DevOps 全攻略精选十二计 v0.1

1、整体框架图

说明：

1、 本文档所有权为高效运维社区，版本为 **V0.1 2017.03.21**

2、 本文档所有内容的开源授权基于 **CC-BY-NC-ND-3.0**；

3、 如需成为联合编撰者（甚至仅修改某些计策）， 请联系@梁定安，电话/微信：**15986614377**

2、攻略目录（十二计）

三十六计 - 持续集成 - 张乐

1. 开发人员每天至少向版本库提交一次代码
2. 执行测试是构建过程的一部分
3. 不要提交无法编译或不能通过测试的代码
4. 每次变更都执行构建，以便尽早发现缺陷
5. 做到只执行一个命令，就能够取出最新的代码，并执行构建
6. 创建一致的目录结构，让构建更容易
7. 通过增加服务器资源、分离较慢的测试、分阶段构建等方法，加快构建速度
8. 修复失败的构建是最高优先级的事情
9. 导致构建失败的开发人员必须参与修复失败构建的工作
10. 将 DDL 和 DML 脚本提交到版本库，以便使用脚本重建数据库和测试数据
11. 将测试分组，按不同时间间隔运行较快和较慢的测试
12. 采集构建相关度量指标，作为持续改

三十六计- 持续部 - 乐

1. 为软件发布创建一个可重复可靠的过程
2. 将编译、测试、部署、发布等几乎所有活动进行自动化
3. 将代码、测试、配置、部署脚本、环境描述等几乎所有内容纳入版本控制
4. 提前并频繁做让你感到痛苦的事情
5. 每次变更都要立即在流水线中传递
6. 时刻准备回滚到前一个版本
7. 只生成一次二进制包
8. 对不同环境采用相同的部署方式
9. 对部署进行冒烟测试
10. 只要有环节失败，就停止整个流水线
11. 分级分层的测试，形成完备的质量防护网
12. 使用蓝绿部署、金丝雀发布等技术来管理发布

三十六计 - 测试方法 - 徐奇琛、潘晓明

1. 需求评审阶段至关重要，各角色重视对需求的评审与管理，控制需求质量建立 ROI 度量。
2. 统一提测流程及 CICD 平台，标准化建设可以有效收敛大量问题降低沟通成本。
3. 避免陷入细节，先覆盖主流程和重要功能模块，可将部分风险提前暴露，真正做到进度控制、风险控制。
4. 移动互联网时代，兼容性乃用户可用性的前提，建立动态运营和加强三方平台合作作为立足之本。
5. 大厂的方案和标准不一定完全适合你的业务，针对产品特点、问题场景建立适合自身的专项测试方案，做到有的放矢并聚焦专项的痛点问题。
6. 集成阶段任何的变化都可能带来蝴蝶效应，必须持续交付和针对性的回归控制风险。
7. 精细化产品的灰度能力，区分场景和建立数据模型。
8. 灰度后的最终交付（最终包）必须再次测试覆盖。
9. 再完善的质量体系覆盖也不能保障线上没[illegible]发问题，功能的开关控制及降级措施，是最后一道质量保护屏障，任何模块[illegible]都需要考虑和设计。
10. 产品质量永远不单单是测试团队[illegible]责，各[illegible]环节都有主动收敛问题的流程和渠道，应建立共赢思维，持续高效地协
11. Appium: 成熟的，适用于移动 app 的自动化工具。它基于 Android 的 uiautomator 框架和 iOS 的 automation 框架(现已被 xctest 取代)。它使用类似 c/s 结构，通过服务端解析界面元素，同时提供了一套完整的 api，支持屏幕旋转，摇晃等 app 特有的操作。成为 移动 app 自动化测试的业绩标杆类工具
12. 持续的引入业界和一线大厂的开源代码扫描框架以及专业付费厂商提升代码覆盖降低代码隐患。

三十六计 - 大数据运维 - 范伦挺

1. 任何数据删除都要默认进回收站，不可偷懒跳过。
2. 所有配置里的秘钥要加密存储，关注平台安全。
3. 轻量级非数据服务要有机房间切换能力，加快恢复速度。

4. 大规模和小规模场景不是量的变化，是质的差异。
5. 实时计算链路长，延时敏感，要有各阶段的详细监控指标，方便问题定位。
6. 提供用户自助排查作业和重启等基础运维能力。
7. 出问题的第一时间要公告给用户，否则各种询问的唾沫会淹死你。
8. 存储瓶颈除了容量，文件数也是个大问题。
9. 大规模计算平台至少要能容忍单机故障，否则别让他上线。
10. 离在线混布是个节约的好思路。
11. hdd&sdd 混合存储提升 shuffle 性能。
12. 规模大、压力大，要时刻关注硬件和网络发展，尽快拿到科技红利。

