

# 阿里云 通用解决方案

## 阿里云灾备解决方案

文档版本：20190718

# 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                                                                                                                         |
|-----------------------------------------------------------------------------------|-----------------------------------|----------------------------------------------------------------------------------------------------------------------------|
|  | 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。  |  <b>禁止：</b><br>重置操作将丢失用户配置数据。             |
|  | 该类警示信息可能导致系统重大变更甚至故障，或者导致人身伤害等结果。 |  <b>警告：</b><br>重启操作将导致业务中断，恢复业务所需时间约10分钟。 |
|  | 用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。      |  <b>说明：</b><br>您也可以通过按Ctrl + A选中全部文件。     |
| >                                                                                 | 多级菜单递进。                           | 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。                | 单击 <b>确定</b> 。                                                                                                             |
| <code>courier</code><br>字体                                                        | 命令。                               | 执行 <code>cd /d C:/windows</code> 命令，进入Windows系统文件夹。                                                                        |
| ##                                                                                | 表示参数、变量。                          | <code>bae log list --instanceid Instance_ID</code>                                                                         |
| [ ]或者[a b]                                                                        | 表示可选项，至多选择一个。                     | <code>ipconfig [-all -t]</code>                                                                                            |
| { }或者{a b}                                                                        | 表示必选项，至多选择一个。                     | <code>swich {stand   slave}</code>                                                                                         |

# 目录

---

|                            |    |
|----------------------------|----|
| 法律声明.....                  | I  |
| 通用约定.....                  | I  |
| 1 阿里云核心产品灾备设计.....         | 1  |
| 1.1 SLB高可用设计.....          | 1  |
| 1.2 ECS容灾备份设计.....         | 4  |
| 1.3 RDS容灾备份设计.....         | 6  |
| 1.4 Redis容灾备份设计.....       | 8  |
| 2 公共云同城容灾解决方案.....         | 13 |
| 3 公共云异地容灾解决方案.....         | 18 |
| 4 混合云容灾解决方案.....           | 21 |
| 5 混合云备份解决方案.....           | 24 |
| 6 混合云 数据库灾备解决方案.....       | 26 |
| 6.1 适用灾备场景.....            | 26 |
| 6.2 混合云数据库备份 解决方案架构.....   | 26 |
| 6.3 同城容灾 解决方案架构.....       | 30 |
| 6.4 两地三中心 解决方案架构.....      | 38 |
| 7 混合云多活解决方案.....           | 39 |
| 7.1 混合云多活解决方案适用灾备场景.....   | 39 |
| 7.2 混合云多活解决方案架构.....       | 40 |
| 8 操作示例 公共云跨可用区高可用解决方案..... | 44 |
| 9 附录 灾备行业趋势及基本概念.....      | 53 |
| 9.1 行业趋势与挑战.....           | 53 |
| 9.2 附录 灾备基本概念.....         | 55 |

# 1 阿里云核心产品灾备设计

## 1.1 SLB高可用设计

负载均衡（SLB）从系统设计、产品配置等多个方面提供了可用性保障。此外，您可以根据业务需求，配合使用云解析DNS等产品实现跨地域容灾。

### SLB系统的高可用

负载均衡实例采用集群部署，可实现会话同步，以消除服务器单点故障，提升冗余，保证服务的稳定性。其中四层负载均衡通过LVS（Linux Virtual Server）+ keepalived的方式实现，七层负载均衡通过Tengine（淘宝网发起的Web服务器项目，在Nginx的基础上，针对有大访问量的网站需求进行了优化）实现。

来自公网的请求通过等价多路径路由（ECMP）到达LVS集群，LVS集群内的每台LVS通过组播报文将会话同步到该集群内的其它LVS机器上，从而实现LVS集群内各台机器间的会话同步。同时，LVS集群会对Tengine集群进行健康检查，将异常机器从Tengine集群移除，保证七层负载均衡的可用性。

#### 最佳实践：

会话同步可以保证长连接不受集群内服务器故障的影响，但是对于短连接或连接未触发会话同步规则时（未完成三次握手），集群内的服务器故障仍可能会影响用户请求。为了防止集群中某台机器故障导致的会话中断，您可以在业务逻辑中加入重试机制，降低对用户访问造成的影响。

### 单SLB实例的高可用

为了向广大用户提供更稳定可靠的负载均衡服务，阿里云负载均衡已在大部分地域部署了多可用区以实现同地域下的跨机房容灾。当主可用区出现故障或不可用时，负载均衡有能力在非常短的时间内（约30秒）切换到备可用区并恢复服务；当主可用区恢复时，负载均衡同样会自动切换到主可用区提供服务。



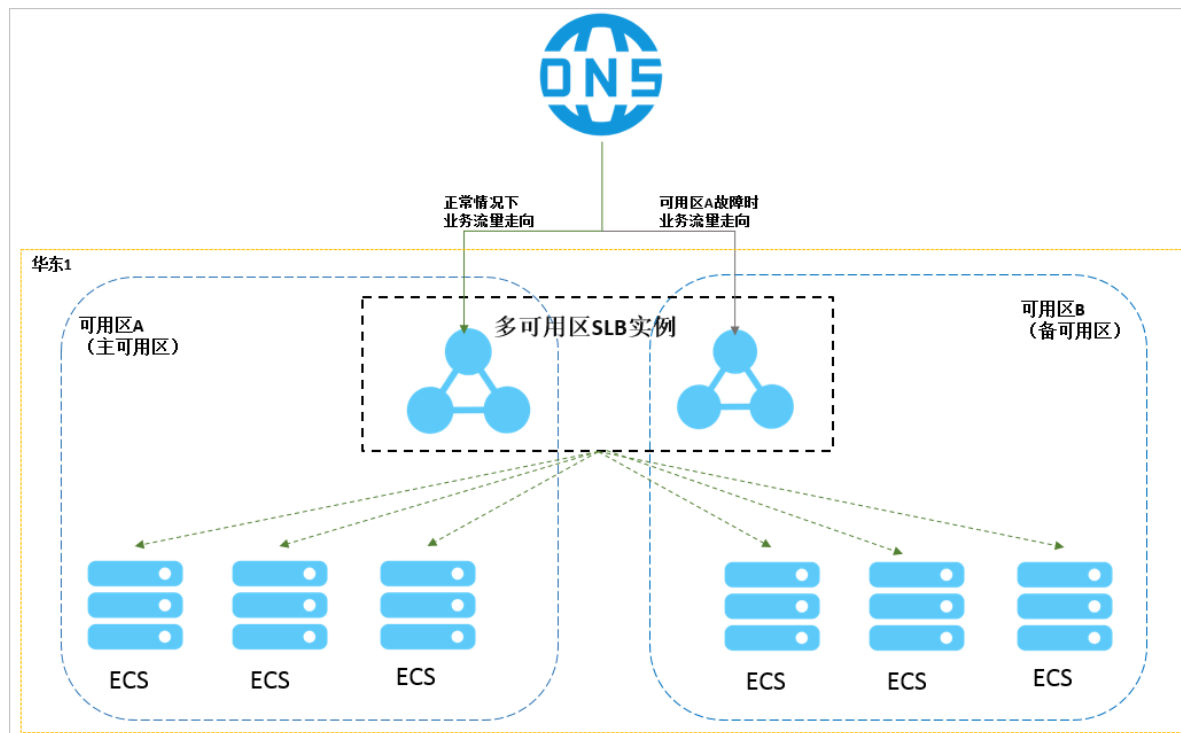
#### 说明：

负载均衡的主备可用区是可用区级别的容灾。只有当主可用区整体不可用时，如机房整体断电、机房出口光缆中断等，负载均衡才会切换到备可用区。而并非某个实例出现故障，就切换到备可用区。

#### 最佳实践：

1. 为了更好的利用负载均衡的主备可用区机制，建议您在支持主备可用区的地域创建负载均衡实例，即在购买负载均衡实例时选择可用区类型为多可用区的地域。
2. 当您选择SLB的主备可用区时，可以根据ECS实例的可用区分布进行选择。大部分ECS实例位于哪个可用区，就将哪个可用区选择为SLB的主可用区，以获取最小的访问延迟。

但是并不建议您将全部ECS实例都部署在一个可用区内，您也需要在SLB的备可用区部署少量ECS实例，以便在极端情况下（主可用区整体不可用时），切换到备可用区后仍旧可以正常处理负载均衡转发的请求。

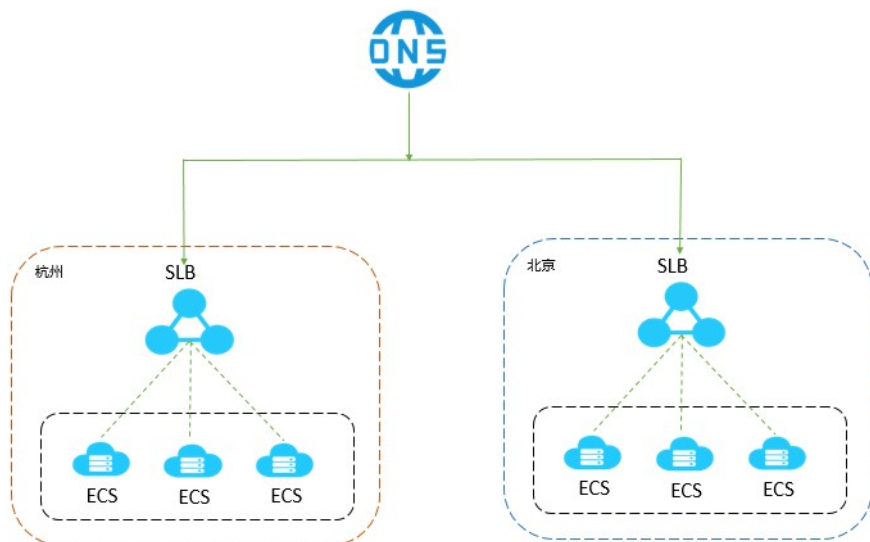


### 多SLB实例的高可用

如果您对可用性的要求特别高，负载均衡实例自身的可用性保障机制可能无法满足您的需求。例如当网络攻击或配置错误等情况导致负载均衡实例不可用时，由于未出现可用区级故障，不会触发负载均衡实例的可用区切换。此时，您可以创建多个SLB实例，通过云解析DNS对访问进行调度，或通过全球负载均衡解决方案实现跨地域容灾备份。

#### 最佳实践：

您可以在一个地域内的多个可用区或多个地域内部署负载均衡实例和后端ECS实例，然后使用云解析DNS对访问进行调度。



### 后端ECS实例的高可用

负载均衡通过健康检查来判断后端ECS实例的可用性。健康检查机制提高了前端业务整体可用性，避免了后端ECS异常对总体服务的影响。

开启健康检查功能后，当后端某个ECS实例健康检查出现异常时，负载均衡会自动将新的请求分发到其他健康检查正常的ECS实例上；而当该ECS实例恢复正常运行时，负载均衡会将其自动恢复到负载均衡服务中。关于健康检查的详细机制，请参见 [健康介绍](#)。

#### 最佳实践：

为了使健康检查功能正常运作，您需要开启并正确配置健康检查。具体的操作流程请参见 [配置健康检查](#)。

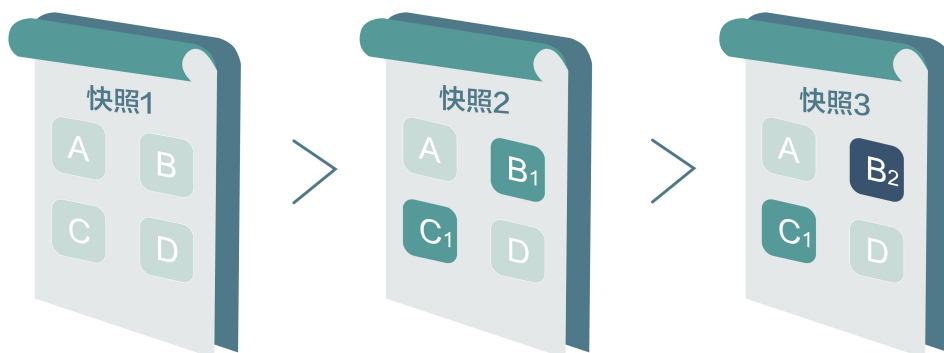
## 1.2 ECS容灾备份设计

保障企业业务稳定、IT系统功能正常、数据安全十分重要，可以同时保障数据备份与系统、应用容灾的灾备解决方案应势而生，且发展迅速。ECS可使用快照、镜像进行备份。

### 灾备设计

#### · 快照备份

阿里云ECS可使用快照进行系统盘、数据盘的备份。目前，阿里云提供快照2.0服务，提供了更高的快照额度、更灵活的自动任务策略，并进一步降低了对业务I/O的影响。使用快照进行备份时，第一次备份为全量备份，后续为增量备份，备份所需时间与待备份数据量有关。



例如，快照1、快照2和快照3分别是磁盘的第一个、第二个和第三个快照。文件系统对磁盘的数据进行分块检查，当创建快照时，只有变化了的数据块，才会被复制到快照中。阿里云ECS的快照备份可配置为手动备份，也可配置为自动备份。配置为自动备份后可以指定磁盘自动创建快照的时间（24个整点）、重复日期（周一到周日）和保留时间（可自定义，范围是1-65536天，或选择永久保留）。

#### · 快照回滚

当系统出现问题，需要将一块磁盘的数据回滚到之前的某一时刻，可以通过[快照回滚](#)实现，前提是该磁盘已经创建了快照。



说明:

- 回滚磁盘是不可逆操作，一旦回滚完成，原有的数据将无法恢复，请谨慎操作。
- 回滚磁盘后，从所使用的快照的创建日期到当前时间这段时间内的数据都会丢失。

#### · 镜像备份

镜像文件相当于副本文件，该副本文件包含了一个或多个磁盘中的所有数据，对于ECS而言，这些磁盘可以是单个系统盘，也可以是系统盘加数据盘的组合。使用镜像备份时，均是全量备份，且只能手动触发。

- 镜像恢复

阿里云ECS支持使用快照创建自定义镜像，将快照的操作系统、数据环境信息完整的包含在镜像中。然后使用自定义镜像创建多台具有相同操作系统和数据环境信息的实例。ECS的快照与镜像配置请参考[快照与镜像](#)。



说明:

创建的自定义镜像不能跨地域使用。

## 技术指标

RTO和RPO：与数据量大小有关，通常而言是小时级别。

## 应用场景

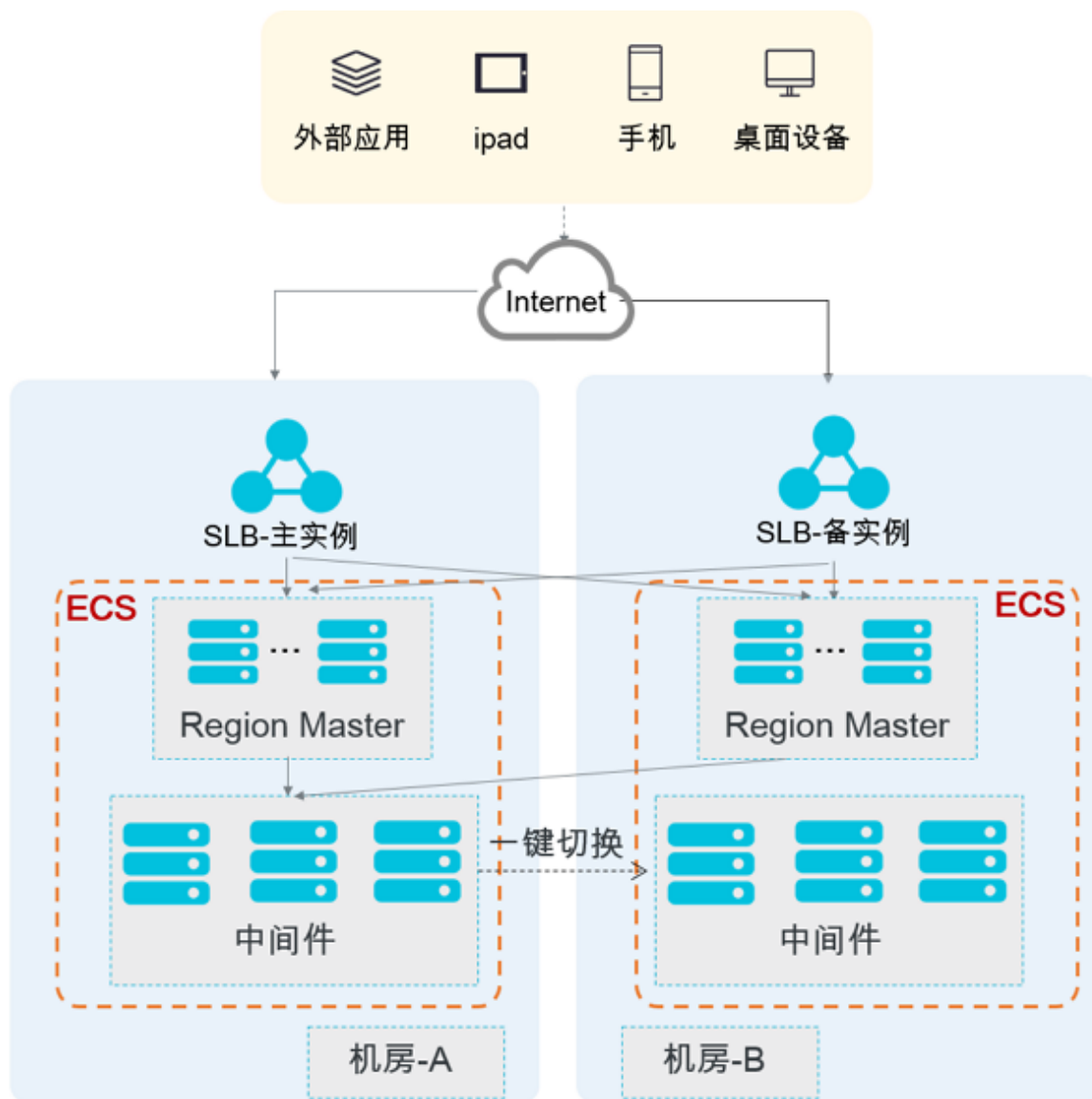
- 备份恢复

阿里云ECS可通过快照与镜像对系统盘、数据盘进行备份。如果存储在磁盘上的数据本身就是错误的数据，比如由于应用错误导致的数据错误，或者黑客利用应用漏洞进行恶意读写，此时就可以使用快照服务将磁盘上的数据恢复到期望的状态。另外ECS可通过镜像重新初始化磁盘或使用自定义镜像新购ECS实例。

