

中大型网站的运维体系

--诸超

zhuchao@gmail.com

Agenda

- 网站运维体系
- 网站运维常见问题
- 理想网站运维体系/我们的努力方向
 - 标准化: ops infrastructure & Dev Env
 - 技术组件化 & 服务化 , 人员专业化
 - 自动化运维: provision, release, mon;
 - 数据化运维: cmdb, log analysis,
 - 监控: technical/(server/app), end user point, business
 - 安全: network/server/app
 - Review架构设计 , 推动架构优化(简化)
- About DevOps , 应用运维
- 我的另外一些感想

中大型网站

■ 200-5000 服务器

■ 5-50个运维员工

■ 组织结构：

– 系统运维(IDC/Network/Server)

– 应用运维(Web/CDN Operation)

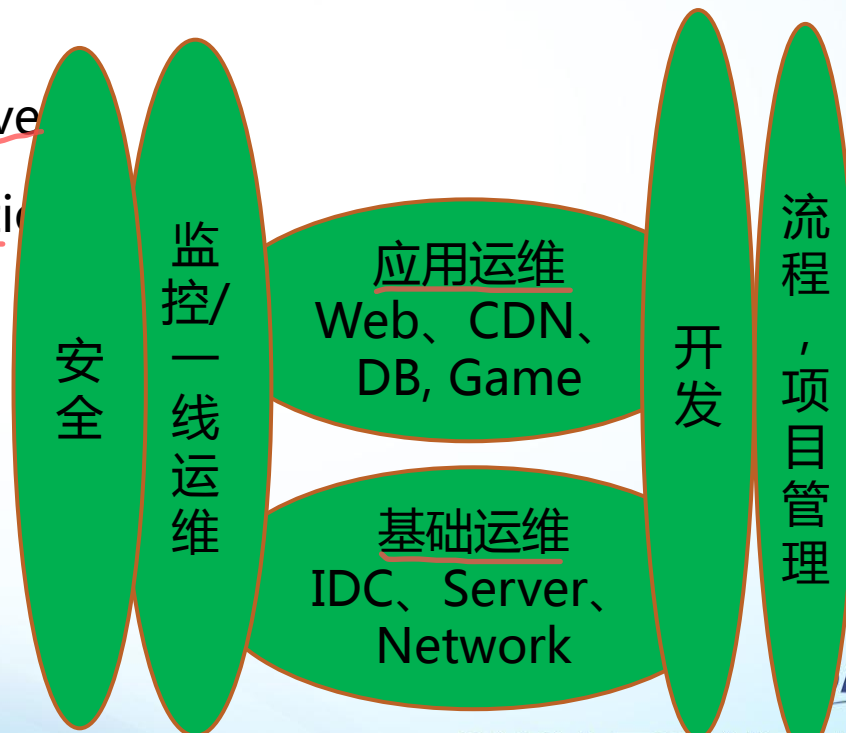
– 数据库

– 运维/平台开发

– 监控值班团队

– 安全

– 流程



2012中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2012

架构设计 · 自动化运维 · 云计算

互联网运维需要

✓ 稳定

✓ 低成本

✓ 快速响应

SACC

2012中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2012

架构设计 · 自动化运维 · 云计算

中小规模的网站运维都有些啥问题

- 人员
 - 不稳定
 - 人员总体过于Junior
 - 人员严重缺乏
- 规划乱：
 - 房建设快，CDN与核心网历史问题多；
 - 应用部署可依据规章少
 - 太多机房，利用率低，跨机房调用问题多
- 数据库跑在虚拟机上，外网上稳定性非常差：
 - 网络：大量单点，千兆互联瓶颈
 - 系统：大量的驱动问题
 - 应用：代码问题和部署问题一样多
 - 单点问题非常多
- 没有有效监控，没有容量分析系统没有规章：想怎么干就怎么干
 - 系统千奇百怪
 - 应用各自为政
 - 非常多单点（系统，应用）
 - 老机房机器30%以上没有人知道应用owner，没有系统密码
- 几乎全部手工操作（除了VOD VMS）：
 - 装机
 - 应用上包
 - 应用升级
 - 应用部署
- 安全问题突出

How

SACC

2012中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2012

架构设计 · 自动化运维 · 云计算

How

– 标准化，规范化：

- Kickstart/Puppet/LDAP/Zabbix/DNS

– 服务化

- 搭建运维基础架构，应用基础架构

具体？

– 监控

- 系统监控，应用监控，业务监控

– 自动化

- 装机，发布/Release，监控

– 数据化运维

- CMDB，日志分析，容量规划

– 网站安全

- 网络，系统，应用

– 推动架构优化/简化

SACC

2012中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2012

架构设计 · 自动化运维 · 云计算

另外

- Embracing the open-source
- Don' t re-invent the wheel
- Don' t be on your own
- Adapt the mainstream
- Don' t be too aggressive
- Simple is beauty