三十六计 - 自动化运维 - 胥峰

1. 自动化运维的终极目标是消灭 SecureCRT 和 Putty 等一切远程客户端，让平台成为唯一 入口。
2. 自动化运维的第一步是脚本化，通过[illegible]可重复的基础架构和环境。
3. 你不用造轮子，可以先考虑开源[illegible]加二次开发满足运维需求。
4. 高效是自动化运维的要求，使用[illegible]或者[illegible]型等提高并行效率。
5. 安全必须是内置在自动化运维中的，通过[illegible]发现和深度防御机制保障安全。
6. 集中控制节点和被控节点加密数据通信。
7. 可以使用价值流程图分析当前的效率瓶颈和确认痛点。
8. 自动化运维的底层数据必须保证完整性，技术手段与流程保障并行。
9. 以自动探测和上报提高 CMDB 配置的效率和维护数据准确性。
10. 监控体系的自动化是整个体系的纽带，它贯穿着事件和故障自愈。
11. 设计大规模监控体系的自动注册功能，不以手动添加被监控指标。
12. 坚持持续改进的监控目标，持续减少漏报和误报比例。

三十六计 - 日常运维 - 梁定安

1. 应对故障要先恢复再排查，无计可施重启试试
2. 运维脚本要带上版本和备注

3. 批量操作前，请先灰度再全量
4. 网络安全要牢记，开放外网高危端口需谨慎
5. 慎防进程 D 状态，及时监控保可用
6. 敏感权限应定期 review，离职转岗应及时清理
7. 保持应用运行的独立性，防止交叉依赖的程序存在
8. 每个偶然的故障背后都深藏着必然的联系，找到问题根源并优化掉
9. 运维的标配软技能：责任心、沟通力、执行力
10. 日常运维口令：打补丁、传文件、批处理、改配置、包管理、看监控
11. 先量化管理运维对象，再优化管理运维对象
12. 对不可逆的删除或修改操作，尽量延迟或慢速执行

三十六计 - MySQL 运维 - 叶金荣

1. 光做好备份还不够，还要做恢复测试，并且检查数据有效性
2. 管理用户和业务用户区分不同权限[illegible]用户切记不可授权过高
3. 绝不监听公网 IP，并用防火墙挡住[illegible]降低被入侵风险
4. 高 InnoDB 表性能、避免主从[illegible]
5. 基数低的列，强烈不建议单独创建索引[illegible]放在联合索引中）
6. 联合索引中，基数高的列放在前面，基数低的列放在后面
7. 性能、压力测试时，测试机客户机一定要和 Server 端分开
8. 连接数爆满时更应该调低最大连接数，而非调高，并且尽快用上 thread pool
9. 环境初始化之一：开启 CPU 最大性能模式
10. mysqld 进程占用 CPU %user 突然飙高，99.99%是因为索引不当导致
11. 每个 SQL 条件都加上引号，并对用户输入强制类型转换，避免 SQL 注入及类型隐式转换风险
12. 不要直接删除数据表，而是先 RENAME；删除大表用硬链接方式更高效

三十六计 - 数据库运维 - 周小军

1. 没有规则创造规则，有规则遵守规则；

2. 养成日常巡检核心监控属性的习惯
3. 数据库要具备限流能力
4. 角色权限要划分清楚，开发权限要最小化原则
5. 业务初期做好分库分库的规划
6. 做好日常数据库容量度量，用历史数据推算下一个容量高峰
7. 对索引要根据访问类型做战略性规划
8. 避免单点：有效可恢复的数据备份，有效可切换的从节点
9. 精通业务，推动业务采用更合适的架构方案
10. 备份系统自动化，中心化调度，保障故障效率和可用性
11. 数据备份 100%覆盖，100%可恢复，每年至少 2 次恢复演练
12. 数据垂直分层自动调度（内存，SSD，SAS，SATA），做到成本与效率的性价比最高