- 容灾应用

ECS可以从架构上来实现容灾场景下的应用，比如：在应用前端购买SLB产品，后端相同应用部署至少两台ECS服务器，或者是使用阿里云的弹性伸缩技术，根据自定义ECS自身资源的使用规

则来进行弹性扩容。这样即便其中一台ECS服务器故障或者资源利用超负荷，也不会使服务对外终止，从而实现容灾场景下的应用。以同城两机房部署ECS集群为例：



- ECS在两机房均部署集群，接入侧通过SLB做两机房的接入流量负载均衡。
- 两机房部署的Region Master节点是对等的，单Region Master节点故障不影响ECS的管控功能。
- ECS的管控节点机房级故障切换，主要是对管控集群依赖的中间件域名重新绑定。如管控节点机房级故障，需重新将中间件域名绑定至另一个机房的管控节点。

## 1.3 RDS容灾备份设计

### 数据备份与恢复

- RDS默认提供备份功能，支持自动备份和手动备份。您可以设置自动备份的周期，还可以根据自身业务特点随时发起备份。更多信息请参考[备份恢复](#)。

- RDS默认支持按备份集和指定时间点进行数据恢复。在大多数场景下，您可以将7天内任意一个时间点的数据恢复到RDS临时实例或克隆实例上，数据验证无误后即可将数据迁回RDS主实例，从而完成数据回溯。更多信息请参考[备份恢复](#)。
- 除了默认的备份恢复功能，RDS for MySQL还提供跨地域备份恢复功能，详情请参见[跨地域备份和跨地域恢复](#)。

## 同城容灾

| 系列     | 说明                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 基础版    | <ul style="list-style-type: none"> <li>· 数据备份存储在OSS或分布式云盘上，通过多副本冗余确保数据不会丢失。（所有RDS实例均是如此。）</li> <li>· 只包含一个节点，没有备节点作为热备份，因此当发生故障时，恢复时间较长。适用于对可用性要求不高的场景。</li> </ul>                                                                                                                                                                                                                                                                                 |
| 高可用版   | <p>采用一主一备的双机热备架构，适合80%以上的用户场景。主节点故障时，主备节点秒级完成切换，整个切换过程对应用透明；备节点故障时，RDS会自动新建备节点以保障高可用。</p> <ul style="list-style-type: none"> <li>· 单可用区实例：主备节点位于同一个可用区。主备节点位于两台不同的物理服务器上，可用区内的机柜、空调、电路、网络都有冗余，保障高可用性。</li> <li>· 多可用区实例（也称为同城双机房或者同城容灾实例）：主备节点位于同一地域的不同可用区，提供跨可用区的容灾能力，且不额外收费。</li> </ul> <div>  说明：<br/>单可用区实例和多可用区实例可以互相转换，具体请参见<a href="#">迁移可用区</a>。 </div> |
| 集群版    | <p>最大支持一主一备高可用架构和七个只读节点，支持横向扩展集群读能力，备节点和所有只读节点都是从主节点同步数据。集群版的高可用能力与高可用版相同，而且只读节点可以创建在和主备节点不同的其它可用区。</p> <div>  说明： <ul style="list-style-type: none"> <li>· 仅RDS for SQL Server 2017提供集群版，详见<a href="#">集群版</a>。</li> <li>· 关于RDS for MySQL的只读实例，详见<a href="#">只读实例</a>。</li> <li>· 关于POLARDB集群的只读节点，详见<a href="#">POLARDB集群</a>。</li> </ul> </div>             |
| 三节点企业版 | <ul style="list-style-type: none"> <li>· RDS for MySQL 5.6/5.7支持三节点企业版（原金融版），详见<a href="#">三节点企业版</a>。</li> <li>· 采用一主两备的三节点架构，通过多副本同步复制，确保数据的强一致性，提供金融级的可靠性，适用于各行业大型企业的核心生产数据库。</li> <li>· 三节点企业版实例的三个节点总是位于同一地域的三个不同的可用区。</li> </ul>                                                                                                                                                                                                             |

## 异地容灾

- 您可以通过数据传输服务（DTS）实现主实例和异地灾备实例之间的实时同步。主实例和灾备实例均具备主备高可用架构，当主实例所在区域发生突发性自然灾害等状况，主实例的主备节点均无法连接时，可将异地灾备实例切换为主实例，在应用端修改数据库连接地址，即可快速恢复应用的业务访问。具体请参见[灾备实例](#)。
- 您也可以将自建机房的数据库或者ECS上的自建数据库实时同步到任一地域的RDS实例。即使发生机房损毁的灾难，数据永远在阿里云数据库上有备份。具体操作请参见[创建实时同步作业](#)。

## 1.4 Redis容灾备份设计

数据是很多业务的核心元素，作为数据载体的数据库承担着举足轻重的责任。云数据库 Redis 版作为高性能的 Key-Value 数据库，在业务场景中往往承载着大量的重要数据。本文将全方位地为您解析云数据库 Redis 版的灾备机制。

### 云数据库Redis版容灾架构演进

程序在运行过程中总会遇到各种各样的问题，例如程序BUG、设备故障、机房断电等，理想的容灾机制能够在这些问题发生时，保证数据的一致性和业务可用性。云数据库Redis版为了保证业务的高可用，不断提升容灾能力，为不同的业务场景提供相应的高可用方案。

下图反映了云数据库Redis版容灾架构的演进历史。

图 1-1: Redis容灾架构演进

当前三种方案同时存在，您可以根据业务需求选择合适的方案。下文将对各方案进行详细介绍。

### 单可用区高可用机制

Redis全系列均支持单机房高可用架构。HA监控系统采用独立的平台化架构，提供跨可用区的高可用机制，使云数据库Redis版比自建Redis更稳定。

#### 标准版-双副本

**标准版-双副本**实例采用双机主从（Master-Replica）架构，高可用HA模块检测到主节点故障时，会自动进行主从切换，将Replica提升为Master，而原来的Master恢复连接后会成为新的Replica。实例默认开启数据持久化功能，支持数据自动备份，您可以使用备份文件回滚实例或者克隆实例，有效地解决误操作问题并实现可靠的灾备。

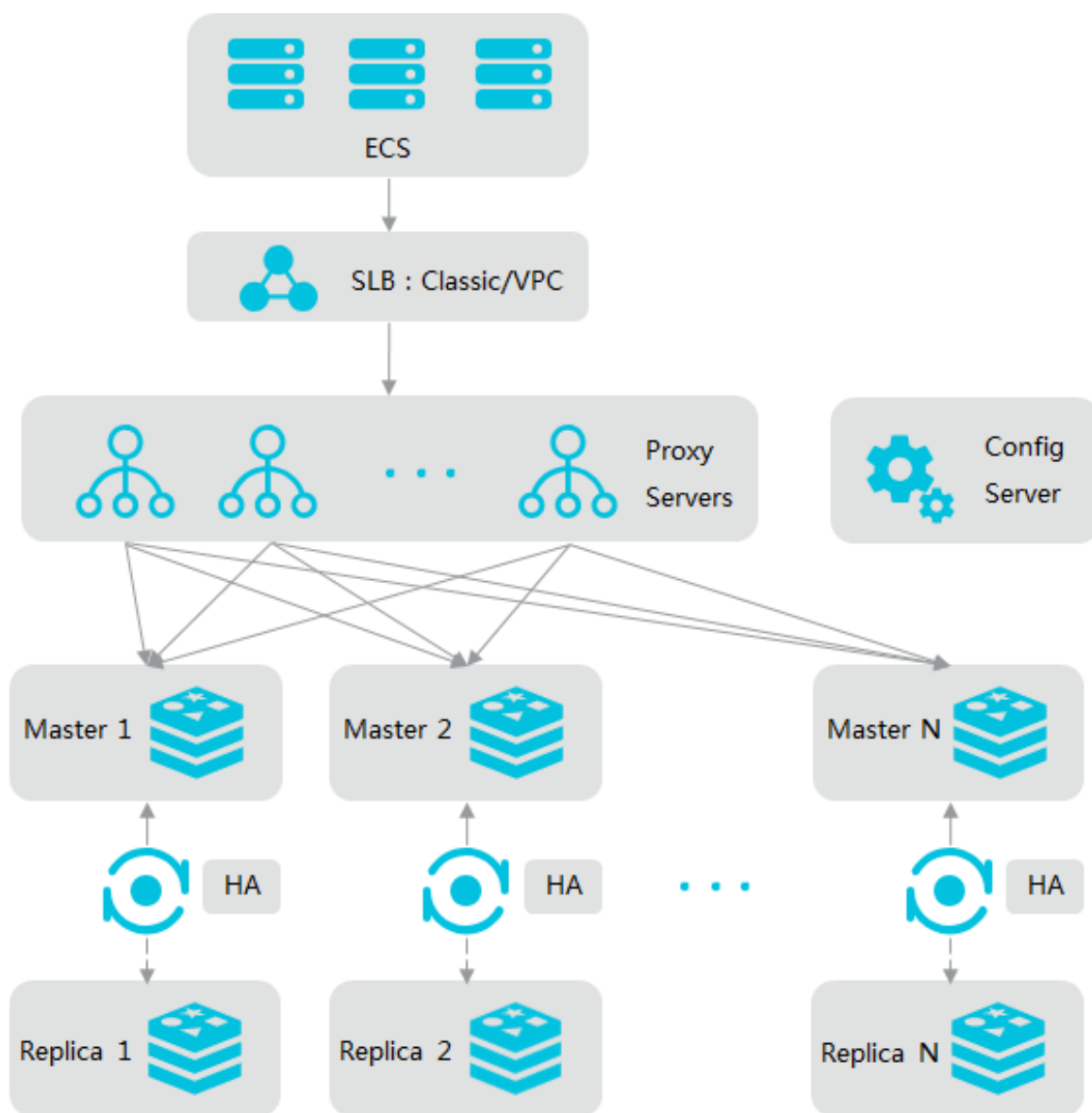
图 1-2: 标准版-双副本高可用架构

## 集群版-双副本

集群版-双副本实例由配置服务器、代理服务器和分片服务器组成：

- 配置服务器（Config Server）是用于提供全局路由信息和配置信息的集群管理工具，采用遵循Raft协议的三副本集群架构；
- 代理服务器（Proxy Server）为单节点架构，集群版结构中会有多个Proxy，系统自动对所有Proxy进行负载均衡及故障转移；
- 分片服务器（Shard Server）同样采用双副本高可用架构，与标准版-双副本实例相同，主节点故障之后，HA模块会自动进行主从切换保证服务高可用，并更新Proxy Server和Config Server的信息。

图 1-3: 集群版-双副本高可用架构

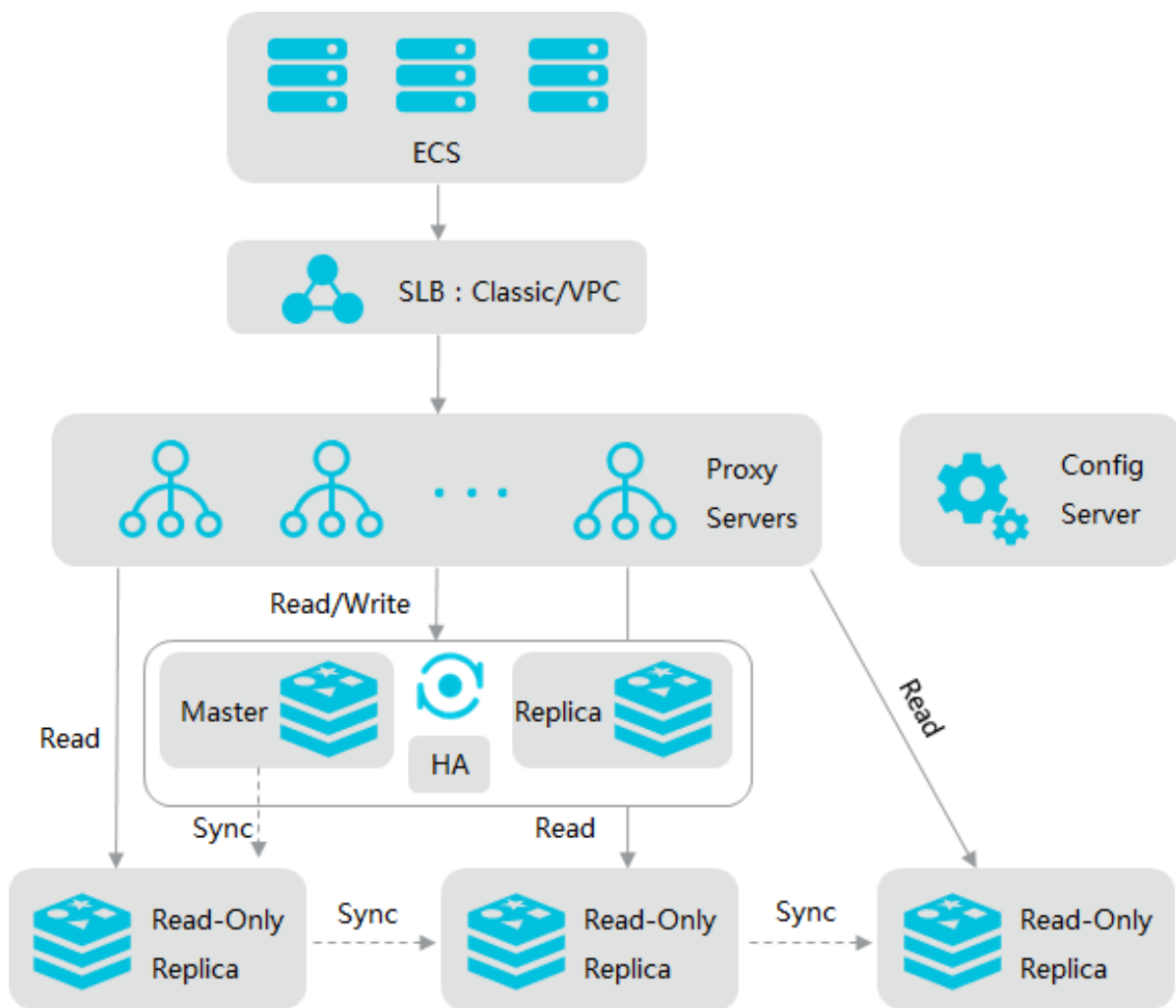


## 读写分离版

**读写分离版**实例由代理服务器、主从架构的读写节点以及若干只读副本（Read-Only Replica）构成。

- 高可用HA模块实时监测各节点的状态，在读写节点的主节点发生故障时发起主从切换，同时将只读节点连接到新的主节点上来；
- 当只读节点发生故障时，HA模块将重建只读节点，并更新相应的路由及权重信息。
- Proxy实时监控只读节点的服务状态，当发现某个只读节点状态异常时会降低该节点的权重。如果只读节点多次连接失败，Proxy将停止该节点的服务，直至其恢复正常。

图 1-4: 读写分离版高可用架构



## 同城容灾机制

Redis标准版和集群版提供跨双机房的同城容灾架构。如果业务为单一地域部署，且对容灾要求较高，可在创建云数据库 Redis版实例时，选择支持同城容灾的可用区，如下图中的华东1多可用区（B+F）或华东1多可用区（G+H）。

图 1-5: 创建同城容灾实例

创建多可用区实例时，备机房将创建与主机房相同规格的Replica实例，主备机房的实例数据通过专门的复制通道同步。

当主机房出现电力或网络问题时，Replica实例将升级为Master实例，系统调用Config Server接口为Proxy更新路由信息。底层网络根据路由精细度实现故障切换，主机房网段的精细度高，因此在下述情况下，数据会直接传输到主机房的实例；当主机房出现故障时，不会上传路由明细信息，此时骨干网中只存在备机房的精细度较低的大网段路由信息，系统就会自动把请求路由到备机房，从而实现故障切换。

云数据库Redis版优化了Redis的同步机制，在同步位点上借鉴MySQL的GTID，实现了全局OpID，并且查找OpID的操作通过后台线程无锁进行。同时，发送AOF binlog是异步同步的过程，可以限流，保障了Redis服务的性能。

图 1-6: 同城容灾实例的数据同步过程

## 跨地域容灾

云数据库 Redis 版提供了全球范围的异地多活服务，即 **Redis 全球多活**，适用于需要在多地域同步部署的业务场景，与传统的灾备方案最大的区别在于多活。异地多活架构使业务能够在多个地域同时进行，各地域中的全球多活子实例实时双向同步。

Redis 全球多活实例由多活子实例、同步通道以及通道管理器构成。

- 多活子实例是基本服务单元，所有子实例均可读写；
- 同步通道支持子实例间的实时双向同步，支持断点续传，对传输中断的容忍度达到了天级别；
- 通道管理器管理同步通道的生命周期，同时处理子实例在故障时的主从切换以及备份重搭，保证多活实例的高可用。

图 1-7: 全球多活同步架构



说明:

子实例间通过异步复制进行同步，不影响 Redis 的服务性能。

使用 Redis 全球多活架构时，可在业务端设置切换条件，使得业务流量在某一地域出现问题时切换到另一地域的子实例上，保证业务的可用性。Redis 全球多活实例的创建方法请参考 [创建多活实例](#)