SACC

2012中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2012

架构设计 · 自动化运维 · 云计算

标准化规范化

SACC

2012中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2012

架构设计 · 自动化运维 · 云计算

统一规范化-Dev

- 统一公司层面运维支持技术开发平台
 - 控制研发技术使用
 - 不是想用什么技术就可以用什么技术的，
 - 要经过arch review讨论
 - 简化技术平台，有利于网站稳定和技术共享
 - 适当允许引入新技术
 - 维护一个稳定版，一个推进版
- 搞深搞好技术，不要啥都搞不懂
- 不随便引入新技术

统一规范化--Ops

■ 操作系统：

- OS Kickstart全部从Cobbler安装,取消光盘安装
- 硬件规格尽量统一，几个template(VM)
- OS内核，package 统一
- Puppet 控制系统和CDN应用
- 服务器命名
- 统一LB配置

■ 统一了，才不会出现诡异配置问题

统一应用部署模式

■ 各类应用基础架构

- 日志格式，路径
- 空间管理，日志删除
- 参数配置文件
- Java, PHP, MySQL, Redis 安装模板

■ guideline/Principle

- IDC consideration , App VM min 2; IP 分配：默认一律内网
- LB 公用：不许新建LB服务
- DB read高可用，写不管
- Cache Consideration
- Logging Consideration

■ 统一了，才能做自动化部署，分析，排障

运维基础服务化

SACC

2012中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2012

架构设计 · 自动化运维 · 云计算

运维基础服务化

■ 为什么要服务化

- 避免重复开发/部署，加快项目部署
- 更好积累经验，用精技术,不用每个业务有自己的Solution
- 避免单点，复用服务
- 简化故障排查，简化系统架构

基础运维基础组件

- Kickstart/Cobbler/Git
- LDAP
- DNS
- Zabbix
- Puppet
- CMDB

Puppet

■ 大规模运维必须的利器！

- 统一, 标准, 快速

■ 控制

- OS初始化
- App环境初始化
- LDAP, SSH, 等安全加固
- 全网/部分推送某个配置变化
- 应用直接部署

■ 注意控制节奏！

■ CDN应用

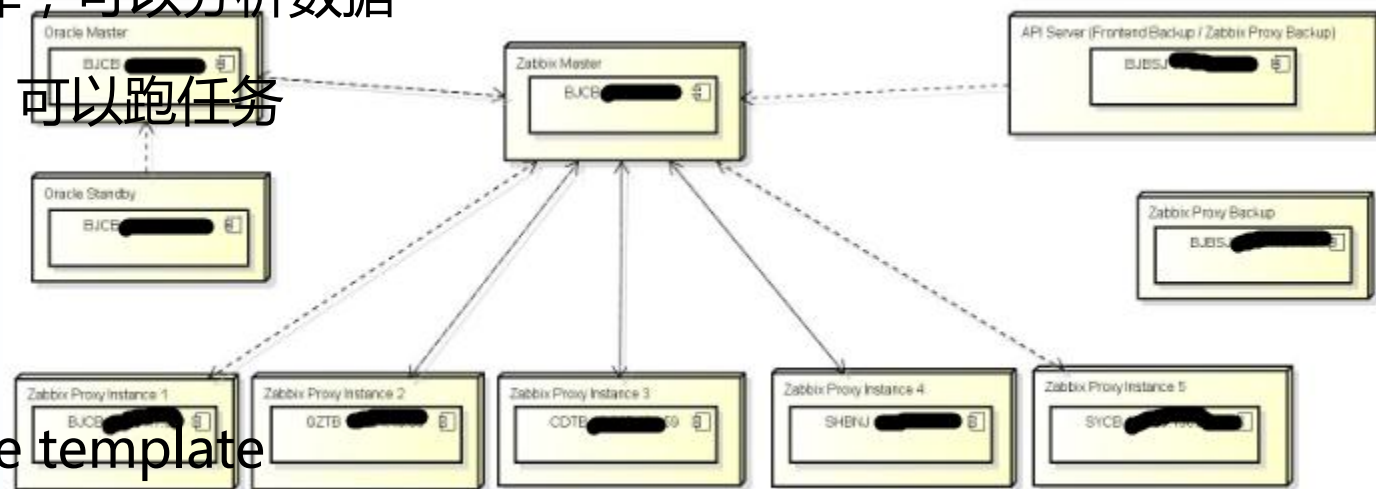
Zabbix

■ Why Zabbix

- 基于数据库，可以分析数据
- 有Agent，可以跑任务
- Flexible

■ Template

- Linux base template
 - Cpu/mem/net/disk/space/
- Def App template
 - Squid/Php/Resin/Nginx/memcache/redis/..
- Self-defined



