**北京沃丰时代数据科技有限公司**

数据灾难恢复与业务可用性连续性

**文档信息：**

|  |  |  |  |
| --- | --- | --- | --- |
| **文档名称** | 数据灾难恢复与业务可用性连续性 | | |
| **文档编号** | WF-CS003 | | |
| **文档密级** | 内部 | **发布范围** | 公司内部 |
| **编制人** | 赵栋 | **编制日期** | 2018-12-17 |
| **评审人** | 周毅 | **评审日期** | 2023-03-23 |
| **批准人** | 张磊 | **批准日期** | 2023-04-23 |

**修订历史记录：**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **版本** | **状态** | **修订内容说明** | **修订日期** | **编制人** |
| V1.0 | 新建 | 新增 | 2018-12-17 | 赵栋 |
| V1.1 | 修订 | 修订文档编号 | 2022-01-15 | 周毅 |
| V1.2 | 修订 | 修订文档信息 | 2023-04-23 | 张帆 |
|  |  |  |  |  |
|  |  |  |  |  |

目录

[1. 数据灾难与恢复 2](#_Toc28337526)

[1.1 项目代码备份与恢复 2](#_Toc28337527)

[1.2 日志备份与恢复 3](#_Toc28337528)

[1.3 数据库备份与恢复 3](#_Toc28337529)

[2.业务可用性连续性 5](#_Toc28337530)

[2.1 接入层 5](#_Toc28337531)

[2.2 应用层 6](#_Toc28337532)

[2.3 数据库层 7](#_Toc28337533)

[2.4 网络层 7](#_Toc28337534)

[2.5 存储层 7](#_Toc28337535)

1. 数据灾难与恢复

1.1 项目代码备份与恢复

|  |  |
| --- | --- |
| 代码备份 | 1.项目代码存储在阿里云ECS上的Gitlab（分布式数据存储仓库），备份采用阿里云磁盘镜像技术，每天凌晨定时磁盘快照，保留5天的快照 |
| 代码恢复 | 1. 阿里云ECS出现故障时，阿里云可以将ECS迁移到不同的物理机上，迁移之后ECS的网络IP不会发生改变，数据是完整的 |
| 1. Gitlab 服务出现问题时，通过每天的磁盘快照来数据恢复 |

* 1. 日志备份与恢复

|  |  |
| --- | --- |
| 日志备份 | 1. 本地数据备份，项目日志会按天或者按小时切割压缩日志，在本地保留一周时间 |
| 2.远程备份，每天定时将日志存储到远程的NAS存储上，保留一月的数据 |
| 日志恢复 | 1.本地日志丢失，通过NAS存储日志备份的数据恢复 |
| 2.NAS存储故障，NAS存储本身是多磁盘多副本，阿里云保证数据不会丢失 |

* 1. 数据库备份与恢复

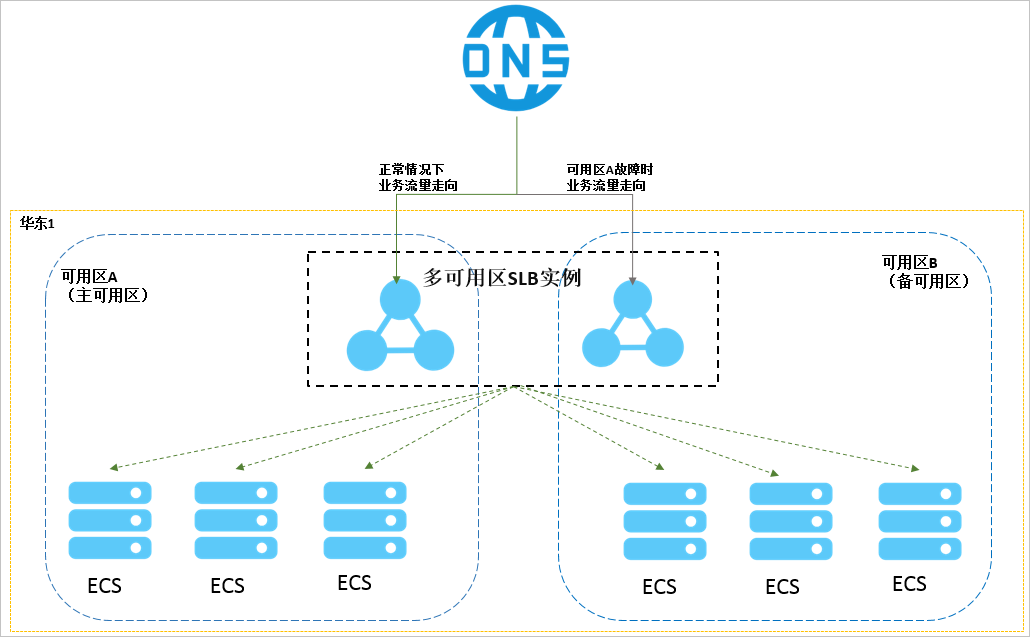
|  |  |
| --- | --- |
| 数据备份 | 1.数据库使用阿里云RDS，每周1、3、5、7对数据进行全量备份，保存7天 |
| 2.数据库增量备份，Binlog大小超过500MB或写入超过6小时就会切换到新的Binlog文件继续写入，保存7天 |
| 数据恢复 | 1. 全量恢复，通过阿里云RDS控制台恢复，选择对应的备份历史进行恢复 |
| 1. 增量恢复，通过阿里云RDS控制台，选择对应的时间点进行恢复 |