。

## 2 公共云同城容灾解决方案

当企业的业务原先即已部署在阿里云上，可采用阿里云的公共云同城容灾解决方案，使用阿里云DNS、SLB等产品，搭建同地域多可用区容灾系统架构，实现同城容灾。

### 公共云同城容灾适用场景

公共云同城灾备解决方案适用的灾备场景为：

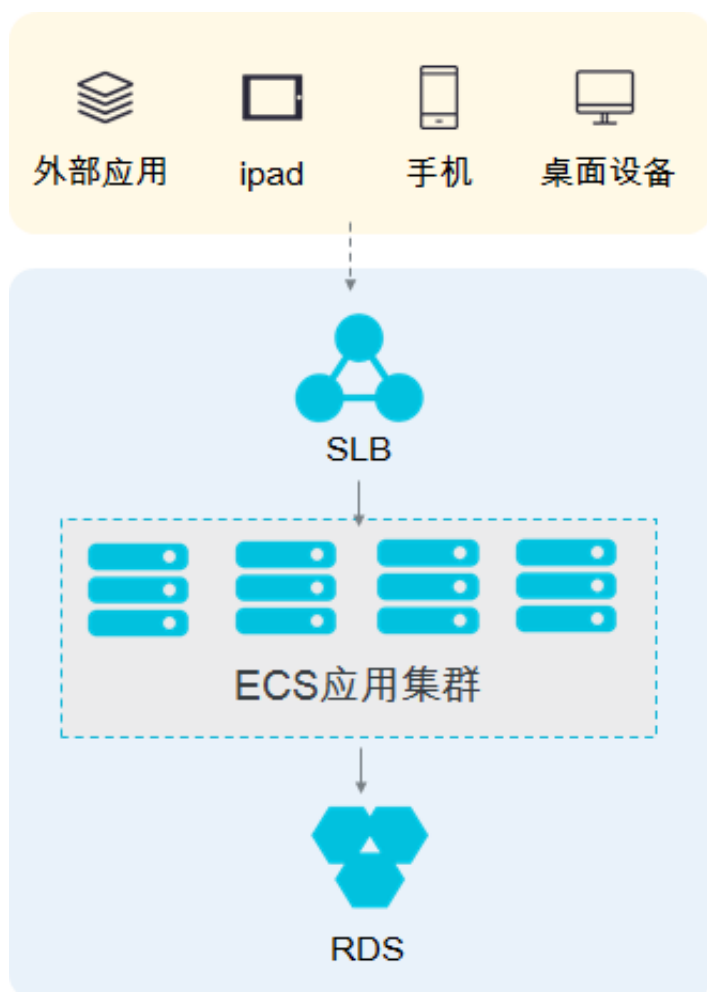
- 公共云形态：企业业务已部署在阿里云上，希望在阿里云的同地域的不同可用区搭建同城容灾架构。
- 应用级：企业希望对整体的应用做容灾备份，而非单独的数据库或存储。
- 云上同城灾备：应对公共云上某地域可用区故障场景，例如：
  - 企业正使用的云产品实例不可用。
  - 可用区的某产品的集群级别的性能衰减或不可用。
  - 基础设置故障导致的整个可用区故障。



说明：

同城容灾的基本概念及技术指标可参考 [容灾备份基本概念](#) 章节。

使用以下阿里云SLB、ECS、RDS、OSS即可搭建一个最简IT系统，如下图所示。

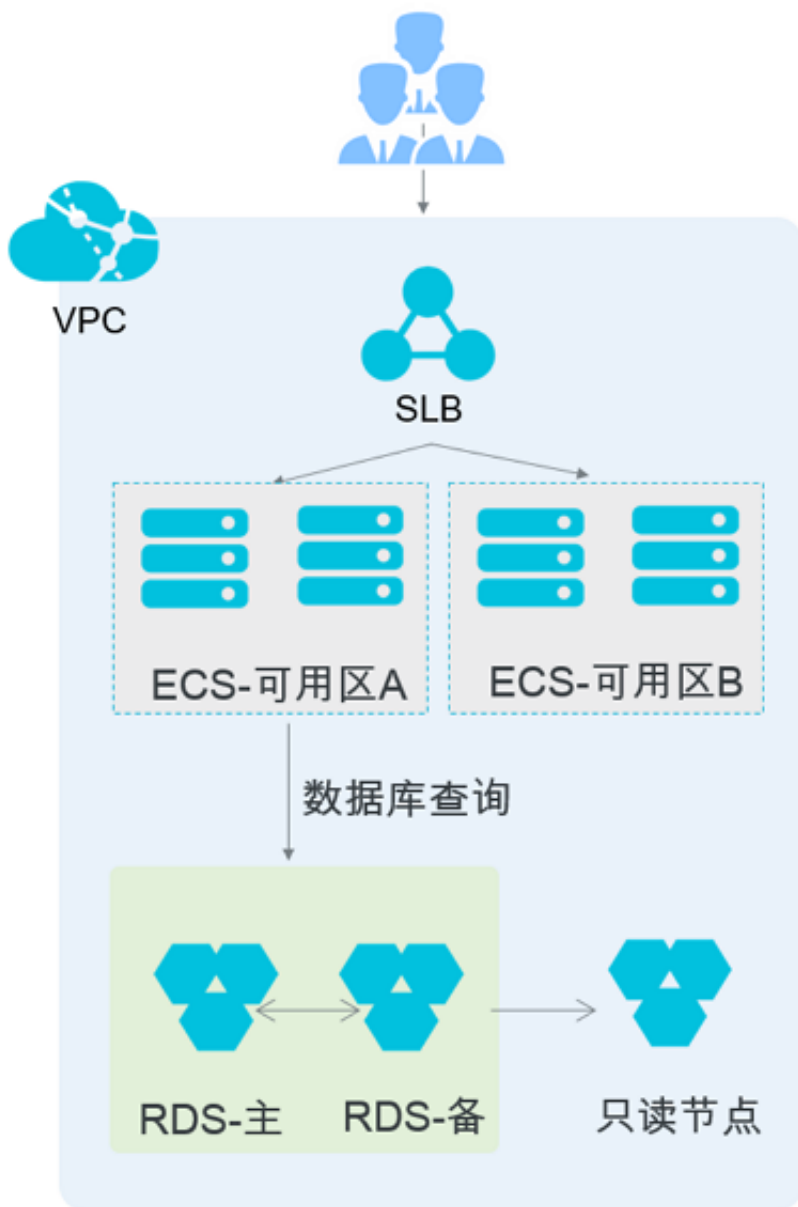


- SLB: Server Load Balancer, 是对多台云服务器进行流量分发的负载均衡服务, 在整个IT系统中, SLB是服务的对外接口, 流量入口。阿里云SLB可通过多可用区来消除单点故障, 保障系统的稳定性。详细的灾备设计及技术指标见 [SLB](#) 章节。
- ECS: Elastic Compute Service, 是一种简单高效、处理能力可弹性伸缩的计算服务, 在整个IT系统中提供计算能力。ECS可使用镜像、快照进行备份, 详细的设计及技术指标见 [ECS](#) 章节。
- OSS: Object Storage Service, 是阿里云提供的海量、安全、低成本、高可靠的云存储服务。在整个IT系统中提供非结构化、半结构化的存储能力, 详细的灾备设计及技术指标见 [OSS](#) 章节。
- RDS: Relational Database Service, 是一种稳定可靠、可弹性伸缩的在线数据库服务。在整个IT系统中提供关系型数据库能力, 详细的设计及技术指标见 [RDS](#) 章节。

企业的复杂IT系统亦可根据业务拆分为不同子系统, 每个子系统参考上述最简IT系统单独购置搭建, 最终组成一个完成企业较为复杂的IT系统。因此, 以下以最简IT系统为例, 示例公共云上的容灾解决方案推荐架构。

## 公共云同城容灾 通用架构

中小型企业业务量不是特别大，对异地容灾要求不是特别强烈，在阿里云平台上可采用以下同城容灾方案：



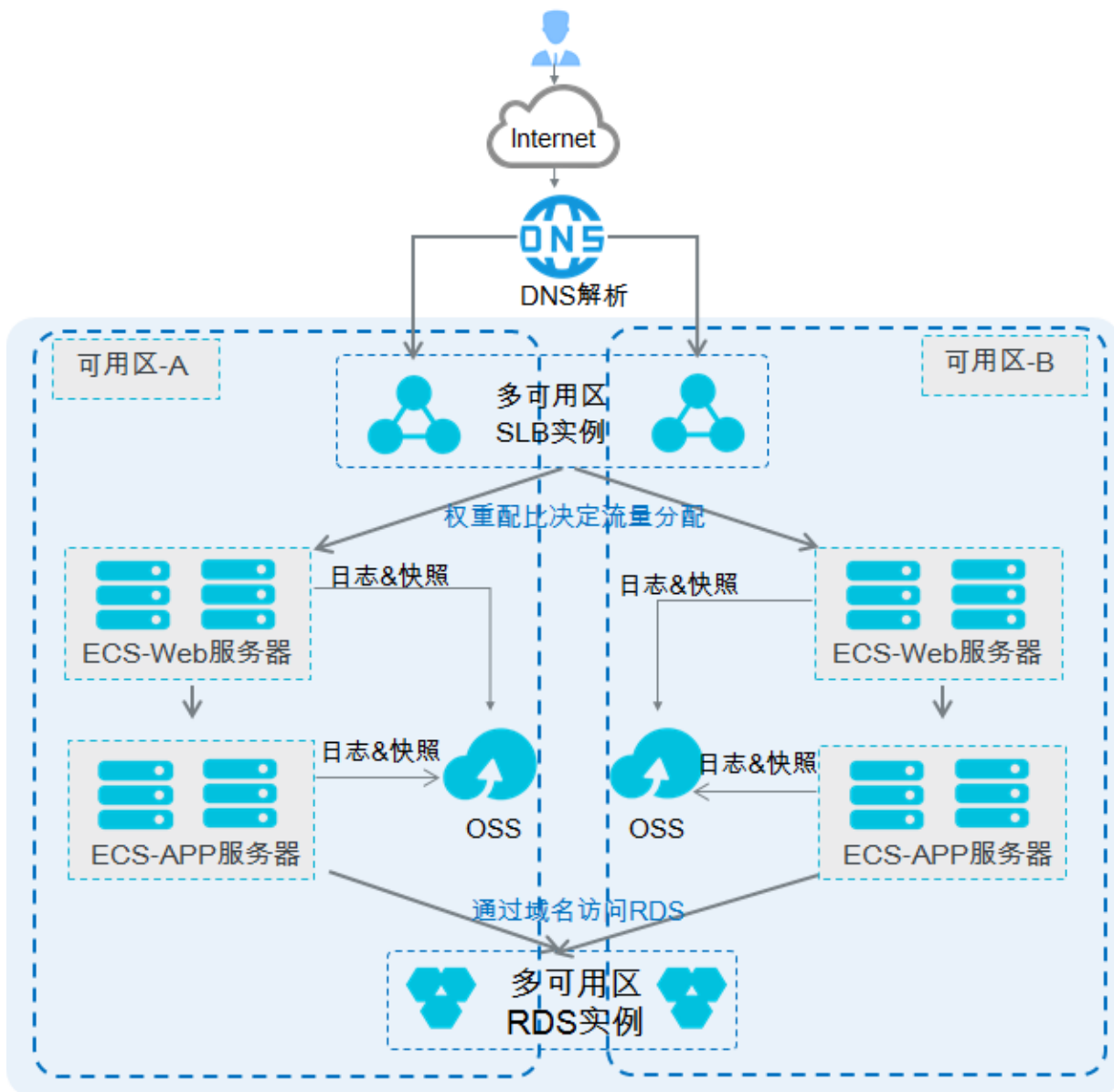
### 架构说明：

- 在同一地域下选择购买云产品。建议在VPC网络环境下，选择同一可用区或者同地域不同可用区的云产品。
- 在前端购买SLB，提供负载均衡功能，当后端ECS资源使用紧张时可以直接横向扩展，对业务无影响。
- 建议ECS服务器至少两台，避免单点故障。

- 数据库业务尽量不要和应用服务部署在同一台ECS上，防止不同服务之间资源抢占，同时方便日常管理和后期扩容。数据库服务器推荐直接购买RDS产品，数据安全有保障，同时也不需要花太多精力去运维管理。

#### 公共云同城容灾 推荐架构

对中大型用户来说，希望业务系统要求具备同城容灾的能力，可以采用以下同城容灾方案：



#### 架构说明：

- 在同城不同可用区之间对原有应用架构做一套完整的备份，SLB、ECS、RDS等均在两个机房同时部署。
- 前端部署DNS解析，如果某个可用区出现像IDC机房断电或者火灾等机房级故障时，可以通过前端切换DNS来及时恢复业务。

- 非机房级故障（某个机房的单产品故障，如其中一个机房的ECS服务器损坏），故障切换保障由单产品的灾备设计保障。

#### 公共云同城容灾 架构优势

- 可用区之间高速、低延时互联，快速复制数据。
- 可用区之间配置网络一体化环境，方便发布、部署、配置变更等工作。
- 负载均衡（SLB）支持多可用区实例，产品化实现容灾及切换。
- SLB可直接同时挂载多个可用区的ECS，实现负载均衡及容灾切换。
- 数据库支持多可用区实例，产品化实现灾备切换。

### 3 公共云异地容灾解决方案

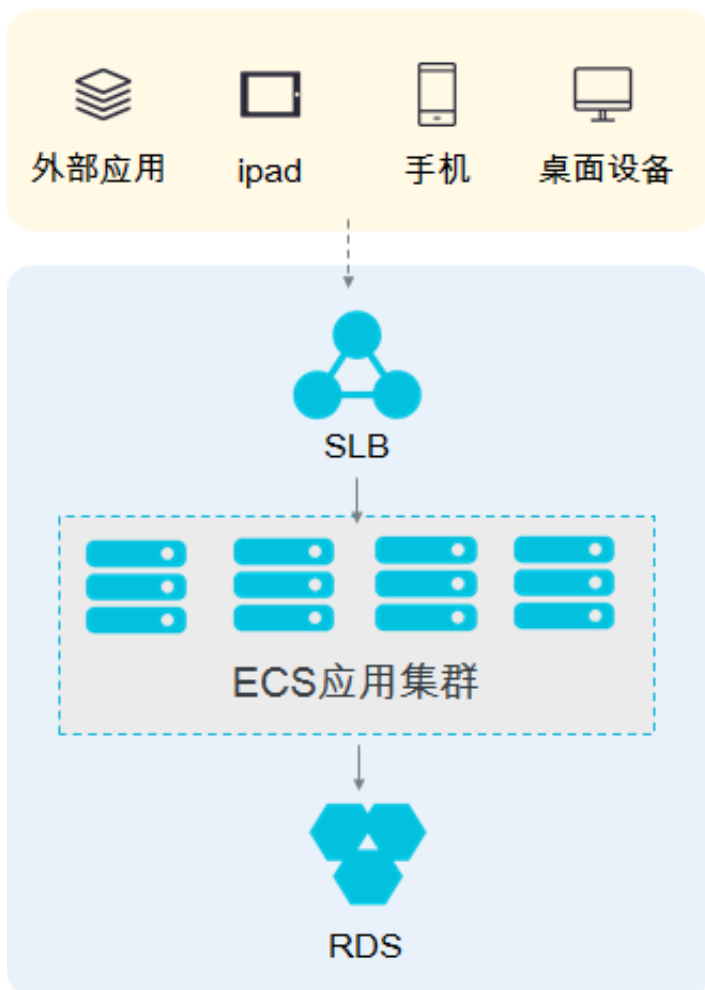
当企业的业务原先即已部署在阿里云上且对异地容灾有较强需求时，可采用阿里云的公共云异地容灾解决方案，使用阿里云DNS、SLB等产品搭建多地域的系统架构，实现异地容灾。

#### 公共云异地容灾适用场景

公共云异地容灾解决方案适用的灾备场景为：

- 公共云形态：企业业务已部署在阿里云上，希望在阿里云的不同地域搭建异地容灾架构。
- 应用级：企业希望对整体的应用做容灾备份，而非单独的数据库或存储。
- 云上异地容灾：可应对公共云上某地域故障场景，例如：
  - 自然灾害导致整个地域不可用，例如地震。
  - 基础设置故障导致的整个地域长时间不可用。