CMDB

■ 资产：

- 多少机房，带宽，ip段，服务器，
- 各自型号分配，
- IDC分布，
- 过保分布，
- 基础运维服务透明化

■ 应用：

- 多少应用，各自是什么业务负责人（研发，运维），各自用了多少机器
- 有什么监控点(URLMON来读取)，
- 告警邮件直接抄送研发
- 上线自动添加监控，下线自动取消监控，维护自动暂停监控

SACC

2012中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2012

大会设计·自动化运维·云计算

各类服务

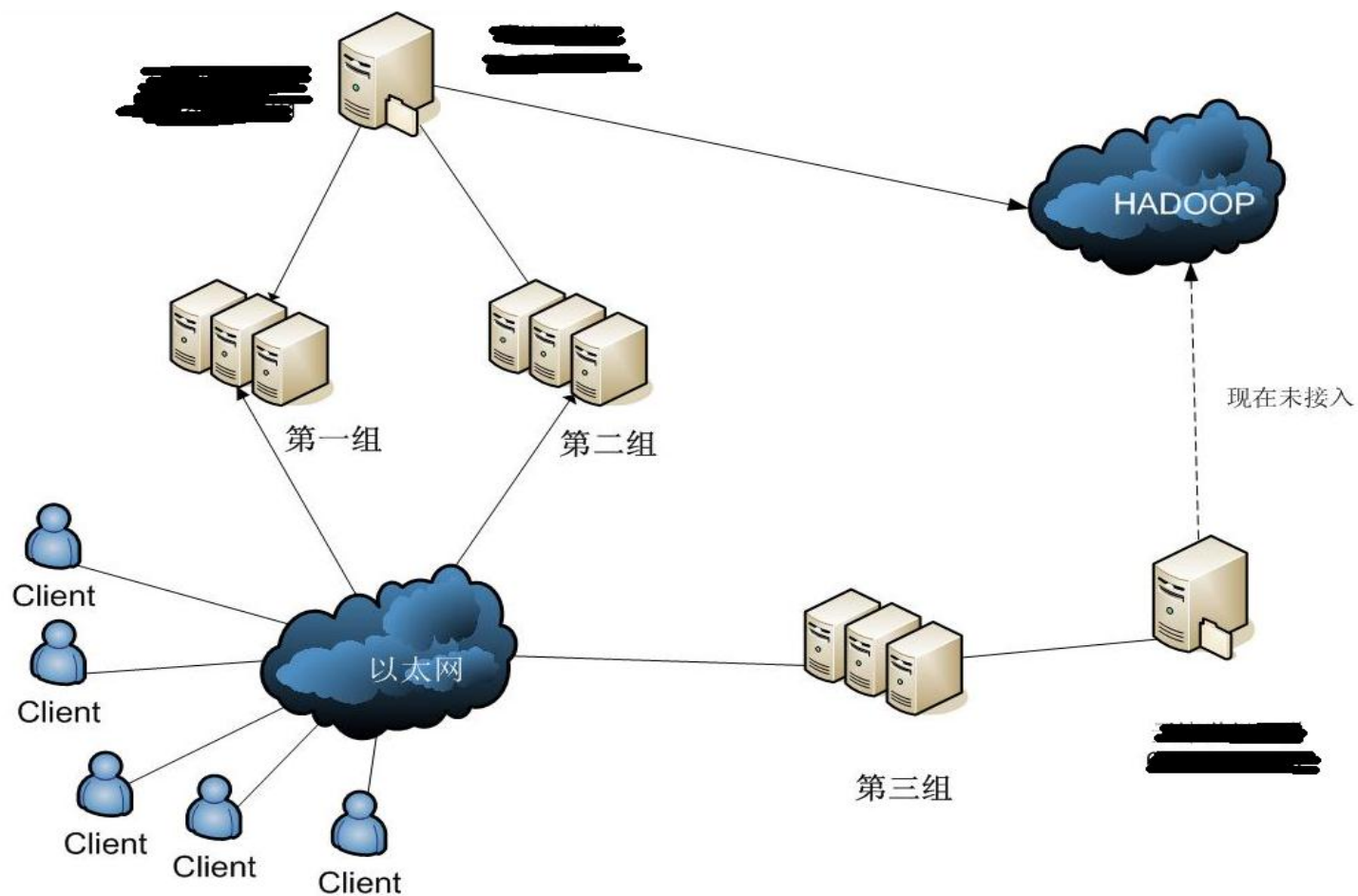
■ 日志相关：

- App日志接收平台，
- 各类Hadoop日志收集平台:Rsync
- 系统/安全日志: rsyslog
- Hive 日志分析
- 实时日志分析平台：fluentd+mongo+zabbix

