SACC
2010系统架构师大会

基于大规模集群的运维架构设计

张旭 阿里巴巴云计算

阿里巴巴云计算
Alibaba Cloud Computing

阿里巴巴集团研发院
Alibaba Group Research & Development

目录

- 我们面临到的情况
- 我们运维的几个基本思路
- 闭环的运维体系
  - 资源分析环节
  - 资产管理环节
  - 集群部署环节（系统部署和应用部署）
  - 运维的支撑系统
    - DNS管理系统
    - roleDB（角色系统）
    - 账户系统
    - 配置管理
    - ACLPUSH系统
  - 监控环节

我们面临到的情况

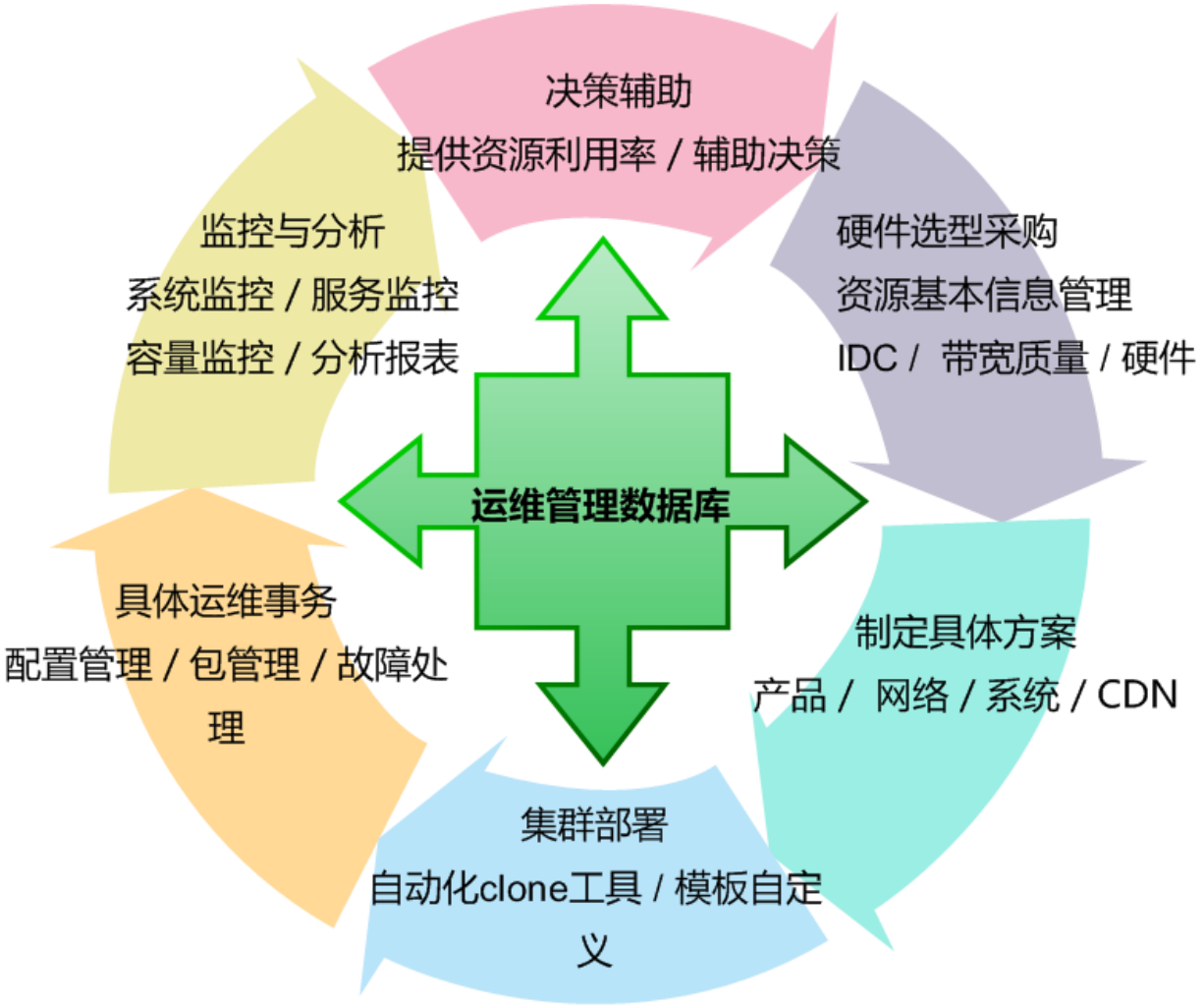
- 迅速增长的设备数量，几千，几万，几十万，……
- 种类繁多的设备类型
- 分布在全国各地的IDC，乃至全球
- 繁琐的日常变更，突发事件处理
- 设备的配置管理
- 系统监控/服务监控
- 产品部门各式各样的需求
- 决策层需要我们提供各类资源的使用情况
- ……