使用以下阿里云SLB、ECS、RDS、OSS即可搭建一个最简IT系统，如下图所示。

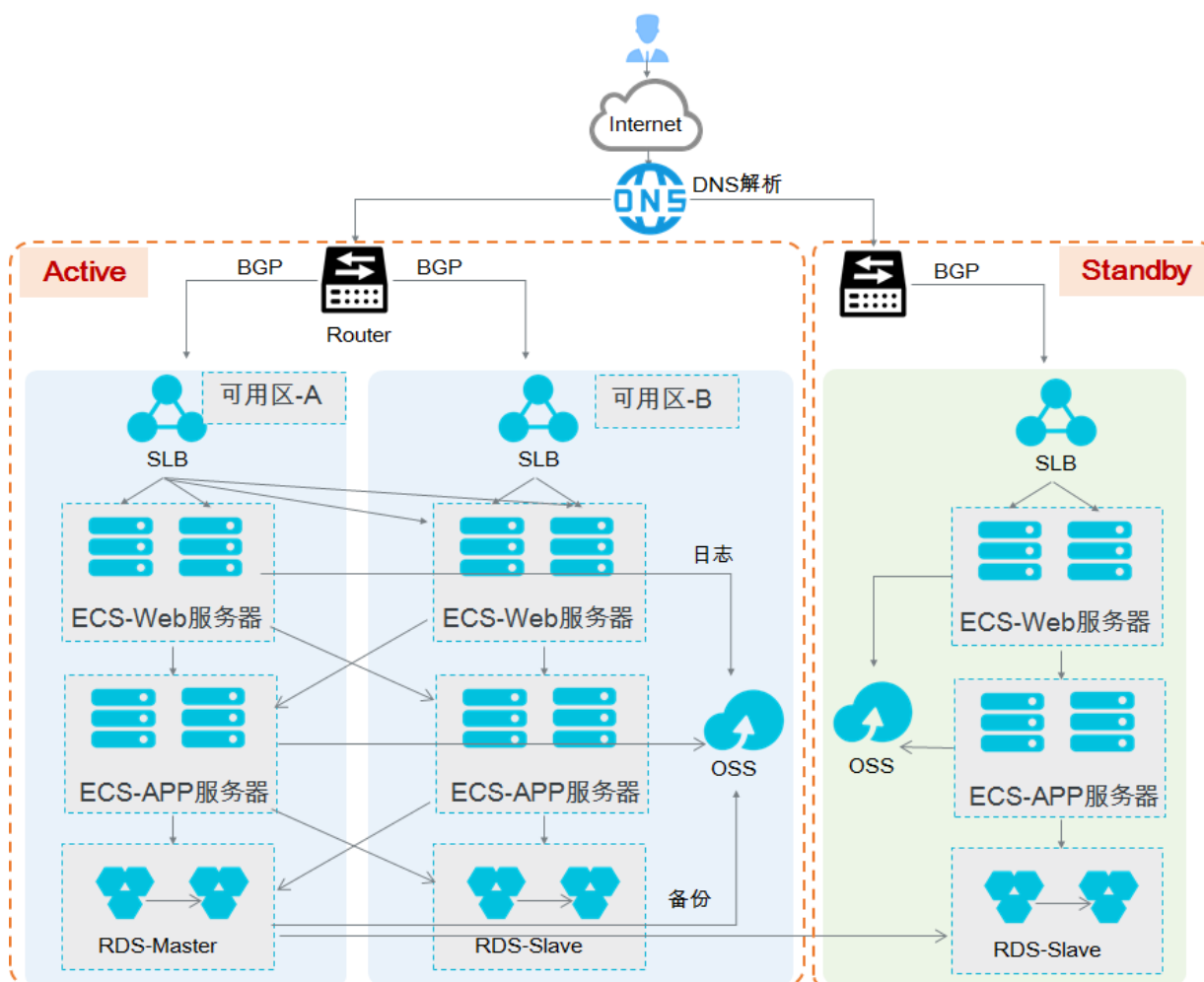


- SLB: Server Load Balancer, 是对多台云服务器进行流量分发的负载均衡服务, 在整个IT系统中, SLB是服务的对外接口, 流量入口。阿里云SLB可通过多可用区来消除单点故障, 保障系统的稳定性。详细的灾备设计及技术指标见 [SLB](#) 章节。
- ECS: Elastic Compute Service, 是一种简单高效、处理能力可弹性伸缩的计算服务, 在整个IT系统中提供计算能力。ECS可使用镜像、快照进行备份, 详细的设计及技术指标见 [ECS](#) 章节。
- OSS: Object Storage Service, 是阿里云提供的海量、安全、低成本、高可靠的云存储服务。在整个IT系统中提供非结构化、半结构化的存储能力, 详细的灾备设计及技术指标见 [OSS](#) 章节。
- RDS: Relational Database Service, 是一种稳定可靠、可弹性伸缩的在线数据库服务。在整个IT系统中提供关系型数据库能力, 详细的设计及技术指标见 [RDS](#) 章节。

企业的复杂IT系统亦可根据业务拆分为不同子系统, 每个子系统参考上述最简IT系统单独购置搭建, 最终组成一个完成企业较为复杂的IT系统。因此, 以下以最简IT系统为例, 示例公共云上的容灾解决方案推荐架构。

#### 公共云异地容灾推荐架构

对于一些大型企业在业务安全性、服务可用性和数据可靠性方面既要求具备同城容灾又要求具备异地容灾时, 可以采用以下异地容灾方案:



#### 架构说明：

- 在不同地域、不同可用区中均对原有应用架构做一套完整的备份。
- 不同地域之间可以采用阿里云的高速通道进行私网通信，保障数据库之间的数据实时同步，将数据传输延迟降到最低。
- 故障发生时可以通过前端DNS实现秒级切换，及时恢复业务。
- 这种容灾架构方式既可以解决单机房故障也可以应对像地震等灾难性故障。

#### 公共云异地容灾架构优势

- 云DNS提供智能解析、方便流量分配或容灾切换。
- 提供VPC之间的高速通道，提供统一发布、部署、配置变更功能。
- 产品化提供OSS不同区域之间的数据复制。
- 通过数据传输服务（DTS）提供不同区域之间的数据同步。

## 4 混合云容灾解决方案

阿里云混合云容灾解决方案使用核心产品混合云灾备一体机，推荐参考以下架构进行混合云容灾方案设计及环境搭建。

### 混合云容灾适用场景

混合云容灾解决方案适用的灾备场景为：

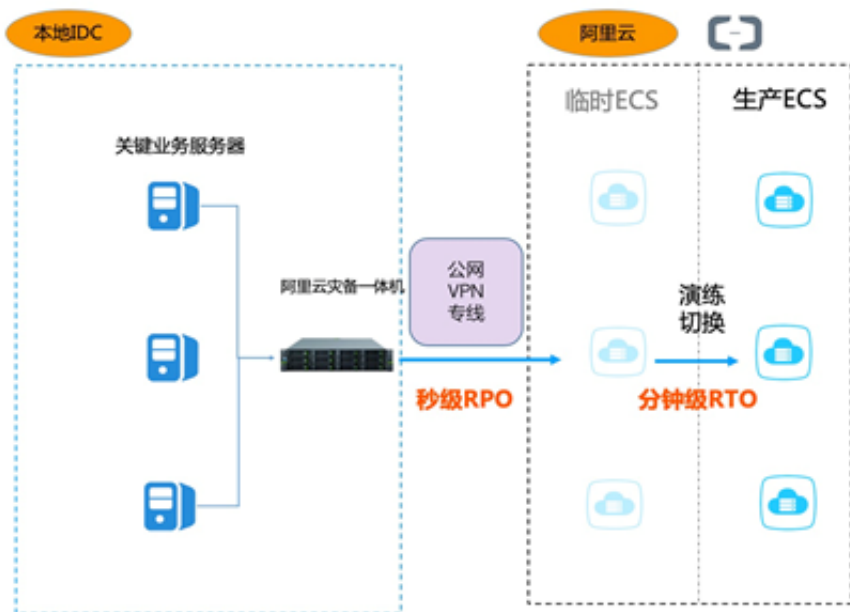
- 混合云形态：企业希望通过混合云的架构形态，将云上作为本地数据的异地容灾点。
- 应用级：企业希望对整体的应用做容灾备份，而非单独的数据库或存储。
- 高标准RTO/RPO：企业对应用灾备的要求达到秒级RPO，分钟级RTO。



说明：

RTO/RPO的具体概念可参考 [附录 灾备基本概念](#) 章节。

### 混合云关键业务型容灾推荐架构



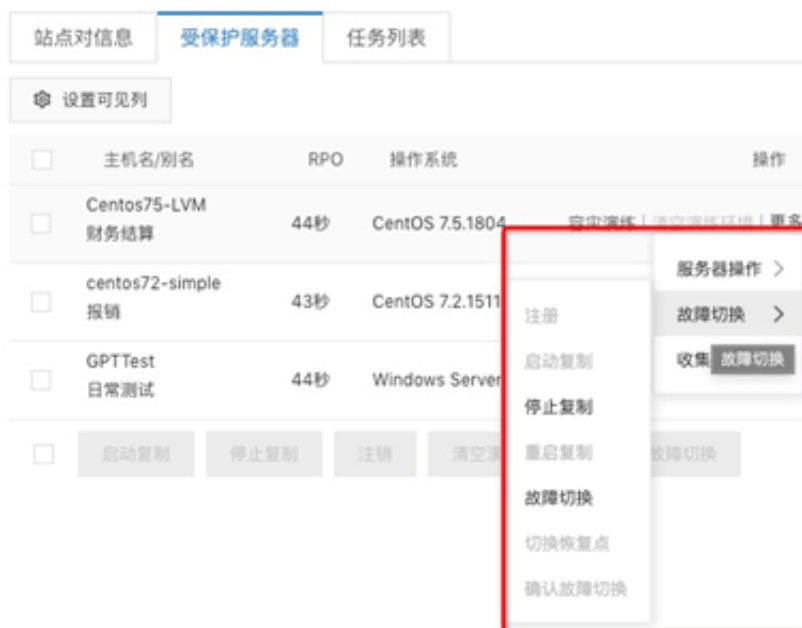
架构说明：

- 用户IDC与云上通过公网，专线或VPN方式构成混合云架构。
- 在本地IDC部署混合云灾备一体机。

BCDR可满足秒级RPO，分钟级RTO。

灾备一体机可将IDC的物理机、虚拟机的数据实时复制到阿里云，极高性能的云容灾。同时也可以将容灾切换到云上的业务回切到本地。

- 混合云灾备服务云上控制台上可监控备份任务状态、云上资源消耗状况等信息，RPO实施数值。
- 用户可以在云上控制台上对服务器进行一键容灾切换。



其中核心产品灾备一体机可根据您的灾备需求，选择不同一体机型号：

| 灾备一体机型号                                                                                                | 适用灾备场景                                                                                                                                                              |
|--------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 混合云灾备一体机 DR 100<br> | <ul style="list-style-type: none"> <li>· 1U机型，应对小企业，ROBO（Remote Office / Branch Office），中小负载等灾备场景</li> <li>· 单台最大支持20个节点，最大提供10 TB缓存容量双电，掉电保护RAID卡，高性能硬盘</li> </ul> |
| 混合云灾备一体机 DR 200<br> | <ul style="list-style-type: none"> <li>· 2U机型，应对较大规模环境</li> <li>· 单台最大支持100个节点，提供最大50 TB缓存</li> <li>· 双电，掉电保护RAID卡，高性能硬盘</li> </ul>                                 |

其中核心产品BCDR网关的核心灾备能力为：

- 应用数据实时复制上云：混合云容灾服务—关键业务型能够实时监测企业应用系统的磁盘 IO，实时抓取数据变化并发送上云，实现数据的实施保护，RPO 达到秒级。
- 应用在云上快速恢复：复制上云的应用可以在阿里云上以 ECS 的形式快速拉起，所需时间在分钟级别。

- 无业务中断的容灾演练：您可以随时对复制上云的应用服务器进行容灾演练，以便验证业务的可恢复性。在验证过程中，源端生产环境不受影响，数据复制不会中断。

#### 混合云容灾架构优势

- 容灾性能优异：  
秒级RPO，分钟级RTO。
- 支持平台丰富：  
支持物理机、虚拟机，覆盖主流的Windows/Linux系统。
- 备份容灾一体集成：  
云上可恢复至一个月内多时间点，兼具容灾与备份能力。
- 安全稳定：  
端到端数据加密，云上容灾环境提供12个9的数据稳定性。
- WAN深度优化：  
仅传输增量数据，且所有数据经过压缩，公网，VPN，专线皆可完成容灾。

## 5 混合云备份解决方案

当企业希望将应用通过混合云的方式将数据、应用备份在阿里云上时，建议使用混合云备份解决方案，使用核心产品阿里云混合云备份服务，参考以下架构搭建环境。

备份为容灾的基础，因此使用混合云灾备一体机，参考[混合云容灾解决方案](#)的方案架构亦可达到仅备份的需求。此外，阿里云提供混合云备份服务，更加经济的满足企业仅备份至云上的需求。使用混合云备份服务时，建议参考以下架构搭建灾备环境。

### 混合云备份适用场景

混合云备份解决方案适用的灾备场景为：

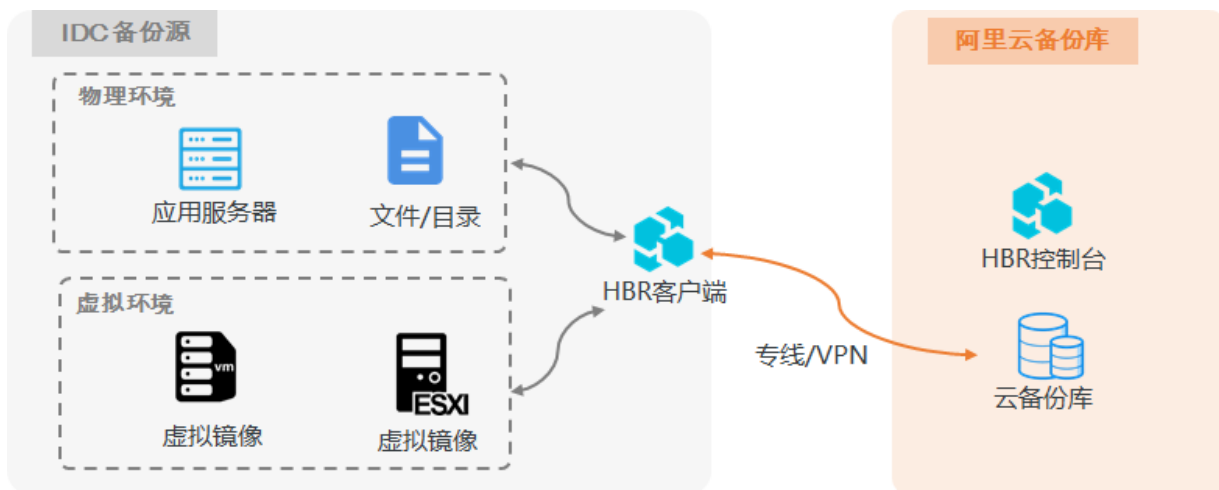
- 混合云形态：企业希望通过混合云的架构形态，将云上作为本地数据的异地备份点。
- 应用级：企业希望对整体的应用做备份，而非单独的数据库或存储。
- 小时级RTO/RPO：企业对应用灾备的RTO/RPO需求为小时级。



说明：

RTO/RPO的具体概念可参考 [附录 灾备基本概念](#) 章节。

### 混合云备份推荐架构



架构说明：

- 本地IDC与阿里云通过物理专线或VPN联通，构成混合云架构。
- 在本地待备份的物理机或虚拟机中安装混合云备份服务客户端（HBR客户端），在客户端中创建云上备份库的地域，通过专线或VPN将本地IDC的待备份数据备份至阿里云上。
- 如果本地IDC故障，可从云备份库中将已备份的数据按需恢复至本地。

其中，混合云备份服务支持备份的数据类型为：

## 混合云备份方案优势

- 重删压缩

HBR采用阿里云自研的重删（重复数据删除）、压缩技术，可有效减少I/O传输量和云备份存储量，从而提高备份速度，节省成本。

- 安全

备份在HBR中的数据采用三副本保存，有效保障数据备份安全。另外，阿里云提供端到端的数据加密校验机制，还可以通过RAM系统为操作人员划分等级权限，减少备份访问路径。

- 无限扩展

HBR备份仓库可以无限拓展，保存海量数据。

- 全面覆盖

HBR支持物理环境以及虚拟环境下的目录、文件的备份和VMware虚拟机的备份。

- 全托管

相比于在自建的数据中心搭建备份系统，或自行搭建云上备份系统，您只需将备份数据托管到HBR的云上备份仓库，无需担心硬件预置、配置、集群扩展、安全等问题。

## 6 混合云 数据库灾备解决方案

### 6.1 适用灾备场景

当企业对其数据库的灾备需求强烈时，可使用混合云数据库灾备解决方案。将企业的数据库通过混合云的架构，备份在云上，构成数据库的异地灾备，当本地数据库发生故障时，可将云上数据库的内容恢复至云下。

混合云数据库灾备解决方案适用的灾备场景为：

- 混合云形态：企业希望通过混合云的架构形态，将云上作为本地数据的异地灾备点。
- 数据级：企业希望对数据库做容灾备份。
- RTO/RPO：阿里云混合云数据库的冷备可达到秒级的RPO，热备可达双向实时同步。



说明：

RTO/RPO的具体概念可参考 [附录 灾备基本概念](#) 章节。

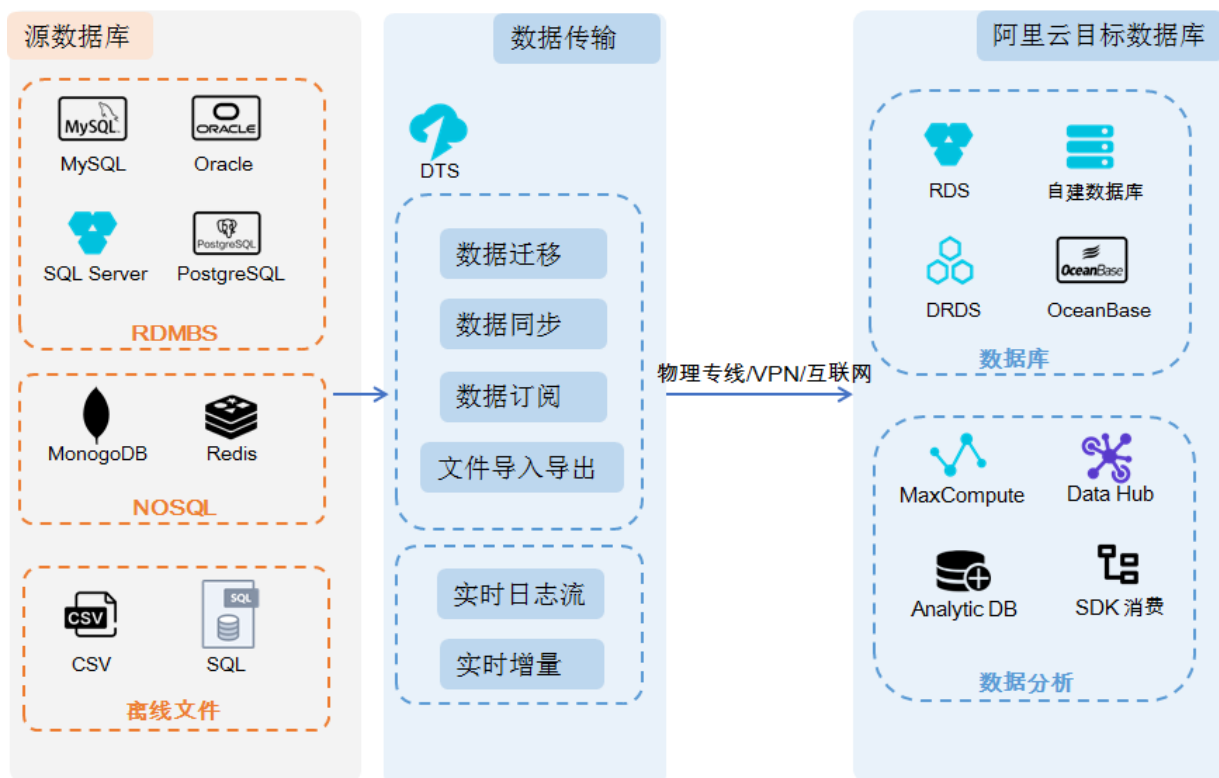
### 6.2 混合云数据库备份 解决方案架构

当企业希望将数据库通过混合云的方式备份在阿里云上时，建议使用混合云数据库备份解决方案，使用核心产品阿里云数据传输、数据备份服务，参考以下架构搭建环境。

通过数据传输（DTS）服务或数据备份（DBS）服务，可将云下的各类数据库同步至云上或恢复至云下。

| 数据库同步工具 | 灾备场景                               | 备份库 | RPO        |
|---------|------------------------------------|-----|------------|
| DTS     | 建议应用于 <a href="#">数据库热备推荐架构</a> 场景 | 数据库 | 云上云下双向实时同步 |
| DBS     | 建议应用于 <a href="#">数据库冷备推荐架构</a> 场景 | OSS | 秒级         |