各类服务

- 监控平台 : Zabbix+URLMon
- 自动化Release 平台
- 单点登录平台:CAS-SSO
- DFS
- Web源站统一: 统一管理优化
- 负载均衡服务化 : LB Pair
- Cache Tier: shared cache service(MC,Redis)
- Database as a service (MySQL)

App/客户端/Web 日志收集



日志传输平台

Why

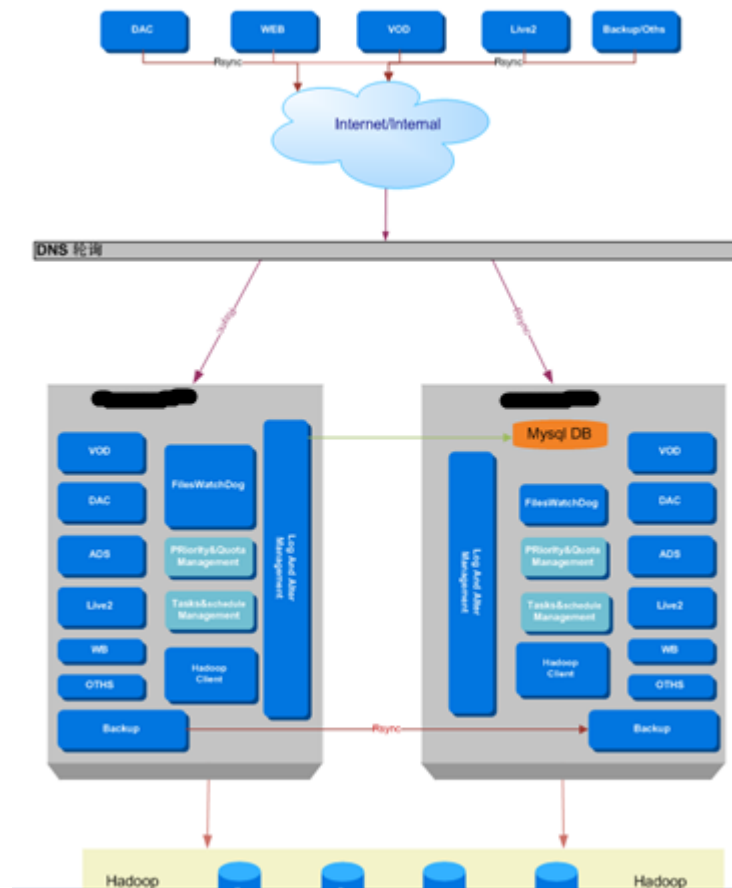
- 有10+ 不同日志进Hadoop需求
- 有5+ 不同进Hadoop的方案
- 断断续续轮流出问题

How :

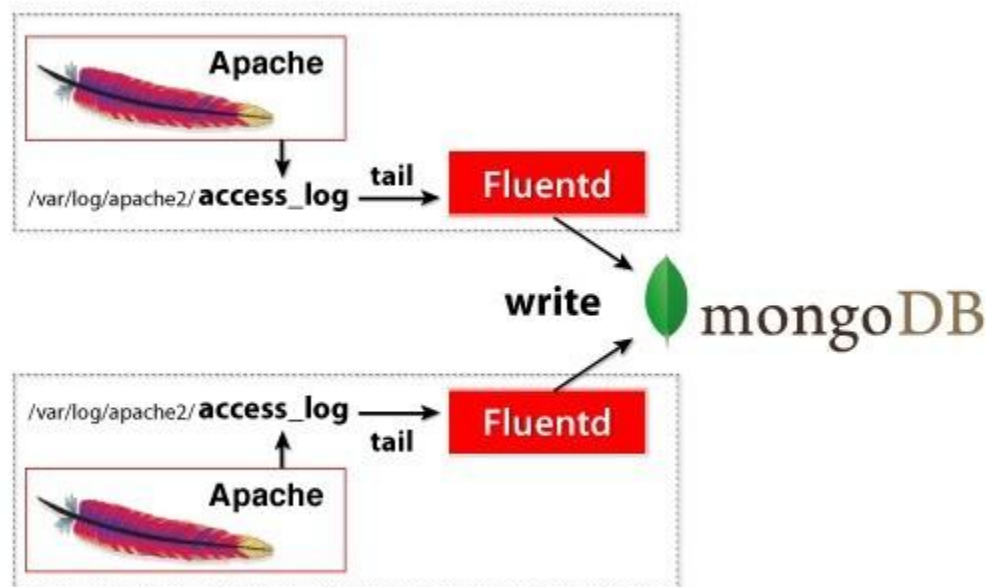
- 一个统一方案
- 吸取各个方案lesson
- 尽量简单稳定
- 非实时
- 新应用要用：配置客户端即可