三十六计 - CDN 运营 -高向冉

1. SSL 证书不能放在现网，必须独立
2. 要分平台域名，不能让 DDos 把
3. 必须关注回源率，回源率高的
4. 域名操作要谨慎，出了问题可能影响
5. HTTPS 域名劫持最高优先级反馈至运营商
6. 内核是传输协议根本，传输协议是网络加速的利器，系统内核监控不能少。
7. Cache 模型尽量使用分片淘汰模式，提升命中率
8. 核心业务调度要以本地覆盖调度模式优先，成本优先的业务以削峰填谷的调度模式优先
9. 用户层监控很重要，要有模拟或真实用户的监控。
10. 故障恢复时间能快则快，哪怕一分钟，TTL 生效时间要针对业务适配
11. 调度系统和 DNS 解析系统必须多地(超过 3 地)容灾部署，如果挂掉影响全局
12. CDN 平台一定要有突发池，灵活调度才能保证平台健康发展。

三十六计 - 存储运营 - 高向冉

1. 数据安全是底线，即使不服务也不能丢数据。
2. 多份存储变更时先变更单份数据节点
3. 变更先少量灰度，变更之前先准备回退方案
4. 索引数据很重要，带状态的模块要注意数据安全，不要随意迁移和清 cache。
5. 更换磁盘必须检查 SN 号
6. 运维删除数据务必备份，并且要谨慎，禁止人工线上删除数据
7. 磁盘更换机器死机必须在一个周期内恢复，否则无法达到 N 个 9 的要求。
8. 存储机架和普通设备不一样，用电也不同，做好机架和交换机级别的容灾备份。
9. 存储不仅仅关注容量还要关注 inode 情况
10. 存储平台是 IO 操作型集群，要和计算资源一起复用做到设备最大化利用。
11. 不同年限的设备性能不同，磁盘读写能力不一致，要区别对待，老化磁盘要定期淘汰。
12. 存储冷热数据分离，业务一定要能[illegible]据。

三十六计 - 网络运[illegible] - 张永福

1. 生产网络的变更切记三思而后行，一个回车敲下去是永远无法撤回。
2. 网络攻城狮要想解放自己，要么学会 coding，要么和程序猿搞好关系。
3. 网络监控不是监控网络，目的是监控业务。
4. 不要轻易相信厂商的方案，在 lab 里面验证后再上线，你比厂商懂自己网络上的业务。
5. 链路的物理承载类型分清楚：裸纤直连、传输电路或是二层专线
6. 面对闪断，要确定好抑制策略和回切策略
7. 传输运维工程师三板斧：看告警、查光功率、环回测试
8. 变更执行的关键，是现场实施人员受控
9. 意识问题，提高重视程度。往往都是小变更出现故障，大变更因为非常重视，一般不出故障。
10. 变更前环境检查、信息收集必须到位，变更后的前后对比。
11. 建立完善的流程制度是运维管理的核心价值

12. 口说无凭，以工单办事

三十六计 - 安全运维 - 韩方

1. 进程启动权限最小化，尽可能使用非 root 账号启动进程
2. 停用和关闭无用的服务，系统服务最小化
3. Linux 下的 ps，netsat 系统命令看到的不一定是操作系统的返回信息， 也可能是木马伪 装后的信息，系统命令有可能篡改，系统内核调用可能被替换
4. 大量的会话状态跟踪表 full 日志异常也可能是被攻击导致；
5. CC 攻击(http flood)服务器上最简单的对抗方法就是限制单 ip 的同时并发请求数; 6. Syslog,authlog 等日志定期备份，便于安全事件的追溯和审计
7. 重要密码一定不能同其他互联网账号密码相同，特别是同其他小网站的账号密码相同， 避免被撞库
8. 运行的业务进程尽不要输出敏感信息到日志文件中，比如避免 java 代码打印数据库连 接的账号信息等；
9. Shell 或 python 等脚本代码的每 这 定要进行加密， 比如 shell 中的数据库访问使 用的账号和密码就需要进 来提 性
10. SSH 等远程登录一定要限制访问 或 堡垒机 IP
11. Iptables 的防火墙规则数量过多，影响性能，可以使用其他基于 hash 查找的防火墙规则 实现的组件
12. Php 的相关危险函数和不需要的远程功能可以关闭

说明：