我们运维的几个基本思想

- 服务至上
  - 外部，全网用户
  - 内部，产品经理/工程师，财务/供保，决策层
- “寄生”于产品
- 流程、工具、人
- 尽可能传承下去，不要轻易“推倒重来”
- 闭环的运维体系
- 使用统一易读语言，有命名委员会
- 对资源敏感
- “懒”，自动化，不复杂，
- 沟通，分享

闭环的运维体系

- 核心：
  - 管理流程
  - 统一数据
  - 确认owner



资源分析

- 资源的现状
  - 资源的投入
    - 负载、存储、带宽利用率，端口使用、Hits，等资源数据
    - 资源的分布情况
  - 资源的产出
    - PV、活跃用户、等业务指标
  - 资源优化方案
    - 产品层面优化，系统层面优化，削峰平谷
- 决策支持
  - 根据模型，得出预测
  - 不要让老板拍脑袋

资产管理

- 资产
  - 硬件且精细：交换机，服务器，防火墙，机架等硬件
  - 硬件只计数：硬盘等备件，交换机模块等
  - 虚拟资产：虚拟服务器，IP、域名资源
- 管理策略
  - 全集团范围内的统一编号和命名
  - 对所有资产字段确定owner
  - 工具：财务信息，硬件信息，连接关系、IP-域名，clone信息校验，等
  - 变更流程cover资产的变更
  - 审计：自动/人工审计，采盘/全盘
  - 接口：WEB，CLI，API

尽可能——提供cli和api

- 除了web方式之外的接口
  - Web方式，很通用
  - Api 接口，很常见，供系统调用
  - Command Line 工具，很方便，为运维人员提供方便的查询接口
- 权限控制
  - Web，Api，较灵活的授权方式
  - Cli，按主机（IP）授权

```
Example:
  ./opsdb -l -p AY22 -o mip,p,g
  ./opsdb -l -i 10.251.32.[1-255] -o ip,p,model --sep ~_~
  ./opsdb -l -s [1-9]7wym2x -o a,sn,mip,clone,site,p
  ./opsdb -l -r %_admin% -o mip,p,r
  ./opsdb -l --date 2010-12-21 -o site,date,hwinfo

  ./opsdb -l -v --parent r%yh.aliyun.com -o ip,parent,r
  ./opsdb -l --vm -i 10.249.89.10[5-7] -o ip,status,clone,date
  ./opsdb -l --site yh -o ip,r -v
  ./opsdb -l -r AY%_kfc -o p,g,r --vm

  ./opsdb -t ay -c
  ./opsdb -t p,ay% --count
  ./opsdb -t p -c | grep '^AY'
  ./opsdb -t gnode -c
  ./opsdb -t rvm -c
  ./opsdb -t r,%_pangu_chunkserver% -c
  ./opsdb -t netC -c
  ./opsdb -t netCvm -c
  ./opsdb -t expire,2010%
  ./opsdb -t model -c
  ./opsdb -t company -c
  ./opsdb -t site -c
  ./opsdb -d -i 10.249.32.15

xu.zhangxu@h05-vm02 ~/opsdb/venus/cli $ ./opsdb -l --vm -i 10.249.89.10[5-7] -o ip,status,clone,date,os,site
r03e05029-vm1.yh.aliyun.com  10.249.89.105   active  clone  YH  2010-07-13
r03e05029-vm2.yh.aliyun.com  10.249.89.106   active  clone  YH  2010-07-13
r03e05029-vm3.yh.aliyun.com  10.249.89.107   active  clone  YH  2010-07-13

xu.zhangxu@h05-vm02 ~/opsdb/venus/cli $
```

集群部署——系统环节

- 半自动的部署工具
  - 界定人工干预的范畴，MAC地址异常，等
- 部署前的准备
  - 审批通过
  - 需要部署的集群和服务器，模板
- 具体部署
  - 每个IDC都有相应的部署环境
- 后续工作
  - 处理异常
  - 更新配置
- 重点：模板抽象和管理

尽可能——使用nfs

- 将home目录挂在到nfs上
  - 省去用户经常性的copy，低碳
  - 便于管理，.vimrc .bashrc
- 如果可能，将系统目录也可以使用nfs
  - 非常方便管理
  - 可以省去一块系统盘
  - 缺点，前期规划复杂，将一些log目录拆出