2 基于Rsync Client+Server日志收集和管理方案

系统逻辑图



实时日志分析平台



离线日志分析

- Hadoop!
- Hive

SACC

2012中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2012

架构设计 · 自动化运维 · 云计算

安全日志分析(WIP)

- 系统: Rsyslog + **PHP**
 - Bash 日志
 - /var/log/message
 - 登陆日志
 - Sudo 日志
 - . . .
- Web安全 : fluentd+Mongo
 - Fluentd + mongo
 - LB post日志

监控

SACC

2012中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2012

架构设计 · 自动化运维 · 云计算

监控

- 定义KPI，定义Threshold
- Anything that fails will bother you
- 基础监控
 - 服务器
 - 网络：多机房，CDN，
 - App metrics：收集为主
- 应用监控/用户体验监控
 - 用户端URL监控
 - 程序接口监控
 - LB Traffic/code/Exceptions
- 业务数据监控
- 安全监控

告警

■ 监控容易告警难

- 需要多次反复调整
- severity
- 及时处理
- Snooze
- Tracking
- Report
- Analysis

■ 误报率

SACC

2012中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2012

架构设计 · 自动化运维 · 云计算

应用日志监控

- Linux系统/Nginx/PHP日志（关键字规律）
- Java OOM
- LB 4xx/5xx错误统计
- CDN 错误统计
- . . .

业务数据监控

■ 实时业务数据的监控是最重要的！

- 服务器down 了没关系
- App down 了没关系
- 在赚钱就行！

■ 介于运营统计和运维监控之间

- 模糊地带

自动化运维

SACC

2012中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2012

架构设计 · 自动化运维 · 云计算

运维自动化

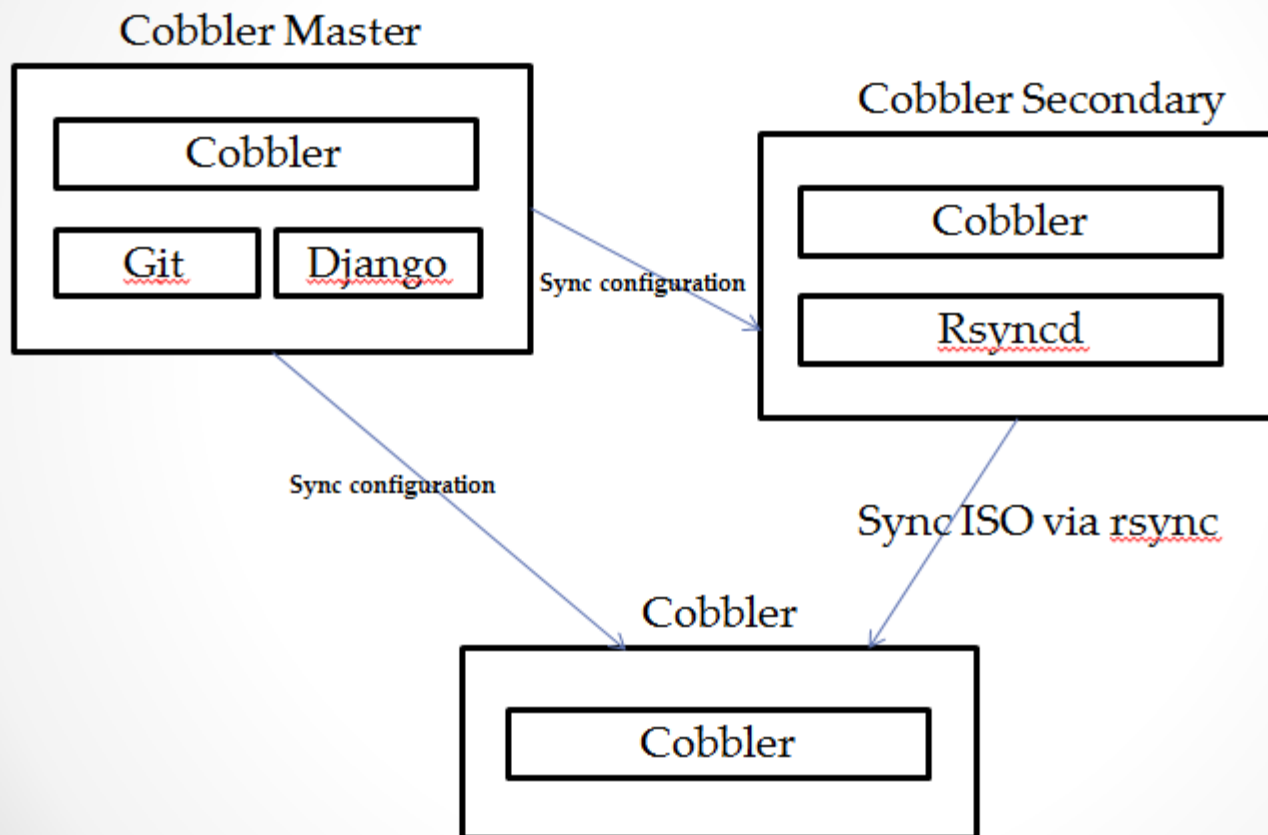
- 统一标准的基础上才能实现自动化
- 自动化才能保证标准化
- 自动化：
 - 应用标准，系统标准，减少诡异问题
 - 大大节约人力:减少对工程师个人经验的依赖
 - 大大提高响应速度: **4小时**减少到**5分钟**

