# 概述

主要涉及故障检测、故障隔离、故障备份和故障恢复。

# 特征

## 主从切换

高可用最主要的就是出现故障时，能够做到业务的无缝迁移，即主备切换。

当其中一台机器的服务宕机后，对于服务调用者来说，能够迅速的切换到其他可用服务，当服务升级为主服务，这种切换速度应当控制在秒级别（几秒钟）。

当宕机的服务恢复之后，自动变为从服务，主从服务角色切换。主从切换一定是要付出代价的，所以当主服务恢复之后，也就不再替换现有的主服务。

## 负载均衡

当服务的请求量比较高的时候，一台服务不能满足需求，这时候需要多台机器提供同样的服务，将所有请求分发到不同机器上。

高可用架构中应该具有丰富的负载均衡策略和易调节负载的方式。甚至可以自动化智能调节，例如由于机器性能的原因，响应时间可能不一样，这时候可以向性能差的机器少一点分发量，保证各个机器响应时间的均衡。

## 易横向拓展

当用户越来越多，已有服务不能承载更多的用户的时候，便需要对服务进行拓展，扩展的方式最好是不触动原有的服务，对于服务的调用者是透明的。

# 方案

## 腾讯

## 阿里

# 应用

## 组建高可用

采用去中心化设计，整个集群无单点。

### 计算节点高可用

计算节点是无状态节点，一般要求为每个业务至少配置2个计算节点。

为降低计算节点异常对业务的影响，可以采用的措施：

1. 监控节点健康状况；
2. 在某些节点发生故障时，实现故障的接管；
3. 异常事务清理

### 数据节点高可用

为了提升数据服务的可靠性和可用性，安全组Group一般由多个数据节点组成。其中一个数据节点为主节点，提供读写服务，其他节点为备节点，提供读服务，在一个安全组中可以设置多个副本。

通过数据节点主备间通过数据库的复制技术来进行主备机之间的数据同步，主机至多个备机之间为星型复制模式，即主机直接向多个备机进行数据同步，具体方式目前支持半同步和异步两种。

为了权衡高可用和高性能，一般有以下几种策略：

**最大性能策略**

底层的数据节点提供最大的写性能，副本间采用异步赋值，即一旦日志数据写到主节点，事务即可提交。

**最大保护策略**

日志数据必须同时写出到主用数据节点和至少一个备用数据节点，事务才被提交。

**最大可用策略**

### 全局事务管理节点高可用

全局事务管理需要支持双机热备部署，主备双活，实现故障时秒级切换。

### 管理节点高可用

管理节点采用双机冷备的模式，可以实现秒级切换。

## 容灾

### 衡量指标

在容灾恢复方面，目前业界公认有三个目标值。

1. 恢复时间：企业能够忍受多长时间没有IT，处于停业状态；
2. 网络多长时间能够恢复；
3. 业务层面的恢复。

整个恢复过程中，最关键的衡量指标有两个：一个是RTO，一个是RPO。

所谓RTO，Recovery Time Object，它是指灾难发生后，从IT系统当前导致业务停顿开始，到IT系统恢复至可以支持各部门运作、恢复运营之时，此两点之间的时间段称为RTO。

所谓RPO，Recovery Point Object，是指从系统和应用数据而言，要实现能够恢复至可以支持各部门业务运作，系统及生产数据应恢复到怎么样的更新程度。这种更新程度可以是上一周的备份数据，也可以是上一次交易的实时数据。

### 同城双活

### 异地容灾