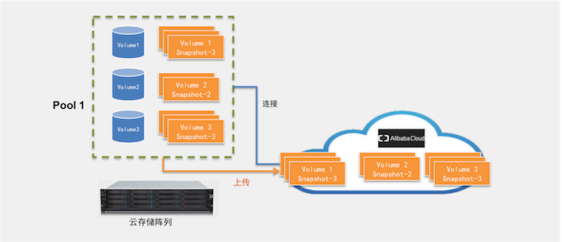
原生云集成

- 混合云存储阵列将本地存储与阿里云OSS整合在一起，为业务提供多种云功能。
- 支持云缓存，云复制和云分层模式，利用云空间扩展本地存储。

	云分层	云缓存	云复制
如果阵列故障	在云上保存部分（冷）数据	所有数据保存在云	所有数据保存在云
如果网络故障	暂时无法访问	只能访问阵列的本地热数据	所有数据可在阵列访问
数据访问性能	热数据：快，冷数据：慢	热数据：快，冷数据：慢	所有数据：快
云数据恢复	不支持	恢复到云上最近的备份	恢复到云上最近的备份

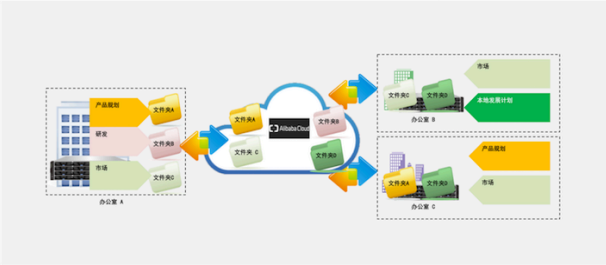
云备份

- 自动云备份简化数据管理与维护，支持用户在阵列本地存储中建立快照，并将各时间的快照镜像上传到预配置的云端OSS Bucket作为备份。



云复制

- 文件级云复制兼顾性能与数据保护，支持混合云存储阵列的本地存储和云端在文件夹级的双向数据镜像。



谢 谢

xujiajie@hotmail.com