自动化

- 全网装机自动化(CDN/核心网)
- Puppet 保证:应用配置与环境统一 (90%以上)
- Web应用部署90%自动化
- CDN应用100%自动化(Puppet+ControlTier)
- 上包自动化(p2p, 多终端,Client)
- 监控自动化
 - 上线自动添加基础监控
 - 下线, 维护自动暂停/删除监控
- 排错自动化 –简单排错

CDN机房自动化装机

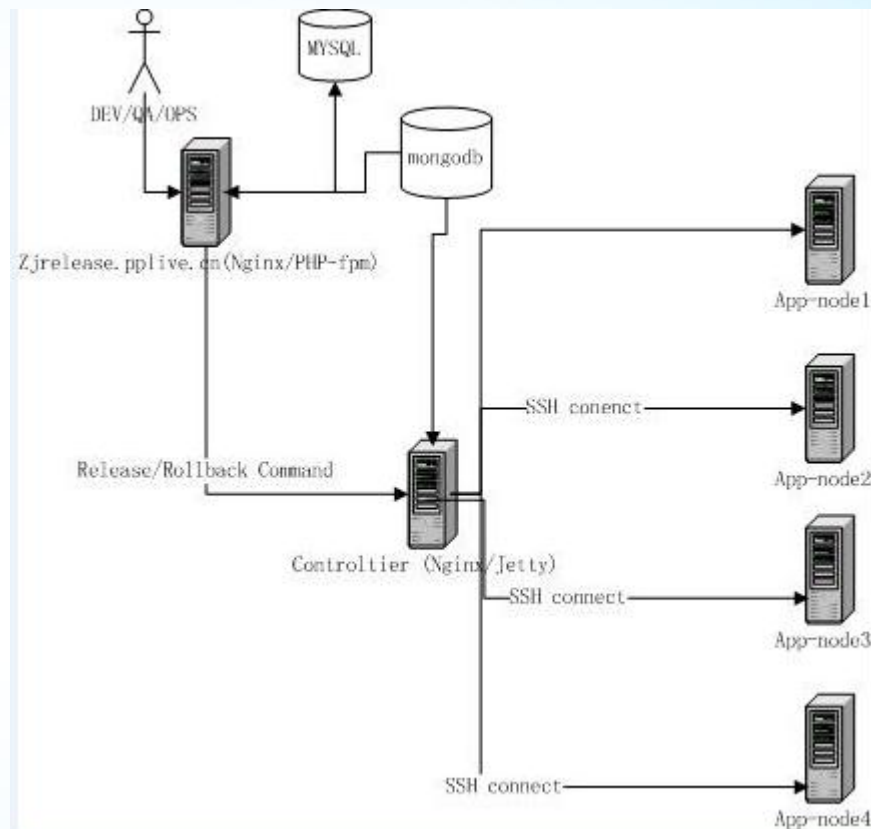
■ ControlTier + Git + Cobbler



一键发布

■ PHP + ControlTier

- 逐个发布
- 与cmdb集成
- 与Zabbix/URLmon集成
- CAS认证
- 借助LB日志分析
- 一键回滚



自动化排错

■ Zabbix Rule Engine

- 适应删除日志
- 自动重启:php/Resin
- 告警邮件自动分析
- 自动Java thread dump
- ...