集群部署——应用

- 定义和区分不同的应用
- 不同的应用调用不同的部署模板
- 半自动的部署过程
- 部署完成后修改相关信息

尽可能——使用主机名

- 应用相对固定，IP总是增减变化
- 一目了然
  - webcache.news.zjm.bj.aliyun-inc.com
  - pop3.mail.zjm.bj.aliyun-inc.com
  - logs.zjm.bj.aliyun-inc.com
- 通过子域区分设备相关属性
  - 服务模块，应用，机房，公司
  - 很方便，可以很多地方减轻工作量

DNS管理系统

- 统一的DNS管理平台
  - 内部和外部的DNS
  - 子域的管理，zone
  - 记录的管理，record
- 和其他系统联动
  - 部署系统
  - 资产管理系统
- 权限管理
  - 按子域授权
- 支持多种接口
  - WEB，CLI，API

roleDB系统（角色管理）

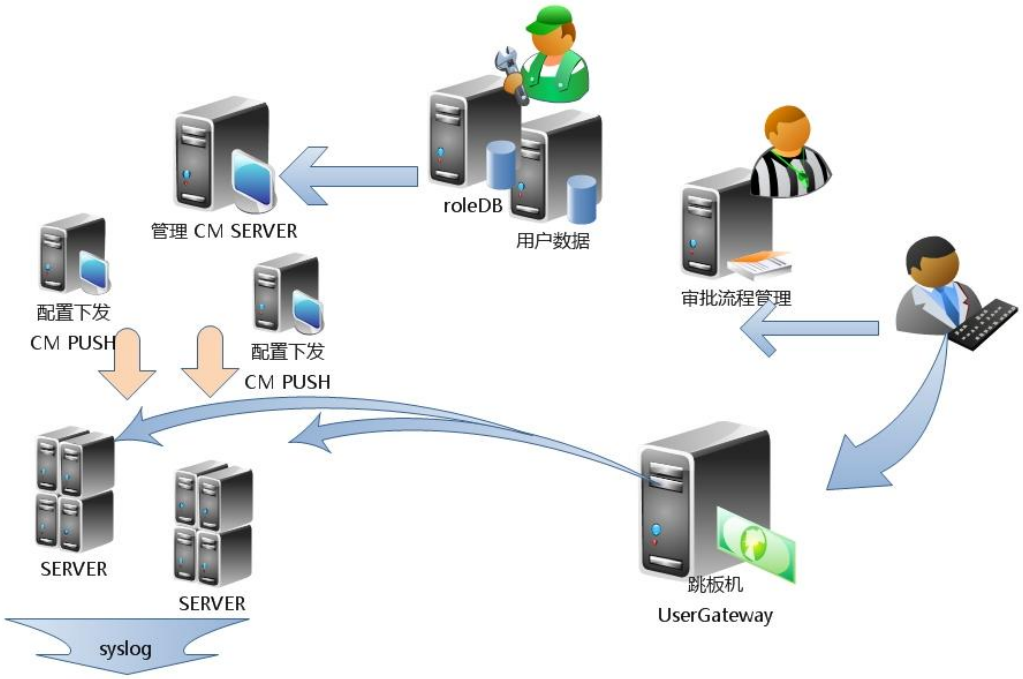
- 角色管理的内容
  - 分组
  - 服务器，人员，产品
- 管理策略
  - 新增，删除，较为严格的控制，（命名委员会）
  - 变更，可授权给相应其他系统
  - 每个角色都有owner
  - 设备、用户可属于多个角色
  - 继承性
  - 域名方式的管理
- 多种接口，WEB，CLI，API

账户管理

- 分类
  - 个人帐号
    - 用于登录，员工邮箱前缀
    - UID就是公司统一分配的员工编号
  - 系统帐号
    - 用于启动服务器，不容许登录
    - 每个系统帐号都有owner
- 统一的登录入口
- 用户操作信息记录
  - 入口统一记录
  - 每台服务器单独记录，实时提交到日志系统中

账户管理架构图

- 账户管理架构图



配置管理

- 运维的核心是配置管理，配置管理的核心是文件管理
  - 将正确的文件放到正确的位置赋予正确的权限【以正确用户的执行】
- 配置管理重要的几点
  - 角色分组信息，服务器、帐号、文件
  - 解决冲突
  - 推送工具
    - Cfengine，Puppet（服务器），
    - ACLPUSH系统（交换机/服务器）
  - 快照、历史记录
- 接口 WEB，CLI，API