## 数据库热备 推荐架构



## 架构说明:

- 用户IDC与云上通过专线或VPN方式构成混合云架构。
- 其中使用DTS:
  - 数据同步时:

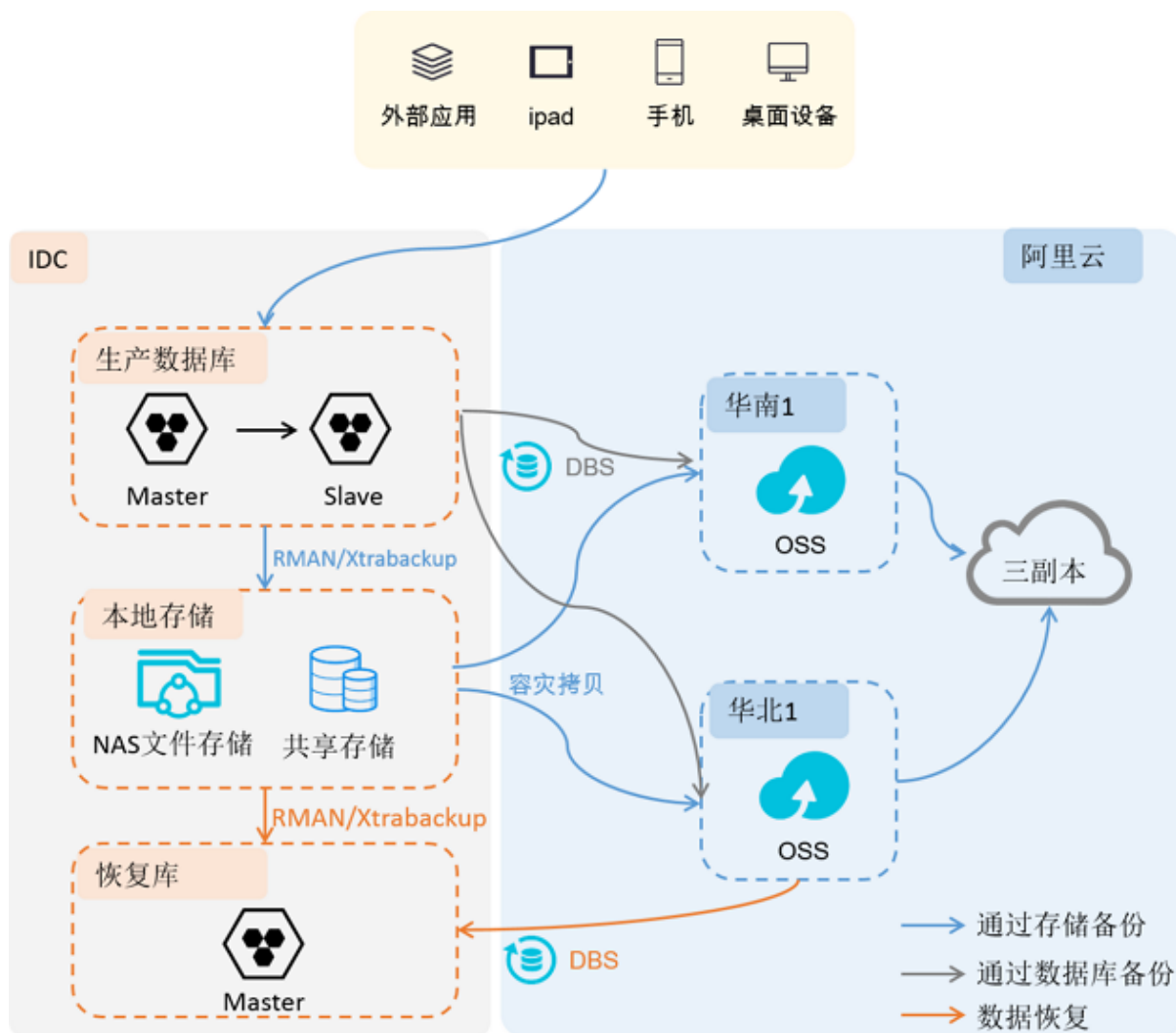
| 数据源                            | 说明                                                                             |
|--------------------------------|--------------------------------------------------------------------------------|
| RDS For MySQL-->RDS For MySQL  | 1000 km+ 情况下, 实现秒级同步延迟                                                         |
| RDS for MySQL<-->RDS for MySQL | 双向数据同步                                                                         |
| RDS for MySQL-->MaxCompute     | 数据同步到 MaxCompute 中, 每张表对应两张表: 全量基线表; 增量日志表。通过全量基线表+增量日志表的 merge, 可以获取任意时刻的全量数据 |
| RDS for MySQL-->Datahub        | 通过这个功能支持 MySQL->流计算 的数据实时同步                                                    |
| RDS for MySQL-->AnalyticDB     | 支持实时报表分析、实时可视化大屏等实时数仓系统                                                        |
| MySQL-->DRDS                   | 目前通过数据迁移—增量数据迁移实现                                                              |

| 数据源               | 说明       |
|-------------------|----------|
| MongoDB-->MongoDB | 高德异地容灾项目 |

- 数据迁移时:

| 数据源                               | 结构迁移 | 全量数据迁移 | 增量数据迁移           |
|-----------------------------------|------|--------|------------------|
| MySQL-->MySQL (RDS及自建)            | 支持   | 支持     | 支持 (DML, 部分 DDL) |
| MySQL-->DRDS /PetaData/ OceanBase | 支持   | 支持     | 支持 (DML)         |
| MySQL-->Oracle (数据回流, 需加白)        | 支持   | 支持     | 支持 (DML)         |
| Oracle-->MySQL (RDS及自建)           | 支持   | 支持     | 支持 (DML, 部分 DDL) |
| Oracle-->DRDS                     | 手工   | 支持     | 支持 (DML)         |
| Oracle-->RDS For PPAS             | 支持   | 支持     | 支持 (DML)         |
| Oracle-->ADS                      | 支持   | 支持     | 支持 (DML)         |
| Oracle-->Oceanbase                | 支持   | 支持     | 支持               |
| SQLServer-->SQLServer             | 支持   | 支持     | 支持 (DML)         |
| PostgreSQL-->PostgreSQL           | 支持   | 支持     | 支持 (有主键表的 DML)   |
| MongoDB-->MongoDB                 | 支持   | 支持     | 支持               |
| Redis-->Redis                     | 支持   | 支持     | 支持               |
| DB2-->MySQL                       | 支持   | 支持     | 支持 (DML, 部分 DDL) |

## 数据库冷备 推荐架构



## 架构说明：

- 关键部件部署：
  - 在用户本地部署有两套数据库：生产数据库和恢复库，分别用于生产数据的存储、故障后数据恢复。
  - 在阿里云的两个区域（例如：华南1、华北1）分别购置存储服务，例如OSS对象存储或者NAS文件存储。
  - 购置阿里云的DBS服务，用于用户本地数据库实时热备份至云上存储。
- 云下生产数据备份至云上：（可通过以下两种方案中的任意一种将云下生产数据备份至云上）
  - 用户可在本地再部署一套存储，将生产数据先备份至本地IDC的存储，再通过本地IDC存储容灾拷贝至云上存储。
  - 用户本地的生产数据库与云上存储之间通过阿里云DBS，将生产数据库中的数据直接热备份至云上两个区域的存储中。

- 数据恢复：
  - 如果用户本地IDC的生产数据库发生故障，但本地IDC的存储运行正常，可通过本地IDC的存储将数据恢复至本地IDC的恢复库。
  - 如果用户本地IDC的生产数据库和存储均发生故障，或没有部署本地存储，则可通过DBS将云上存储将数据恢复至本地恢复库。
- 架构特点：
  - 优点：技术要求高、一致性好，恢复时间短。
  - 缺点：因为是完全重新构造数据库实例，RTO不可控，随着数据库是来大小而变化。
  - 应用场景：比较成熟的备份手段，适用于大部分的关系型数据库。

### 架构优势

- 使用数据传输（DTS）服务：
  - 支持多种数据库间的数据实时同步，轻松解决异地灾备、异地多活等应用场景。
  - 双向同步：支持RDS For MySQL实例间的双向数据同步，助力用户构建异地多活架构。
  - 高级功能：同步链路搭建完成后，同步过程中，支持动态修改同步对象、动态修改同步速度等多种操作。
- 使用数据库备份（DBS）服务：
  - 可以为多种环境的数据提供强有力的保护，包括企业数据中心、其他云厂商、混合云及公共云。
  - 数据库备份提供数据备份和操作恢复的整体方案，具备实时增量备份、精确到秒级的数据恢复能力。

## 6.3 同城容灾 解决方案架构

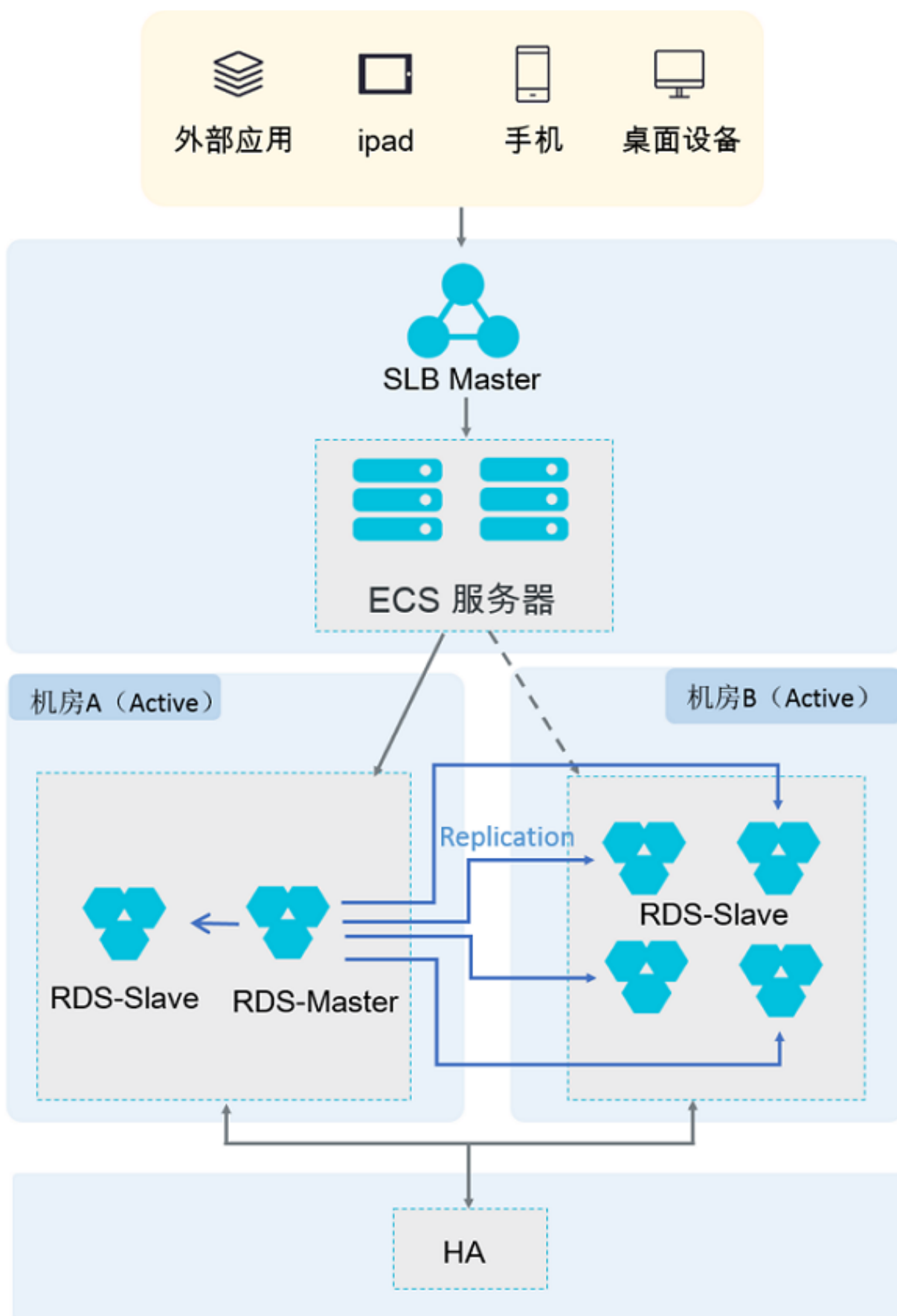
当用户需要实现同城机房级的数据库灾备方案时，可购置阿里云DTS服务，阿里云DTS可实现数据迁移、数据实时同步等功能。同城容灾时用户可选择复制加高可用、A-S（Active-Standby）模式或A-A（Active-Active）模式：

- 复制加高可用：同城两机房中均部署数据库，通过复制从主用机房的数据库将数据复制备份至备机房的数据库中。当主用机房的数据库发生故障时，业务切换至备用机房的数据库。
- A-S模式：同城两机房中部署完全一致的数据库，其中一个机房（Standby）的资源完全用于备份，不对外提供业务。当主用机房（Active）发生故障时，业务切换至备用机房。
- A-A模式：同城两机房中部署完全一致的数据库，两个机房均对外提供业务，但在两个机房中均预留一部分资源作为备份。当其中一个机房发生故障时，业务会切换到另一个机房，占用另一个机

房预留的资源。如果用户资源充足且对同城容灾要求较高时，建议采用A-S模式；如果用户资源紧张，建议采用A-A模式。

#### 同城容灾——复制加高可用

以用户使用阿里云数据库RDS为例，复制加高可用的架构如下：

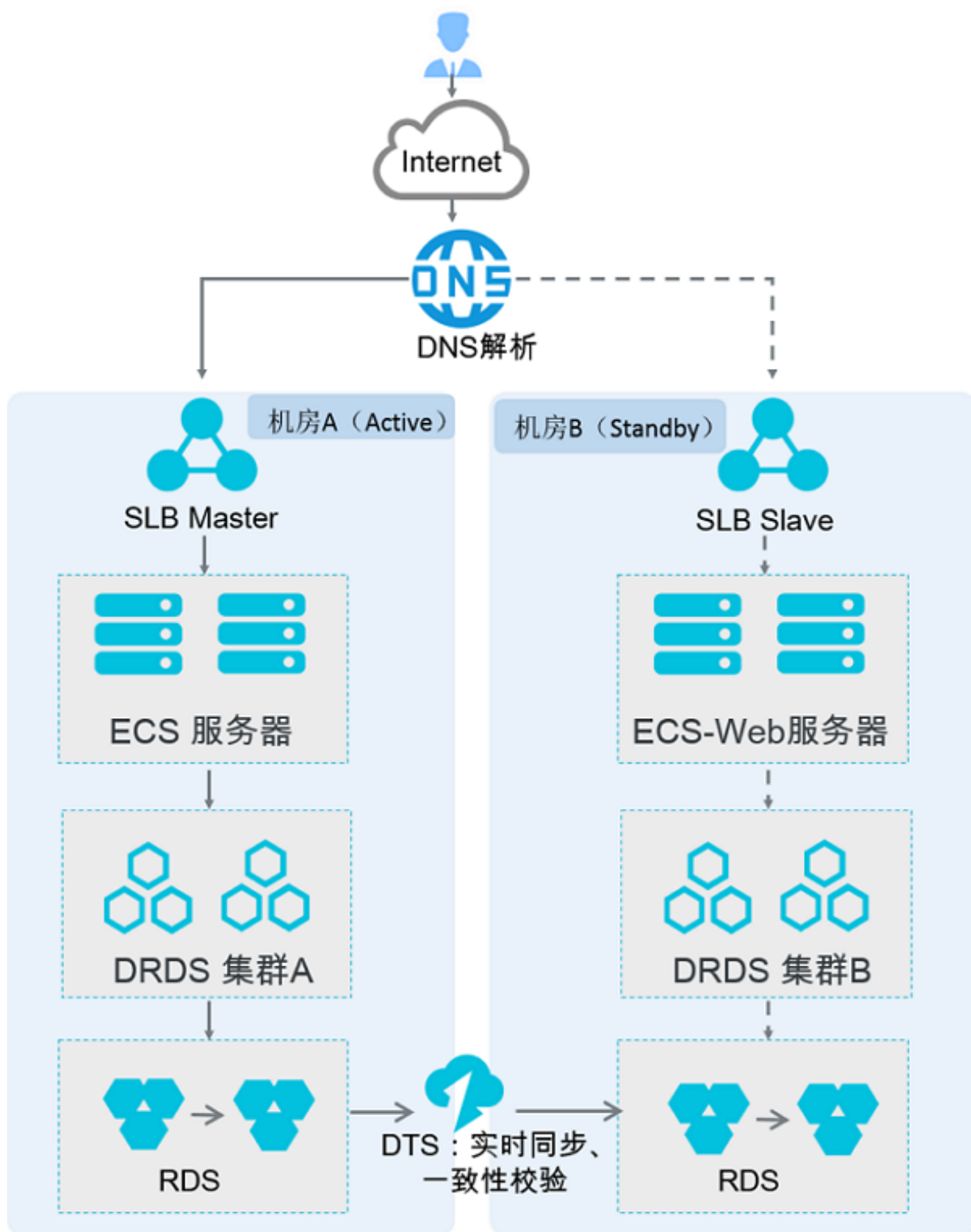


架构说明：

- 关键部件部署：
  - 在机房A和机房B机房分别部署RDS数据库集群。
  - SLB、ECS、HA均可跨机房对接应用，两个机房部署一套即可，通过HA管控两个机房的数据库。
- 数据备份与恢复：
  - 正常情况下，机房A的数据库通过复制的方式将数据备份至机房B的数据库。
  - 机房A数据库故障时，可通过HA将流量直接转移到机房B访问，暂时抛弃机房A的资源，等机房A恢复后重新配置为备选可用区。
- 架构特点：
  - 优点：轻量级切换成本低。
  - 缺点：可能存在少量数据不一致的风险，比如丢失一个事务。