http code by each backend server

```
1 "10.204.101.111:8080" "-"
3 "10.204.101.112:8080" "-"
328 "10.204.101.112:8080" "404"
342 "10.204.101.111:8080" "404"
```

http code by URL:

```
8 Code: 404 URL: /%b2%bd%b2%bd%be%aa%d0%c4(%b5%da32%bc%af).mp4 Refer: "-"
8 Code: 404 URL: /%b2%bd%b2%bd%be%aa%d0%c4(%b5%da33%bc%af).mp4 Refer: "-"
8 Code: 404 URL: /%b2%bd%b2%bd%be%aa%d0%c4(%b5%da34%bc%af).mp4 Refer: "-"
8 Code: 404 URL: /%b2%bd%b2%bd%be%aa%d0%c4(%b5%da35%bc%af).mp4 Refer: "-"
8 Code: 404 URL: /%c9%f1%d6%ae%cd%ed%b2%cd(%b5%da17%bc%af).mp4 Refer: "-"
8 Code: 404 URL: /%c9%f1%d6%ae%cd%ed%b2%cd(%b5%da18%bc%af).mp4 Refer: "-"
8 Code: 404 URL: /%c9%f1%d6%ae%cd%ed%b2%cd(%b5%da30%bc%af).mp4 Refer: "-"
8 Code: 404 URL: /%c9%f1%d6%ae%cd%ed%b2%cd(%b5%da31%bc%af).mp4 Refer: "-"
8 Code: 404 URL: /%c9%f1%d6%ae%cd%ed%b2%cd(%b5%da32%bc%af).mp4 Refer: "-"
12 Code: 404 URL: /%5Bmobile%5D%BC%E0%D3%FC%B7%E7%D4%C6.mp4dt?type=aphone Refer: "-"
```

http code by Server Name:

```
1 Code: 499 Server Name: [REDACTED]
3 Code: 499 Server Name: [REDACTED]
30 Code: 404 Server Name: [REDACTED]
640 Code: 404 Server Name: [REDACTED]
```

http code by Client IP:

```
2 Code: 404 Client IP: [REDACTED]
2 Code: 404 Client IP: [REDACTED]
```

数据化运维

-----监控和日志数据的分析

SACC

2012中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2012

架构设计 · 自动化运维 · 云计算

数据化运维

- 监控 → 告警
 - 告警阈值的制定
- 日志分析
 - 服务域名可用性
 - CDN命中率，性能，流量，
 - Top-down 分析
- 容量分析和优化
 - 提前发现问题
- 结合CMDB
 - 机器究竟都在干嘛？数据！

监控告警优化

- Top alerts by domain, category, technology
- Top reasons
- Review weekly, action
- Avg act-fix time;
- Problem Management
 - By team
 - By Tech
 - By function

WebCDN优化

- CDN 总体吞吐量？连接？单机QPS？Hit ratio？流量？High/low？瓶颈？
- 用户来自哪里？是否有合适的用户覆盖？
- 智能解析是否最优？低速用户来自哪里？
- CDN各类服务命中率如何？各类服务响应时间如何？
- CDN 对与用户响应时间，源站响应时间？
- CDN top 资源利用率 (by domain/referrer),
- CDN top picture ? Avg size?
- 什么服务应该CDN，什么服务不应该CDN？
- Top 出错率：机器，URL，ErrorCode，Service

VOD CDN 数据分析

- 整个播放Chain上面的各个服务：
 - 请求数
 - 成功率
 - 平均响应时间
 - 数据展现。。。
- 各个维度的QoS数据
 - 机房级别的带宽利用率
 - 机器的带宽利用率，平均下载时间
 - 机器级别错误率
 - 按照地域的卡顿率
 - 按照App的平均卡顿率，下载速度，vv，
 - 按照码流

容量分析和预警

- When will my application fail?
 - 知道应用/系统可能瓶颈
 - 收集Metrics
 - Reporting/Alerting
- Canary program
- Right sizing