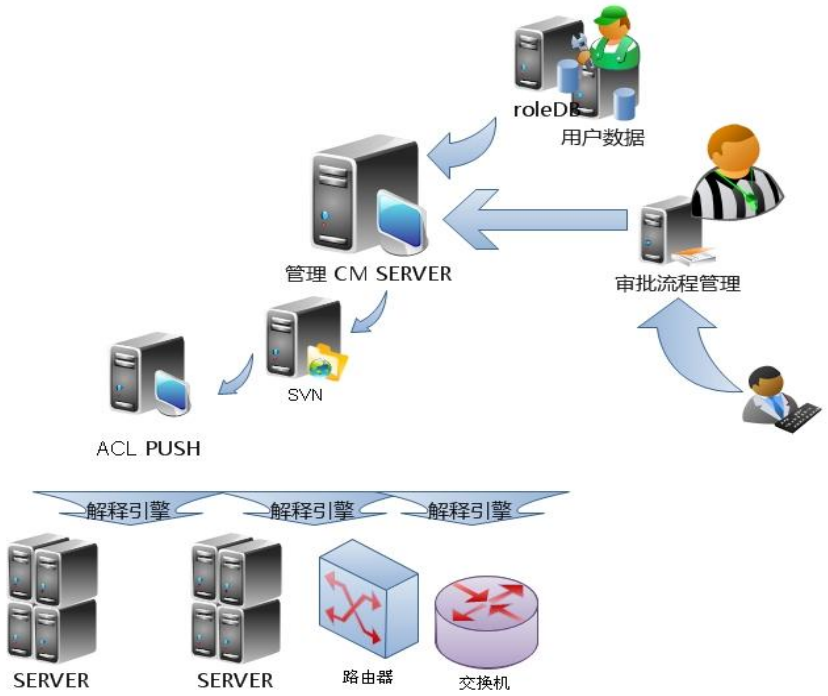
ACLPUSH系统

- 特殊的配置管理
  - 多种策略的解释引擎
    - 不同交换机，Cisco3550，FORCE10 S50， 交换机语法
    - 不同操作系统，iptables，Linux, FreeBSD
- 结合其他系统
  - 角色分组信息，交换机，服务器
  - 解决冲突
  - 快照，历史记录
  - 版本保存在SVN，日志保存在DB
- 支持多种接口，WEB，CLI，API

```
usage: ./aclcmd.pl: command [args ...]
commands and arguments:
   agents     Check all agents' status
   commit     Commit all changes to version control.
              options:
                 --pretend   Don't commit, just show working repo's changes.
   dist       [COLO | pushdir/COLO.index ...]   Distribute specified COLO's acl files and index to ag
fferent COLOS.
   dumpindex [pushdir/COLO.index]   Dump file index content for debug purpose.
   gen        [options]   Process all files in policy directory and generate acl configs.
              options:
                 --debug   Don't push generated acl into pushdir, just print internal object on scree
                 --all   Do not skip those unchanged acl config
   help       Print this help
   plugins    List all device plugins
   push       [COLO | pushdir/COLO.index ...]   Push out acl file in specified COLO (after "dist" is
              options:
                       --status   Don't do push, just query remote push status and wait for complete
   update     Update all dir from version control.
```

ACLPUSH架构图

- ACLPUSH架构图



监控环节

- 监控分类
  - 系统监控，单机，系统层面，设备层面，
  - 服务监控，集群，CDN层面，用户感受，用户新闻，服务质量，行业排名
  - 容量监控，产品，业务指标，资源利用率，投入是否合理
- 监控工具
  - 系统监控，agent，snmp
  - 服务监控
    - 终端用户模拟
    - 服务器log分析
    - 页面中的分析脚本（谨慎）
  - 容量监控
    - 结合财务信息，
    - 业务数据进行综合比较
    - 需要建立分析模型

尽可能——使用热备服务器

- 对于单机故障，让系统自动替换热备设备
  - 以前是磁盘常用，现在是服务器
  - 当服务器出故障的时候，自动将热备（buffer）替换上去
  - 将应用归纳，可自动化的、重复性故障处理过程用工具处理
  - 目前基本每周集中修理一次故障机器即可
- 需要资源，合理规划成本

其他运维相关系统

- Syslog系统，负责采集，聚合，分析syslog信息
  - 服务器系统log，应用log，交换机log
- 日志分析系统
  - 根据模型分析所有收集到的日志
- IPDB，负责管理IP网段的相关信息
  - 网段的管理，IP的管理
- 包管理，负责管理服务器的安装包
  - 统计某个包在那些服务器上安装、分析、接口
- 事件/变更，审批/处理 平台
  - 流程管理
- 运维知识库，Wiki分享平台
- ……

谢谢大家！

Q & A

旺旺：aladdinzhang（阿里巴巴中国站）

邮箱：aladdin.zhang@gmail.com

电话：13911550077