#### 同城容灾——A-S

以用户在阿里云的一个Region购置了两套最简IT系统为例，数据库的A-S同城容灾解决方案架构示意如下：



#### 架构说明：

- 关键部件部署：

- 在机房A和机房B机房分别部署对等的DRDS+RDS数据库集群。
- 购置阿里云DTS服务，RDS之间通过DTS进行数据的实时同步和一致性校验，保证两个机房RDS数据的一致性。

- 数据备份与恢复：

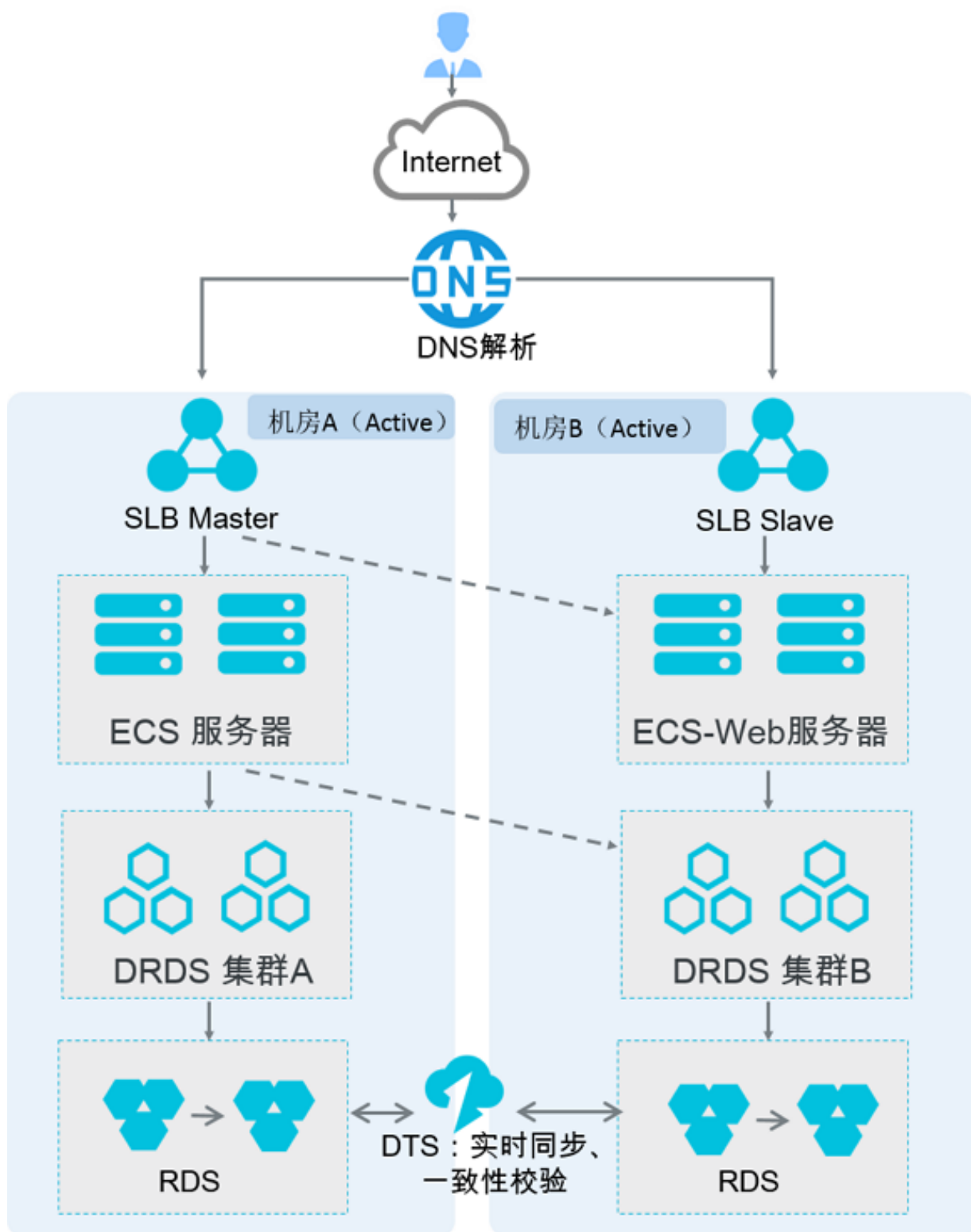
- 正常情况下，保证DTS实时同步的稳定运行，如果出现异常，需要处理保证DTS同步的稳定性和准确性。
- 如果机房A数据库故障或者机房整体故障，流量直接转移到机房B访问，暂时抛弃机房A的资源，等机房A恢复后重新配置为备选可用区。
- 如果只是应用端故障则将流量转移至机房B访问，同时需要对数据段做一致性校验，校验完成后，机房B成为主数据库，机房A作为备数据库，数据同步的流向发生变化，由机房B同步到机房A。
- 需要配置RDS-DTS-RDS之间的同步链路。

- 架构特点：

- 优点：性能最好，Zone A 故障时可以自动切换，人为干预程度低。
- 缺点：资源利用率50%。

## 同城容灾——A-A

以用户在阿里云的一个Region购置了两套最简IT系统为例，数据库的A-A同城容灾解决方案架构示例如下：

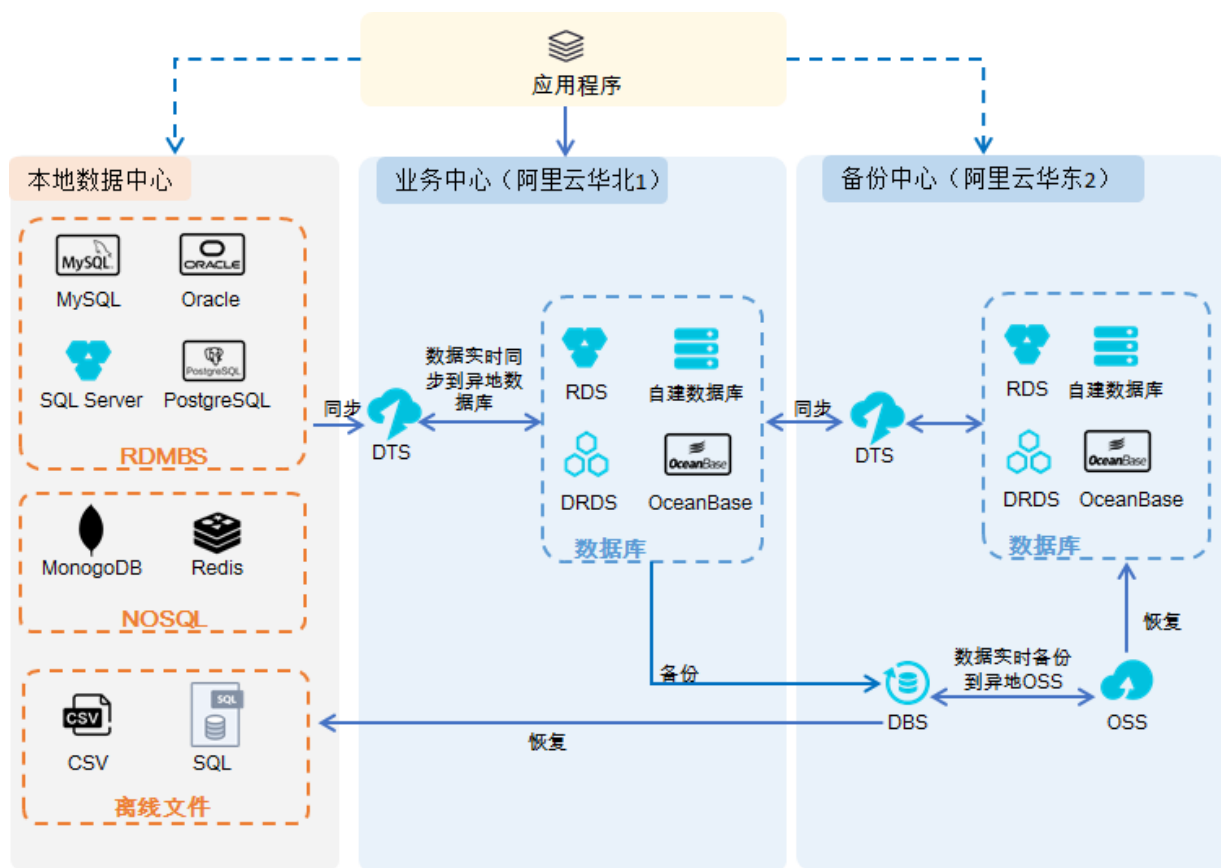


架构设计说明:

- 关键部件部署：
  - 在阿里云的同一个Region的两个可用区（机房A与机房B）部署两套最简IT系统。其中机房A与机房B均为Active状态。
  - 前端接入可部署DNS解析与SLB负载均衡，计算可使用阿里云ECS弹性计算服务。数据库可使用阿里云DRDS、RDS。
  - 数据库间使用阿里云DTS服务实现数据迁移、数据的实时增量同步。
- 同城灾备流程：
  - 在机房A正常运行状态下，用户生产数据从机房A的数据库，通过DTS实时同步至机房B的数据库，且通过DTS来校验两个机房数据库中数据的一致性。
  - 当机房A发生故障，整个机房无法工作时，前端DNS将流量解析至机房B，用户生产数据存储至机房B的数据库中。
- 架构特点：
  - 优点：资源利用率较方案一高。
  - 缺点：应用需要接受使用机房B应用服务带来的跨区访问延迟，机房A故障时切换需要人工修改机房B应用服务上应用配置的数据库连接地址为机房B的DRDS库地址。

## 6.4 两地三中心 解决方案架构

### 数据库两地三中心 推荐架构



#### 架构说明：

- 通过云下业务中心、云上业务中心、云上备份中心构建混合云形态的“两地三中心”灾备解决方案，云上云下的网络可通过专线或VPN联通。
- 三中心部署“无状态”应用程序，同时对数据库进行云上云下实时同步，并且对数据库进行备份。
- 当本地业务中心或云上业务中心故障时能够将业务流量转移至另一中心或者备份中心，故障恢复后业务流量可以切换回优选业务中心。

## 7 混合云多活解决方案

---

### 7.1 混合云多活解决方案适用灾备场景

企业业务快速发展之际，平衡业务、运维、成本、安全等多因素构建企业容灾系统架构是当前趋势，混合云多活解决方案架构基于本地数据中心及云端平台，提供混合云多活的灾备架构，满足企业的业务的连续性需求。

#### 为何选择混合云

混合云多活解决方案首先基于混合云的基本架构，可解决企业在构建灾备系统的同时，应对业务扩展、扩容运维、成本、安全等多维度的问题：

- 业务扩展：

对于企业业务而言，企业必须做到快速响应业务需求，同时企业业务需求是灵活多变的。公共云平台具有弹性伸缩能力，能应对频繁业务活动，例如双十一之类的对于流量突发增长活动，云平台可以采取峰值应对。融合传统IDC与云上平台的能力，混合云可解决企业业务扩展对系统架构的需求。

- 扩容运维：

传统的IDC完成一次具体的扩容，须从服务器的采购申请，到服务器的上架，再到安装操作系统、部署应用等等，完整的流程复杂且耗时长久，且在扩容过程中可能遇到一系列的问题，例如因为服务器环境差异导致系统故障等问题。使用混合云架构进行云上扩容，您无需关注底层云平台的运维，仅需要关注云上应用的运维，大大降低扩容门槛和运维技术难点。

- 成本控制：

混合云形态可利用云上资源减少传统灾备常见的资源闲置，同时可以降低整体的软硬件运维成本，且无需投入将系统完整迁移到公共云，节约迁移过程中对系统进行改造和迁移时间的成本。

- 安全控制：

从安全角度出发，采用混合云模式可将互联网接入和前台应用相关的计算、缓存节点全部迁移到阿里云上，充分利用阿里云成熟完善的安全防护解决方案，同时核心组数据依然可以保留在IDC中，保障核心数据的安全。

#### 灵活选择同城双活或者异地多活

混合云多活解决方案可以根据客户所在位置和灾备策略，选择公共云同城可用区或者异地可用区构建同城双活、异地双活或者异地多活。混合云异地多活（当只有一个异地云端节点时即为异地双活）是在多个地域同时对外提供服务，可以同时为分布在全国各地的用户提供就近接入服务也可以

提供异地容灾能力，当某地域的业务中断时可将业务流量切换至其他运行正常的地域中，继续对外提供服务。

相比传统本地灾备或双活架构，混合云多活解决了以下问题：

- 传关键时刻无法确定切换到灾备中心是否可以切换成功。
- 灾备中心不提供服务时，整个灾备资源会处于闲置状态，成本比较高。
- 平时提供服务的数据中心还停留在单地域，当业务体量大到一定程度时，这种模式无法解决单地域资源瓶颈的问题。
- 传统双活数据中心物理距离较近（通常50公里以内），无法应对自然灾害或大面积的电力、网络故障。

而采用混合云多活的架构，不仅可以解决传统异地容灾的需求，同时还可提高整体资源的利用率、应对业务增长时异地部署的需求。阿里云结合阿里巴巴集团多年双十一的异地多活架构实践，为您提供稳定、经济的混合云多活解决方案。

## 7.2 混合云多活解决方案架构

使用混合云多活方案时，建议参考以下架构搭建环境。

### 混合云多活架构要点

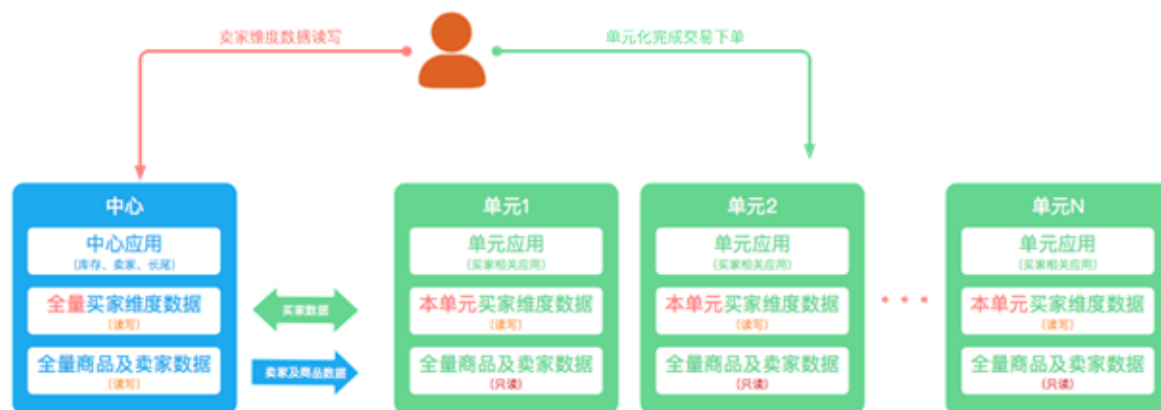
混合云多活其本质为异地多活，是通过异地的资源冗余，来保证在极端异常的情况下业务也能够正常运行。构建融合云上、运行的混合云架构时，需注意以下要点：

- 单元封闭：

应用要走向异地，首先要面对的便是物理距离带来的延时。如果某个应用请求需要在异地多个单元对同一行记录进行修改，为满足异地单元间数据库数据的一致性和完整性，我们需要付出高昂的时间成本。此外，如果某个应用请求需要多次访问异地单元，且各单元间服务再被服务调用，那物理延时将无法预估。因此，数据库异地多活的问题转移到了如何避免跨单元的问题，即要做到单元内数据读写封闭，不能出现不同单元对同一行数据进行修改，所以我们需要找到一个维度去划分单元，避免数据写冲突。

