高可用系统研究

张彦

修订于2016-12-01

MEIZU

大纲

- 什么是高可用系统
- 如何搭建高可用系统

什么是高可用系统

- 符合下述的2个特征就是高可用系统
  - 单位时间内，系统不可用的时间短
    - 例如：一年内，系统不可用的时间不超过5分钟
  - 若发生系统不可用，能在短时间内恢复可用
    - 例如：若在10年内总的不可用时间不超过50分钟，但其中某一次不可用时间就达到40分钟，也不算是一个高可用系统

两个指标

- 可靠性
  - 平均无故障工作时间MTTF
- 可维护性
  - 平均故障修复时间MTTR
- 要提高可用性，就要想法提高这2个指标

如何搭建高可用系统

- 从软硬件环境角度
  - 系统稳定，故障率低
  - 冗余部署，及时切换
- 从运营维护角度
  - 按计划停、开机
  - 预言故障，早作准备
  - 故障突发时，及时发现，定位故障原因，迅速修复

从软件环境角度

- 使用主流和成熟的技术，新技术选型慎重
- 软件过程受控，软件质量高
- 软件系统具有良好的扩展性，采用模块化的架构设计，支持热部署，配置更新不停机
- 采用分布式架构，可集群部署，平滑的集群扩张

技术选型

- 当前处于技术爆炸的年代，各种新技术层出不穷
- 技术选型不能太激进，建设一个稳定的系统是最重要的
- LAMP、JAVA EE都是主流且成熟的技术框架

软件过程

- 目标
  - 开发高质量的软件
  - 培训高素质的人员
- 确立软件过程，制定相关的规范、流程
- 分析、设计、开发、测试、培训和部署
- 里程碑和检查点
- 关键过程域（KPA）
  - 项目计划
  - 需求管理
  - 设计评审
  - 配置管理
  - 变更管理
  - 代码走读，同行评审
  - 技能培训和软件过程流程培训

扩展性和模块化

- 软件架构要考虑扩展性
- 模块化带来平滑的扩展
  - 扩展时不需要重新启动系统
- 采用模块化架构是一种解决方案
  - JavaEE的oSGI支持模块化，可动态加载和卸载模块，避免重启服务

分布式架构

- 分布式架构可用于创建集群
  - 负载均衡
  - 通过冗余，提高可用性

分布式架构实践

- 状态信息集中存储
  - 例如，web应用程序中的session，保存到缓存服务器中，当前主流的分布式缓存有memcache，redis等
- 锁定当前资源
  - 单部署时，不存在资源争用，在分布式环境里，要采用对资源加锁的方法避免争用
- 分布式文件系统
  - 分布式文件系统，例如FastDFS，对大量小文件的处理能提供稳定性和更好的性能
- Nosql数据库
  - Nosql数据库更适合在互联网环境下处理海量数据

从硬件的角度

- 服务器可靠，避免硬件故障
- 服务器所处环境可靠，避免自然灾害
- 网络通畅，带宽充足

服务器可用性

- 有冗余设备
  - 冗余电源
  - 冗余网卡
- 磁盘raid
  - 提供数据安全性
  - 抵抗硬盘故障

机房环境

- 机房质量
- 工作人员素质
- 服务响应时间

网络线路

- 带宽
  - 带宽充足
- BGP机房
  - 电信联通移动无障碍

从软硬件结合的角度

- 以冗余抗风险
  - 集群部署
  - 服务器双工/多工方式
  - 备份的网络线路
  - 多个资源提供商（CDN，短信通道，支付通道），分散风险
- 状态侦测和自动切换
  - 如果故障发生时能自动切换到备用系统，则可靠性大大提高
  - 自动切换的前提是状态侦测

冗余部署

- 冗余部署是提高可靠性的有效手段
- 重要的系统必须有冗余部署
- 采用主备机的方式
  - 正常情况下主机提供服务，一旦主机故障，能迅速切换为备机提供服务
  - 通过keepalive侦测主机故障并自动切换ip
- 采用集群部署的方式
  - 集群里的单个服务器故障，不影响整个集群
  - 应用程序支持分布式架构
  - 集群规模收缩和扩张都不需要重启

从运营维护的角度

- 按计划停机
  - 软硬件升级
    - 在软、硬件系统升级前，制定计划
    - 列出可能的风险，并预备风险处理方案
    - 严格按计划执行升级
  - 维护性停机，定期进行
    - 通过在业务低峰期有计划的停机重启，避免在业务高峰期突发故障
    - 确定哪些系统要按计划维护性停机，及停机的周期
  - 更新配置
    - 设计系统，避免更新配置需要停机
    - 配置服务器统一配置管理，配置更新自动广播

预言故障，早作准备

- 故障是可以预测的
  - 根据历史数据
    - 业务高峰期易发生故障
    - 新业务上线易发生故障
    - 系统升级易发生故障
  - 根据环境变化
    - 对外部环境要敏感，第三方资源的异常也会影响可用性
    - 与第三方保持良好的沟通，提前获取异动信息

故障突发处理

- 建立突发故障处理流程
- 组建突发故障处理小组
- 沟通渠道
  - 发生故障时，确保对内对外沟通无障碍
- 故障分级制度
  - 不同级别的故障的界定
  - 不同级别故障的处理授权
  - 故障级别的升迁
  - 故障处理的沟通机制

故障突发处理

- 迅速发现故障
  - 早一分钟发现，早一分钟处理，早一分钟修复
  - 自动化监控工具，能及时发现大多数故障
    - 自行开发监控工具
    - 采购专业的监控工具
    - 使用免费的监控工具
  - 运营维护人员能更准确的判断是否发生故障
    - 运维人员的经验
    - 运维人员的责任感

故障突发处理

- 迅速定位故障
  - 软件系统故障
  - 硬件环境故障
  - 外部环境故障
- 只有定位故障才能找到故障原因
  - 凭经验定位故障
  - 分析日志定位故障
  - 使用Profiler工具
  - 采用自动测试工具，执行测试用例定位故障

故障突发处理

- 迅速修复故障
  - 启用备用系统
  - 回滚到上一个版本
  - 修复在线bug
- 运维知识库
  - 从运维知识库查询类似故障修复步骤
- 故障处理预案
- 故障处理总结

THE END

谢谢观看

MEIZU