2.业务可用性连续性

2.1 接入层

接入层采用阿里云负载均衡服务，简称SLB。

负载均衡实例采用集群部署，以消除服务器单点故障，提升冗余，保证服务的稳定性。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。



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。

2.2 应用层

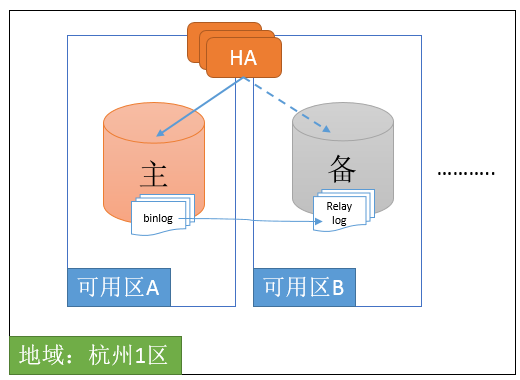
应用层采用阿里云弹性计算服务，简称ECS。

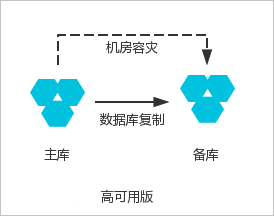
相较于普通的IDC机房以及服务器厂商，阿里云使用更严格的IDC标准、服务器准入标准以及运维标准，保证云计算基础框架的高可用性、数据的可靠性以及云服务器的高可用性。

公司所有项目的应用层均采用多可用区部署方案搭建主备服务或者双活服务。此外，ECS实例支持弹性伸缩，包括纵向的弹性和横向的弹性。纵向弹性即单台云服务器ECS的配置变更，可以根据业务量的增减自由变更配置。横向的弹性，对于高峰期可以使用弹性的方式横向扩展出多台，当业务高峰消失时，可以将多余的资源释放掉，以减少业务成本。

2.3 数据库层

数据库层采用阿里云的云数据库服务，简称RDS。

线上项目采用高可用版本的RDS，其采用一主一备的双机热备架构，当主节点故障时，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。



2.4 网络层

网络层采用NAT网关和专有网络（简称VPC）。

NAT网关跨可用区部署，可用性高。单个可用区的任何故障都不会影响NAT网关的业务连续性。

阿里云所有线路使用BGP线路，当单条线路出现问题时候，服务依然是可用的。

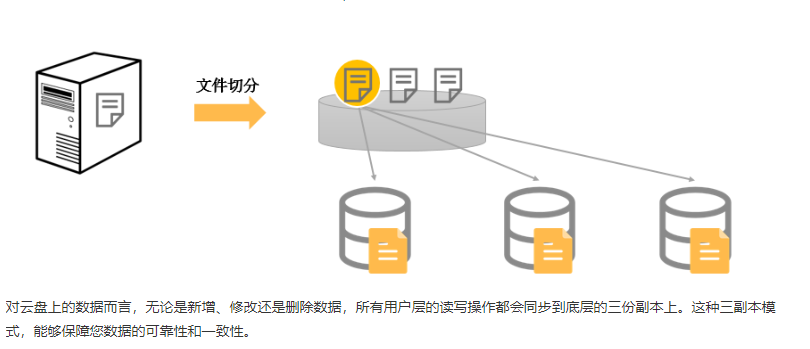
另外，当公司网络故障，网络管理员会排查问题原因，如果此时线上有紧张问题，通过手机4G网络进行远程维护。

2.5 存储层

存储层代用ECS云盘、OSS、NAS等存储服务。

阿里云云盘三副本技术通过分布式文件系统为云服务器ECS提供稳定、高效、可靠的数据随机访问能力，为ECS实例实现99.9999999%的数据可靠性保证。

当有数据节点损坏，或者某个数据节点上的部分硬盘发生故障时，集群中部分Chunk的有效副本数就会小于三。此时，Master就会发起自动同步任务，在Chunk Server之间复制数据，使集群中所有Chunk的有效副本数达到三份。







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。

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作为阿里巴巴全集团数据存储的核心基础设施，多年支撑双11业务高峰，历经高可用与高可靠的严苛考验。OSS的多重冗余架构设计，为数据持久存储提供可靠保障。同时，OSS基于高可用架构设计，消除单节故障，确保数据业务的持续性。

OSS有以下优势：

1）服务设计可用性不低于99.995%。

2）数据设计持久性不低于99.9999999999%（12个9）。

3）规模自动扩展，不影响对外服务。

4）数据自动多重冗余备份。

存储层除采用ECS云盘、OSS对象存储外，还采用了文件存储（简称NAS），其也是采用三副本技术，通过分布式文件系统为存储盘提供稳定、高效、可靠地数据读写能力。生产环境对文件存储添加了备份策略，以生成多个备份副本数据，在发生数据损坏时进行恢复。

1. 线上变更

生产环境配置变更严格按照线上环境配置变更规范，每一次变更都有负责人，每一项操作都有对应的操作人和检查人。

1. 线上业务遭受网络攻击

当遭遇网络攻击的时候，马上成立应急响应小组，第一时间确认攻击影响范围，定位攻击来源，及时的做出应急响应。