- 数据拆分：

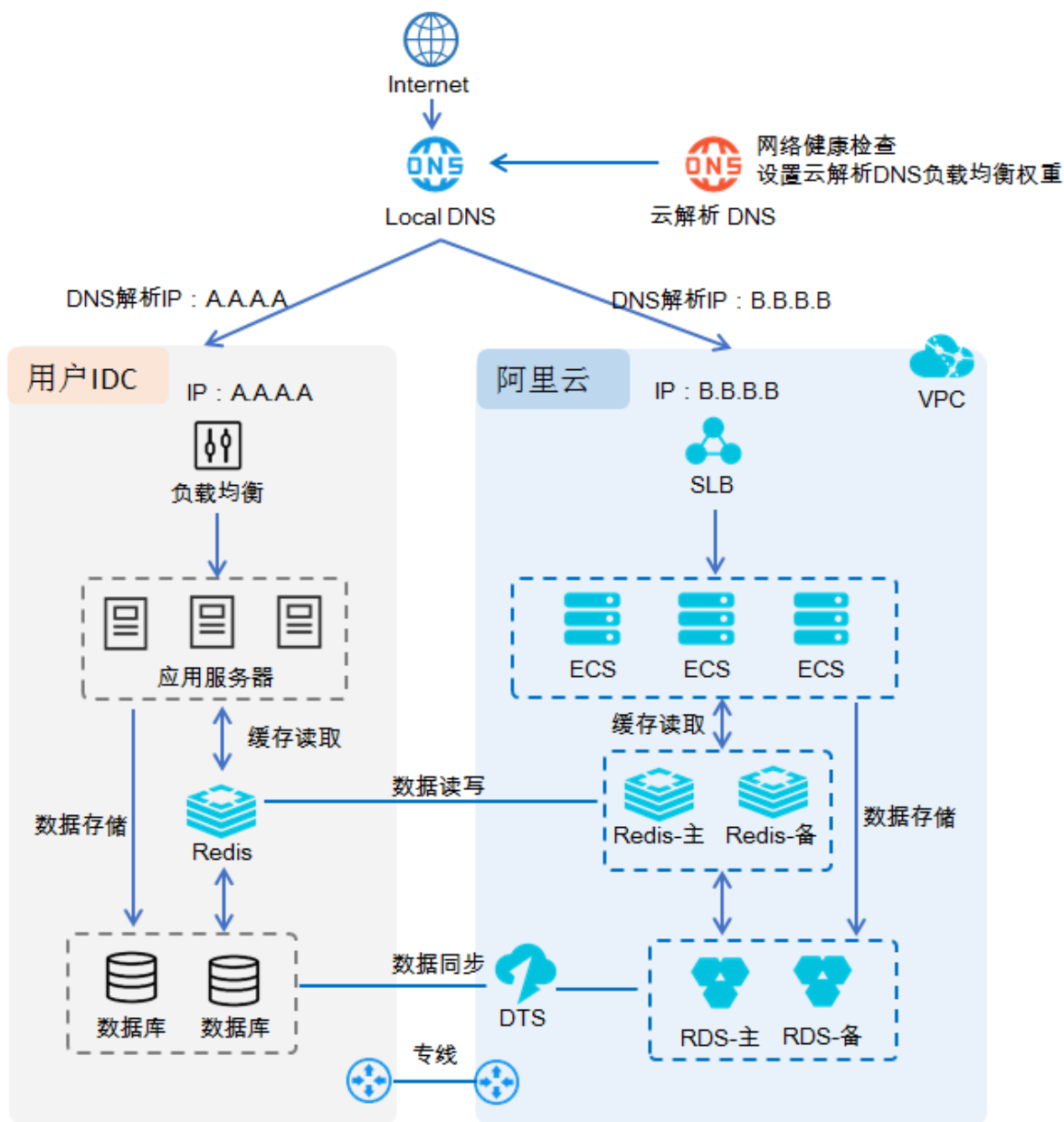
选择什么维度来解决单点写的问题，要从业务本身入手去分析。例如电商的业务，最重要的流程即下单交易流程，从下单业务对数据划分单元时，改造成本最低、用户体验相对好的便是买家维度，即通过买家ID进行下单业务拆分，如下图所示。



买家的下单操作在买家所在的本单元内即可完成读写封闭。按照上述示例划分业务，就意味着非买家维度的就需要做一定的妥协。对于非买家维度的操作，比如卖家操作（例如商品数据的修改）就可能会跨单元，对于买家与卖家数据读一致的问题，可以接受“最终一致”的就通过读写分离的方案，不能接受“最终一致”的则需要跨单元访问。

为了实现最佳业务体验，混合云多活架构的设计需结合业务场景和应用实现做进一步优化设计（可联系阿里云产品经理获取架构设计咨询建议），以下以最简IT系统为例，示意混合云双活架构如何搭建（扩展2个以上阿里云可用区即为混合云多活）。

## 混合云多活推荐架构



## 架构说明：

- 建议开通高速通道，通过专线搭建混合云的形态，应用系统同时部署在用户本地IDC和云端，构成本地业务中心+云上业务中心的混合云双活解决方案。

- 本地业务中心与云上业务中心负载分担，同时提供业务服务：

- 接入侧：

使用智能DNS分发流量至混合云的双数据中心，将应用做成无状态模式，在两个应用中心做对等的部署，突破运营商地域限制，按照地域切分流量。

- 应用部署：

应用系统同时、对等地部署在用户本地IDC和云端两个中心。每个中心的应用集群同时挂在对应数据中心的负载均衡下，由对应数据中心的负载均衡将流量分发至应用集群中的某个节点中。

- 缓存侧：

推荐通过Redis做应用的缓存读取。阿里云Redis产品兼容开源 Redis 协议，当云上、云下均使用阿里云Redis时，云上云下的Redis间可双向读写同步，通过CRDT（Conflict-free Replicated Data Type）机制检测并解决数据冲突，保障数据最终一致性。当云下使用开源Redis，阿里云可以接受来自云下IDC的单向读写同步信息。



说明：

如果云下IDC使用开源Redis，则可能出现无法接受阿里云Redis增强的缓存处理能力。阿里云Redis可能无法向云下Redis写数据，只能单向读取数据。建议您在本地IDC线下部署阿里云Redis。

- 数据侧：

应用数据分别存储在云上、云下的数据库中，通过DTS做云上、云下数据库间的数据同步，保障云上、云下数据库数据一致性。

### 混合云多活架构优势

- 多数据中心：阿里云在全球分布有多个数据中心，用户可在就近、合适区域选购、部署阿里云产品。
- 稳定：每个区域及产品比较稳定，阿里云关键部件（SLB、ECS、Redis、RDS等）经多轮迭代具备比较完善的灾备能力，可以实现更细粒度的控制，可以通过更多已经产品化的功能模块实现容灾。
- 弹性：用户可根据业务需求横向、纵向扩缩容，按需购买使用的服务。

## 8 操作示例 公共云跨可用区高可用解决方案

对于企业而言，无论业务是否上云，服务的稳定性和连续性一直都是至关重要的。为了降低不可抗力因素对服务的正常运行造成的影响，您需要努力提高产品的高可用性和容灾能力。虽然目前的产品已经有很高的可用性了，但是仍不能忽视构建服务高可用性和容灾的重要性。

为了提高服务的高可用性和容灾能力，通常会使用到如下几种云产品：云服务器ECS、负载均衡SLB、数据库RDS以及对象存储服务OSS。

### 可用区 (Zone)

**可用区**是指在同一地域内，电力和网络互相独立的物理区域。同一可用区内的 ECS 实例网络延时更小。

在同一地域内可用区与可用区之间内网互通，可用区之间能做到故障隔离。是否将云服务器 ECS 实例放在同一可用区内，主要取决于对容灾能力和网络延时的要求。

- 如果您的应用需要较高的容灾能力，建议您将 ECS 实例部署在同一地域的不同可用区内。
- 如果您的应用在实例之间需要较低的网络时延，则建议您将 ECS 实例创建在相同的可用区内。

您可以在地域列表中查看每个地域的可用区数量。您也可以在 OpenAPI Explorer 上通过 API 接口地域列表查看完整的可用区列表。

### 产品介绍

#### ECS

云服务器Elastic Compute Service (ECS) 是阿里云提供的一种基础云计算服务。ECS实例作为一个虚拟的计算环境，包含了CPU、内存、操作系统、磁盘、带宽等最基础的服务器组件，是ECS提供给每个用户的操作实体。

您无需提前采购硬件设备，而是根据业务需要，随时创建所需数量的云服务器实例。使用过程中，随着业务的扩展，您可以对云服务器进行扩容磁盘、增加带宽。如果不需要了，您还可以释放资源，节省费用。

云服务器ECS实例本身没有高可用性和容灾功能，需要通过架构搭建来实现。

#### SLB

**负载均衡** (Server Load Balancer) 是将访问流量根据转发策略分发到后端多台云服务器 (ECS实例) 的流量分发控制服务。负载均衡扩展了应用的服务能力，增强了应用的可用性。

负载均衡通过设置虚拟服务地址，将添加的ECS实例虚拟成一个高性能、高可用的应用服务池，并根据转发规则，将来自客户端的请求分发给云服务器池中的ECS实例。

关于负载均衡在提高服务器高可用性和容灾中的作用，可以从以下 2 点来阐述：

- 负载均衡的服务提供是基于集群部署的。各集群有一定数量的节点，避免了单点故障，个别或者部分节点服务器宕机不会影响负载均衡服务的提供。

负载均衡系统中四层负载均衡（LVS）服务、七层负载均衡（Tengine）服务和控制系统等关键组件都采用集群化部署，以提高扩展性和可用性。

- 当前提供的负载均衡实例大多是多可用区实例，主备实例在同城不同的可用区机房。当主实例机房出现故障，能及时进行切换，来实现容灾和服务的高可用性。想了解多可用区在各个地域的分布情况，请点击[这里](#)。

## RDS

[阿里云关系型数据库](#)（Relational Database Service，简称 RDS）是一种稳定可靠、可弹性伸缩的在线数据库服务。基于阿里云分布式文件系统和高性能存储，RDS 支持 MySQL、SQL Server、PostgreSQL 和 PPAS（Postgre Plus Advanced Server，一种高度兼容 Oracle 的数据库）引擎，并且提供了容灾、备份、恢复、监控、迁移等方面的全套解决方案，彻底解决数据库运维的烦恼。

- 关于单机基础版RDS，请[点击这里](#)。
- 对于双机高可用版RDS，您可以在同一可用区有主备实例。在主实例出现故障时可以进行主备切换，具有高可用和容灾特性。
- 关于多可用区RDS，其主备实例在不同可用区。
- RDS之间还可以用DTS同步和迁移数据。

## OSS

[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。您可以通过调用API，在任何应用、任何时间、任何地点上传和下载数据，也可以通过Web控制台对数据进行简单的管理。OSS适合存放任意类型的文件，适合各种网站、开发企业及开发者使用。按实际容量付费真正使您专注于核心业务。

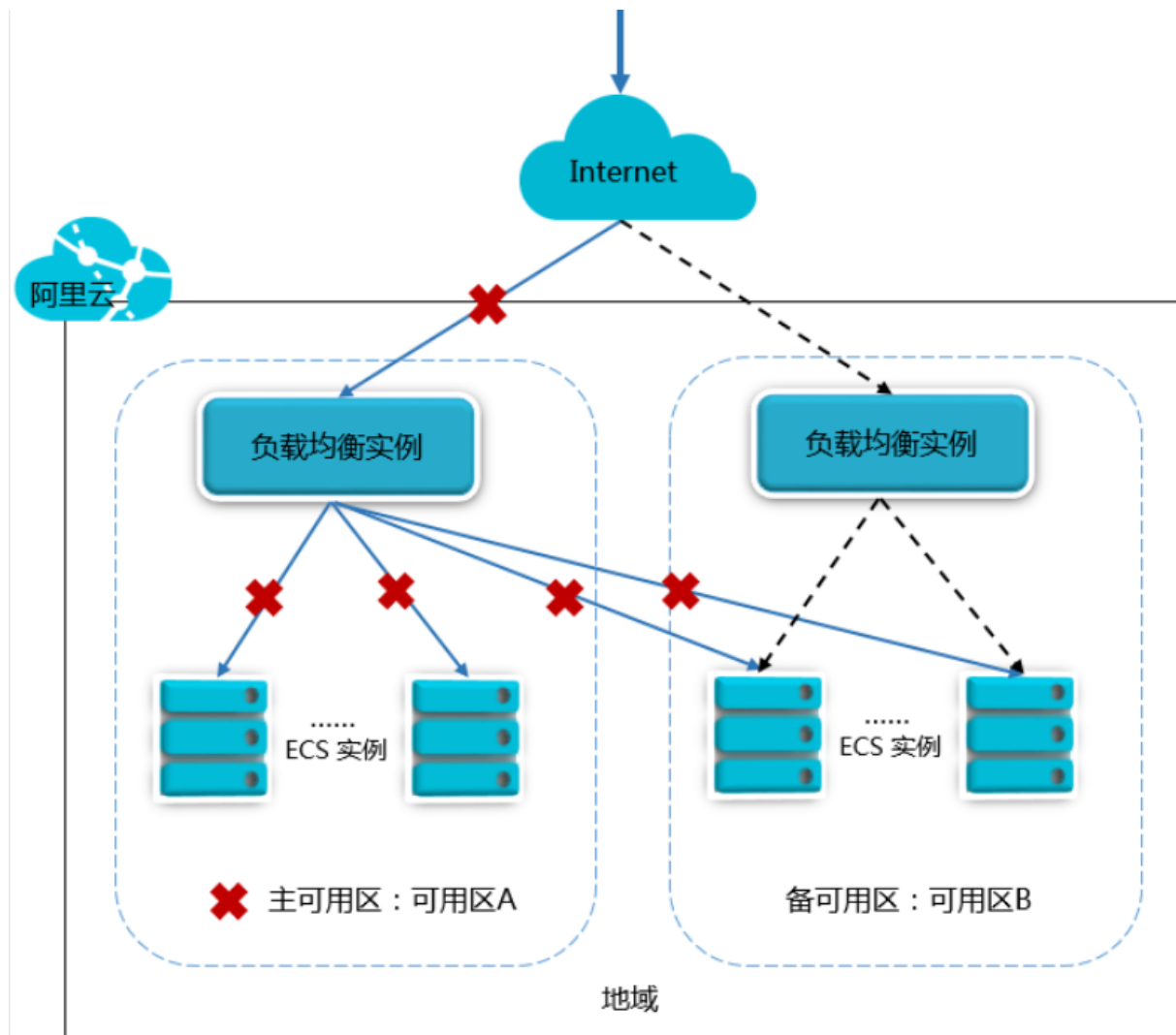
文件以Chunk分块方式存储，默认每块存三副本，并分布在不同机架的ChunkServer节点上。在盘古集群中Master允许宕机1台，Chunkserver允许同时宕机2台，KVServer与WS允许宕机多台。

针对服务高可用性以及容灾功能的具体架构和搭建过程，下面作详细介绍。

### 多可用区SLB + 不同可用区ECS

如下图所示，在负载均衡实例下绑定不同可用区的 ECS，当可用区A未出现故障时，用户访问流量如蓝色实线所示；当可用区A发生故障时，用户访问流量的分发将变成黑色虚线，这样即可以避免

因为单个可用区的故障而导致对外服务的不可用，也可以通过不同产品间可用区的选择来降低延迟。



关于上述架构的搭建流程，请参照如下步骤。

## 1. 登录阿里云控制台，选择负载均衡，单击右上角创建负载均衡。



以华北2为例，购买主可用区B、备可用区A的多可用区实例。



## 2. 在SLB主备可用区分别创建ECS实例。

分别在华北2可用区A和B创建测试实例，本例中采用默认安全组，专有网络（VPC），1核2G内存CentOS 7.2实例。



### 3. 创建监听并添加后端服务器。

- 在负载均衡控制台界面，找到创建的实例，单击管理。
- 单击后端服务器，选择未添加的服务器，找到对应实例并单击添加。



- 完成后，您可以在已添加界面看到对应ECS实例及其权重。
- 单击左侧监听栏，选择添加监听，根据需要选择监听属性。本例中采用TCP四层模式，监听80端口，后端转发80端口，使用默认加权轮询，并开启会话保持，使用默认1000s超时间。