关于网站架构

SACC

2012中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2012

架构设计 · 自动化运维 · 云计算

按照数据流提炼网站通用基础架构

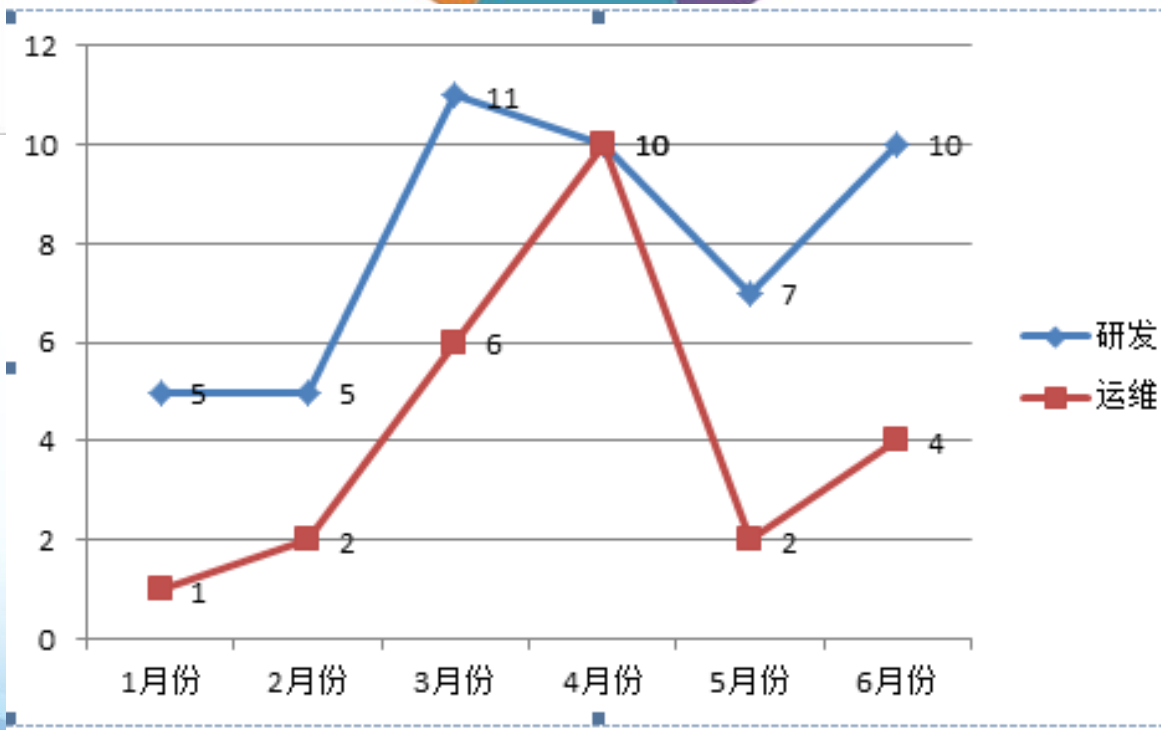
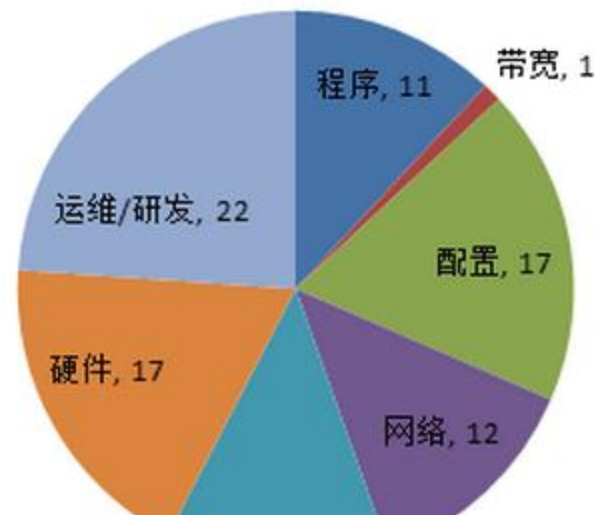
- 系统稳定性取决于应用架构
 - Dev 了解 IDC Strategy
 - Ops了解 App 数据流
- Ops总结几个数据流的Pattern，归纳几个通用解决方案
 - 简化
 - 服务话
 - 消除单点
 - Scalable service

架构优化

- 推动应用架构简化
 - More tiers, more tears
- 通过事故推动研发优化/简化架构
 - 不然没有人鸟你
- 每一层有高可用方案，每一层可以扩展
 - 尤其是数据库层面
 - 每一个组件高可用

流程

- 变更管理流程
- Incident Report
- 成本Report



文档与分享

- 文档化很重要
 - 知识的传承, 自我总结
 - 团队内部的知识分享
- 文档化了：
 - 主要系统网络拓扑
 - 主要技术决策背景原因利弊分析
 - 所有主要项目的设计，拓扑
 - 所有主要项目的事故总结
- 业内技术交流
 - 参加公开技术交流
 - 私下运维同行的交流

SACC

2012中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2012

架构设计 · 自动化运维 · 云计算

About DevOps

- 知道IDC布局
- 知道IDC 策略
- 知道基本硬件平台
- 可以看到服务器状态，性能指标，看到日志
- Should Dev has production access?
- Platform for Dev/Ops
- Dev should understand the environment their code runs on
- Ops should understand the Dev code/logic

2012

Monitoring

Windows平台的集中配置管理和监控

实时业务数据监控

网络质量/安全监控

运维日志监控/分析平台

BI日志收集平台

运维资源平台/CMDB

Automation

资源使用分析和容量优化

应用Release自动化

核心网交换机高可用和千兆互联解
决

内部DNS

VM 管理平台

排错分析自动化

Application

应用标准化

Layered Service

Redis/Mongo/Hadoop

应用安全

攻击报警系统

2012中国系统架构师大会

SYSTEM ARCHITECT CONFERENCE CHINA 2012

架构设计 · 自动化运维 · 云计算