- 设置健康检查为TCP模式，检查后端80端口。
- 完成上述操作后，您可以在监听页面看到添加的监听及其状态。

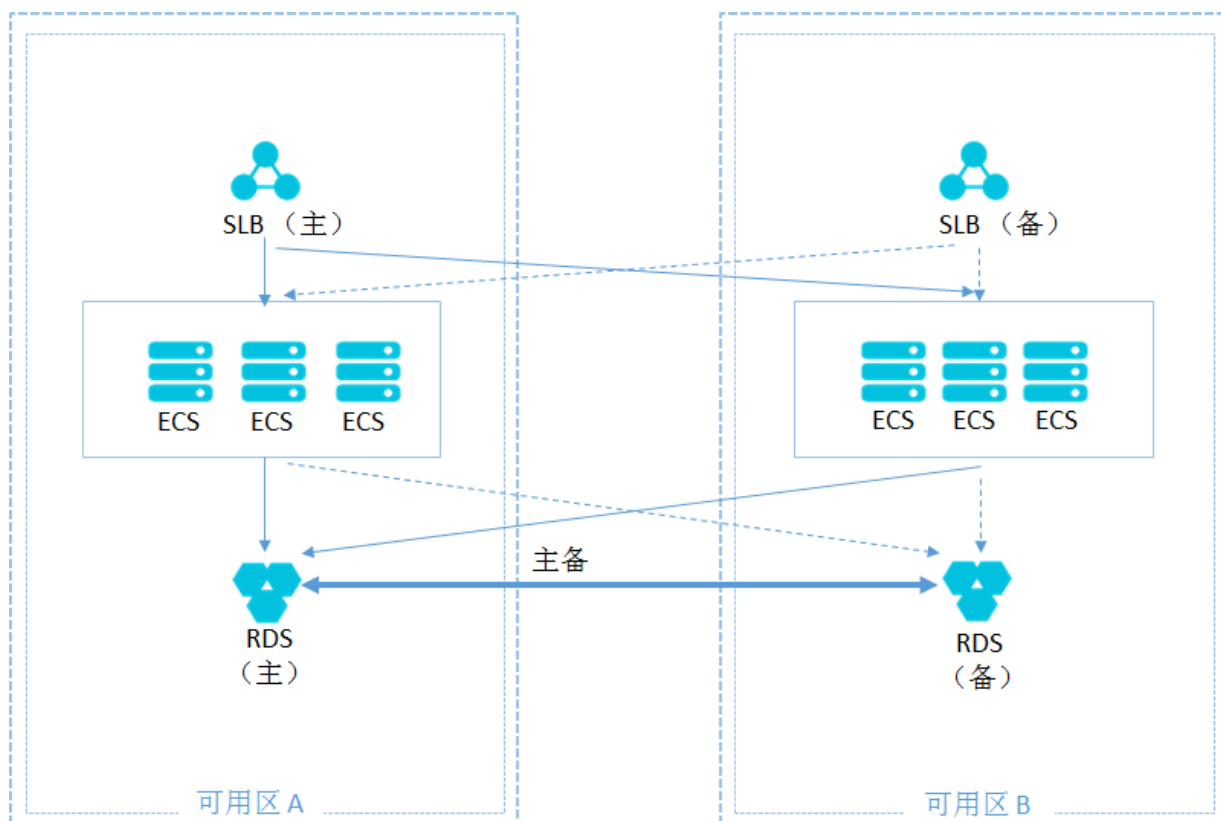


#### 说明:

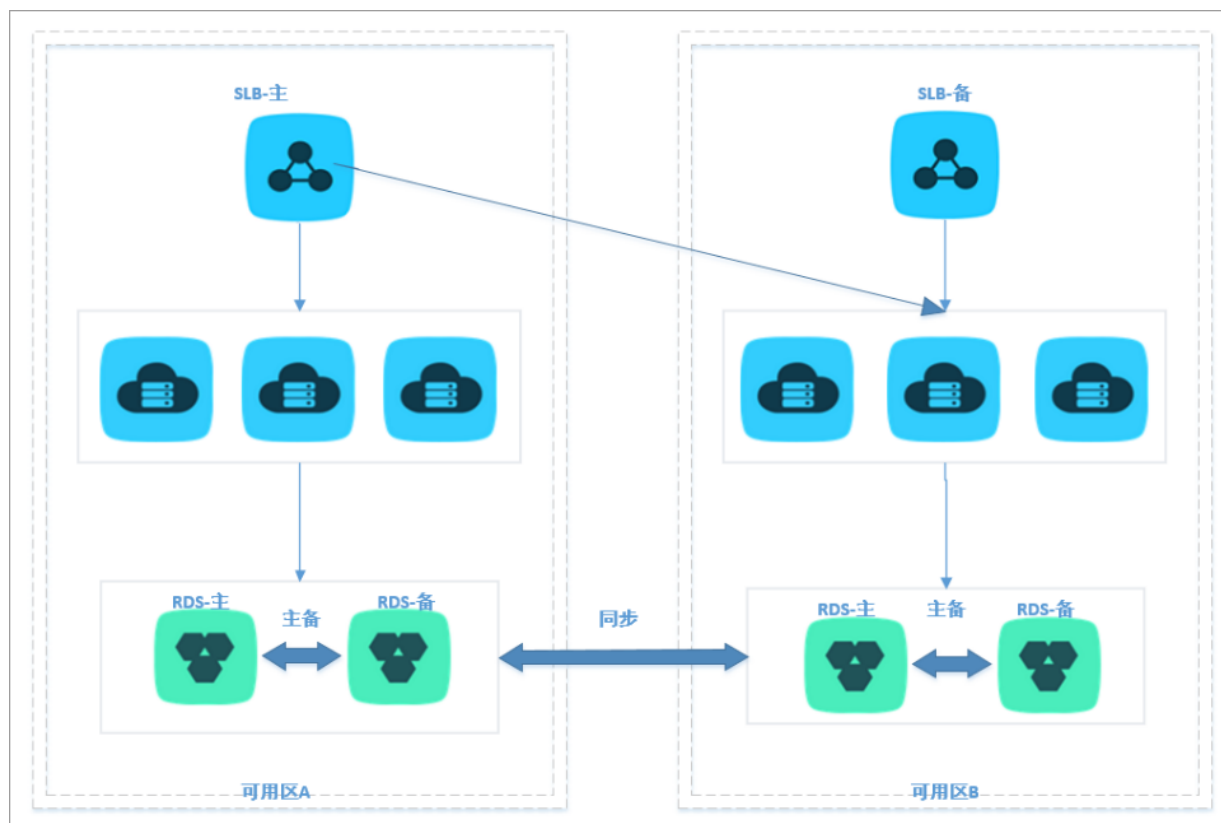
后续客户只需要在ECS上部署相关服务并监听80端口，并将域名解析到SLB公网IP，那么负载均衡即可将请求转发到后端ECS并提供服务。

多可用区SLB + 不同可用区ECS + 高可用RDS

关于多可用区的RDS架构，如下图所示：



对于没有多可用区RDS的地域，可以在对应可用区分别建立一台RDS，其中备用可用区作为备库，跟主可用区的RDS实例进行同步。



关于多可用区RDS的搭建流程，具体如下所示：

1. 在多可用区SLB和不同可用区ECS的基础上，购买RDS实例。



2. 选择其中具有多可用区RDS的地域。

3. 完成购买后，您可以在控制台进行查看。

同样在控制台中，您可以查看RDS高可用信息以及进行主备切换，如下图所示。



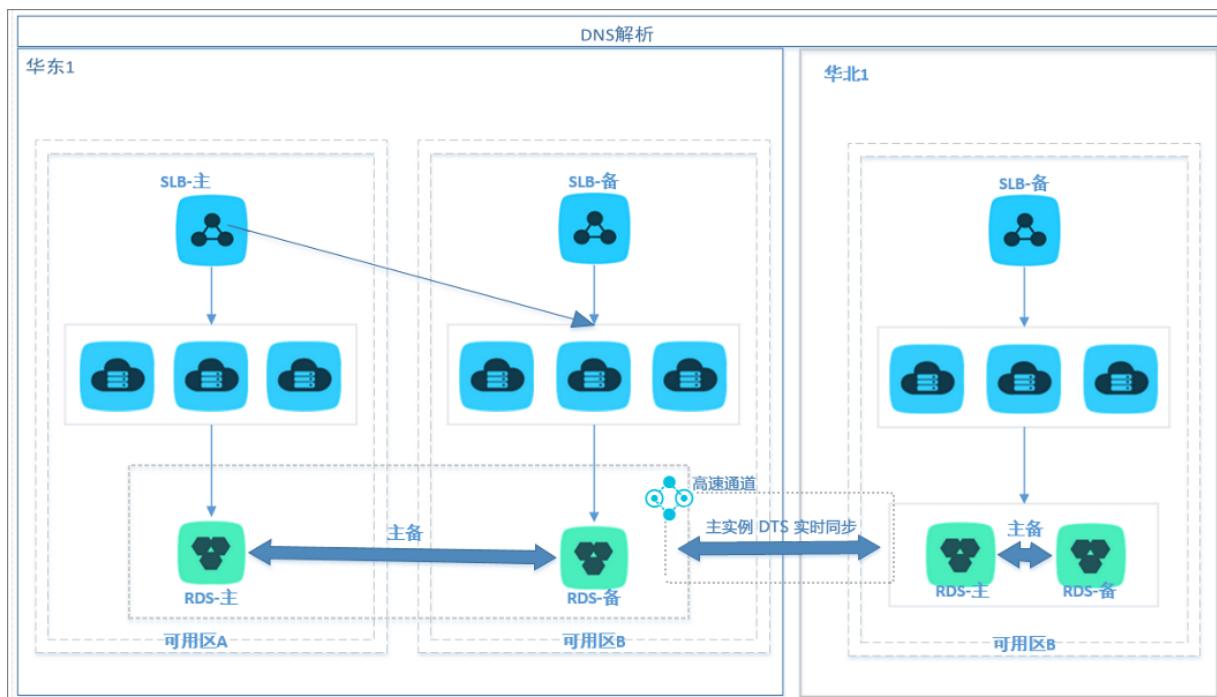
针对不同可用区分别搭建RDS的情况，具体示例如下所示。

1. 分别在可用区A和B购买双机高可用RDS。

2. 创建DTS同步。

高可用性-异地容灾

在同城多可用区的情况下，异地也同时部署一套环境，可以更大程度地提高服务的高可用性，并达到异地容灾的目的。



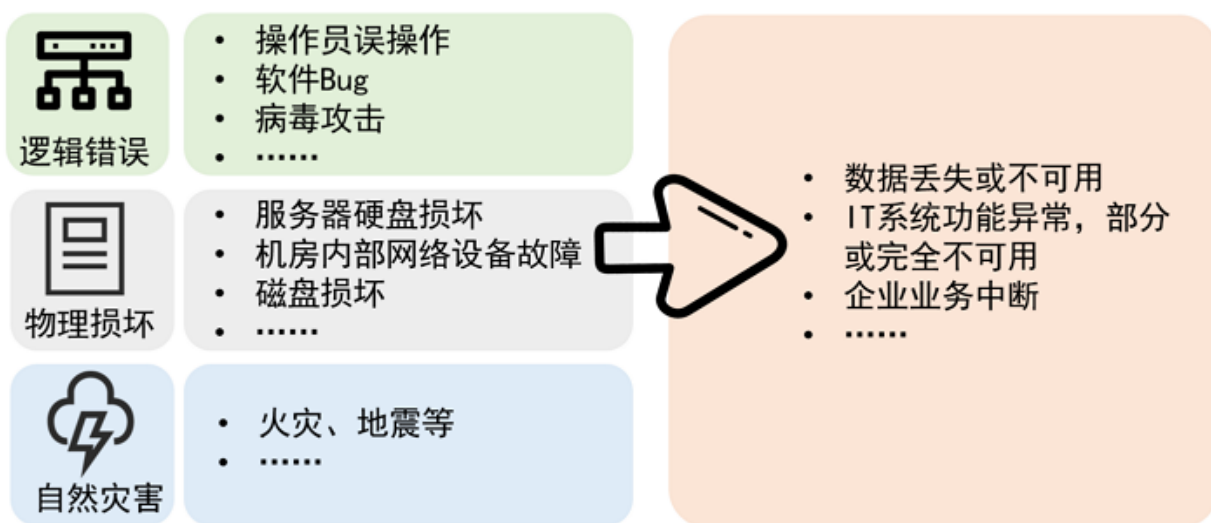
说明:

最终的服务访问区域可以通过配置DNS解析来实现，同时RDS用DTS同步来实现。

## 9 附录 灾备行业趋势及基本概念

### 9.1 行业趋势与挑战

对于各行各业而言，用户数据、系统数据均是企业最核心、最重要的财富，业务的稳定运行、IT系统功能正常是企业最重要的发展诉求。而这些诉求常常因为一些不可预期不可力抗“天灾人祸”变得十分困难，例如：



综上，保障企业业务稳定、IT系统功能正常、数据安全十分重要，可以同时保障数据备份与系统、应用容灾的灾备解决方案应势而生，且发展迅速。



说明：

灾备是指容灾+备份：

- 备份的定义：指用户为应用系统产生的重要数据（或者原有的重要数据信息）制作一份或者多份拷贝，以增强数据的安全。
- 容灾的定义：指在相隔较远的两地（同城或者异地）建立两套或多套功能相同的IT系统，互相之间可以进行健康状态监视和功能切换。当一处系统因意外（天灾、人祸）停止工作时，整个应用系统可以切换到另一处，使得该系统功能可以继续正常工作。

#### 传统灾备方案痛点

为应对灾备需求，各企业使用传统方案，自建灾备中心，然而，使用此种方案不仅物资消耗大，还面临着如下诸多挑战。

| 传统灾备方案          | 灾备特点                                                                                | 挑战                                                                                                                                                                    |
|-----------------|-------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 采用应用级别的复制软件     | 实现应用级容灾                                                                             | <ul style="list-style-type: none"> <li>· 建设维护异地灾备机房成本高昂</li> <li>· 软硬件部署、维护难度高</li> <li>· Failback需要大量操作与测试</li> </ul>                                                |
| 采用CDP技术         | <ul style="list-style-type: none"> <li>· 实现应用级容灾</li> <li>· RPO/RTO较好</li> </ul>    | <ul style="list-style-type: none"> <li>· 建设维护异地灾备机房成本高昂</li> <li>· 需要昂贵的CDP设备</li> <li>· 软硬件部署、维护难度很高</li> <li>· 不能复制应用缓存中的数据</li> <li>· Failback需要大量操作与测试</li> </ul> |
| 利用存储设备复制。实现应用容灾 | <ul style="list-style-type: none"> <li>· 能有效实现应用级容灾</li> <li>· 确保RPO/RTO</li> </ul> | <ul style="list-style-type: none"> <li>· 建设维护异地灾备机房成本高昂</li> <li>· 双活存储设备和配套网络设备昂贵</li> <li>· 软硬件部署、维护难度很高</li> <li>· 应用感知能力有限，需要较多人工脚本联动</li> </ul>                  |

然而，随着企业数据量暴增，数据价值成几何增长，企业对业务连续性的要求进一步增高，传统灾备方案投入巨大且建设周期长，维护成本高，已无法满足未来IT系统发展的需要。

#### 云灾备方案的优势

近年随着云计算的稳健迅速发展，基于云计算技术的云灾备方案应运而生。云灾备方案系统建设成本更低、系统恢复更快。传统灾备方案与云灾备方案的对比如下表所示。

| 方案细节 | 传统灾备                                                 | 云灾备                           |
|------|------------------------------------------------------|-------------------------------|
| 实现方式 | 大多基于物理设备实现，需要在多点部署相应的物力资源，根据不同系统可靠性的要求，备份的地点和规模差异很大。 | 基于混合云或公共云，将业务系统的灾备点之间部署在云端。   |
| 建设周期 | 以月为单位计算                                              | 以天为单位计算                       |
| 投资规模 | 需购买大量服务器、存储及网络物理设备，投入规模较大                            | 弹性扩展，初期投入很少，后续可根据实际业务需求逐步扩大投资 |
| 运维成本 | 需大批专业人员维护相关设备，运维成本高                                  | 无需关注运维，无需专业维护人员投入             |

云灾备方案以经济、高效、弹性的优势，将成为未来灾备领域发展的主要方向。

## 9.2 附录 灾备基本概念

灾备即是容灾与备份结合的保障企业数据、业务高可用的方案之一。根据可防范的风险内容、RTO/RPO核心灾备技术指标，可将灾备防护分为不同的等级。

### 关键技术指标

进行灾备解决方案设计时，需关注灾备的两个关键技术指标：

- RTO: RecoveryTime Object, 恢复时间目标。指灾难发生后，从IT系统宕机导致业务停顿之刻开始，到IT系统恢复至可以支持各部门运作，业务恢复运营之时，此两点之间的时间段称为RTO。RTO是反映业务恢复及时性的指标，体现了企业能容忍的IT系统最长恢复时间。RTO值越小，代表容灾系统的恢复能力越强，但企业投资也越高。
- RPO: Recovery Point Object, 恢复点目标。指灾难发生后，容灾系统进行数据恢复，恢复得来的数据所对应的时间点称为RPO。RPO是反映数据丢失量的指标，体现了企业能容忍的最大数据丢失量的指标。RPO值越小，代表企业数据丢失越少，企业损失越小。

### 灾备等级

根据《中华人民共和国国家标准 GB/T 20988-2007 信息安全技术 信息系统灾难恢复规范》，灾备的防护等级可分为以下几个等级。

| 防护等级            | 数据备份                                                                                                     | 数据备份处理     | 可防范的风险                                                                                               | RTO    | RPO    |
|-----------------|----------------------------------------------------------------------------------------------------------|------------|------------------------------------------------------------------------------------------------------|--------|--------|
| 第1级 基本支持        | <ul style="list-style-type: none"> <li>· 完全数据备份，每周一次</li> <li>· 备份介质场外存放</li> </ul>                      | -          | 业务数据破坏                                                                                               | 2天以上   | 1~7天   |
| 第2级 备用场地支持      | <ul style="list-style-type: none"> <li>· 完全数据备份每天一次</li> <li>· 备份介质场外存放</li> <li>· 每天多次定时批量传送</li> </ul> | 灾难时调配      | <ul style="list-style-type: none"> <li>· 业务数据损坏</li> <li>· 业务处理场地不可用</li> </ul>                      | 24小时以上 | 1~7天   |
| 第3级 电子传输和部分设备支持 | <ul style="list-style-type: none"> <li>· 完全数据备份每天一次</li> <li>· 备份介质场外存放</li> <li>· 每天多次定时批量传送</li> </ul> | 配备部分数据处理设备 | <ul style="list-style-type: none"> <li>· 业务数据损坏</li> <li>· 业务处理场地不可用</li> <li>· 部分设备/网络故障</li> </ul> | 12小时以上 | 数小时~1天 |

| 防护等级              | 数据备份                                                                                                         | 数据备份处理                                                                                                                         | 可防范的风险                                                                                                 | RTO    | RPO    |
|-------------------|--------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|--------|--------|
| 第4级 电子传输及完整设备支持   | <ul style="list-style-type: none"> <li>· 完全数据备份每天一次</li> <li>· 备份介质场外存放</li> <li>· 每天多次定时批量传送</li> </ul>     | 全部设备，可用状态（冷战）                                                                                                                  | <ul style="list-style-type: none"> <li>· 业务数据损坏</li> <li>· 业务处理场地不可用</li> <li>· 全部备用设备/网络故障</li> </ul> | 数小时~2天 | 数小时~1天 |
| 第5级 实施数据传输及完整设备支持 | <ul style="list-style-type: none"> <li>· 完全数据备份每天一次</li> <li>· 备份介质场外存放</li> <li>· 数据实时复制</li> </ul>         | 全部设备，就绪/运行状态（温站）                                                                                                               | <ul style="list-style-type: none"> <li>· 业务数据损坏</li> <li>· 业务处理场地不可用</li> <li>· 全部备用设备/网络故障</li> </ul> | 数分钟~2天 | 0~30分钟 |
| 第6级 数据零丢失和远程集群支持  | <ul style="list-style-type: none"> <li>· 完全数据备份每天一次</li> <li>· 备份介质场外存放</li> <li>· 同步实时备份，实现数据零丢失</li> </ul> | <ul style="list-style-type: none"> <li>· 备用与生产的处理能力一致并完全兼容</li> <li>· 应用软件集群、实时无缝切换</li> <li>· 远程集群系统的实时监控和自动切换（热活）</li> </ul> | <ul style="list-style-type: none"> <li>· 业务数据损坏</li> <li>· 业务处理场地不可用</li> <li>· 全部备用设备/网络故障</li> </ul> | 数分钟    | 0      |

#### 灾备方案要点

灾备方案的核心内容是帮助企业平衡 RTO 和 RPO 的需求，找到最佳实现技术和手段。从经济角度，帮助企业找到最佳的总体投入（TCO）和投资回报（ROI）。