



GOPS2017
Shanghai



GOPS

全球运维大会

2017

上海站

指导单位:  信息中心联盟
SHANGHAI CENTER FOR INFORMATION TECHNOLOGY

主办单位:  信息技术协会
SHANGHAI INFORMATION TECHNOLOGY ASSOCIATION

 数据中心联盟
SHANGHAI DATA CENTER ALLIANCE

大会时间: 2017年11月17日-18日

大会地点: 上海光大会展中心国际大酒店 (上海徐汇区漕宝路67号)



证券行业DevOps第1步：IT资源自动化管理

国信证券 张浩水

目录

➔ **1** 国信证券及讲师介绍

2 行业特点及挑战

3 投奔DevOps怀抱

4 平台的建设成果

5 成功经验和总结

国信证券介绍



About me



NAME: 张浩水

工作单位: 国信证券



2008, 中科院自动化研究所毕业



2008到2015年, 招商银行系统运维及基础设施运维



2015年至今, 国信证券运维架构师, 负责运维平台建设



目录

1 国信证券及讲师介绍

➔ 2 行业特点及挑战

3 投奔DevOps怀抱

4 平台的建设成果

5 成功经验和总结

1、稳态业务同质化，运维以ITSM体系为主

- 1. ITSM建设主要以纯流程管理为主，线上流程和线下手工操作脱节，运维效率低。
- 2.传统业务以GUI为主，自动化系统需要编写大量的界面事件脚本。
- 3.自动化能力建设无法复用。



国信证券 ITIL 运维服务流程平台

事件记录单

事件记录

工单编号:	事件来源:	事件发生日期:
影响范围:	紧急度:	优先级:
事件类型:	事件类型:	报告影响级别:
影响开始时间:	影响结束时间:	影响时长(时):
记录人: 张迪夫 06224	记录日期: 2017-07-07	请求人电话: 701737
联系人: 张迪夫 06224	联系人部门: 系统运行部	请求人名称: [Shanghai Securities Co., Ltd.]
事件分类:		记录时间:
事件标题:		
事件描述:		

事件处理

事件原因描述:

事件处理过程与解决步骤:

事件根本原因:

Copyright © 2017 国信证券股份有限公司

2.敏态业务持续业务创新，运维产能滞后业务发展

IT规模

- 证券创新、Fintech推动运维也要同步创新。
- 纯流程手工式运维严重滞后于今天行业发展的需要。
- 运维的压力日益加重，创新业务带来IT基础设施、应用与服务的指数级增长。

```

584 root      23      0 4128 260 494 0 0.0 0:00.00 /sbin/mingetty --chuspup /dev/tty3
585 root      23      0 4128 260 494 0 0.0 0:00.00 /sbin/mingetty --chuspup /dev/tty4
2210 saasops    23      0 584m 15m 1984 0 0.0 1:26.34 ssh client
2289 saasops    23      0 502m 137k 1892 0 0.0 0:00.02 /bin/db_./bin/sysofd safe --default-file=/etc/my.conf --name=saasops --mode=force-recovery1
2594 saasops    23      0 1700m 160m 2282 0 0.0 0:48.83 /usr/local/saasops/psysql/bin/psysql --default-file=/etc/my.conf --name=/usr/local/saasops/psysql --data
2897 saasops    23      0 233m 22m 1572 0 0.0 0:00.52 /usr/local/saasops/python/bin/python ./auto_detect_mail.py
3005 saasops    23      0 234m 22m 1580 0 0.0 0:00.15 /usr/local/saasops/python/bin/python ./auto_detect_mail.py
3256 saasops    23      0 235m 22m 1586 0 0.0 0:00.35 /usr/local/saasops/python/bin/python ./auto_detect_mail.py
3307 saasops    23      0 234m 22m 1512 0 0.0 0:00.37 /usr/local/saasops/python/bin/python ./auto_detect_mail.py

[root@develop_3 ~]# ?
[root@develop_3 ~]# ?
[root@develop_3 ~]# ls
cpgroup.py  monitor-bondkit.py  saasops  varsites  www.monitor  install.sh  java_tools  code-wt.3.3-linear-ssl.tar.gz  as  stop_monitor.sh  test_mail  t_log  zachwei_mail
[root@develop_3 ~]# ./stop_monitor.sh
monitor
2017-11-01 09:32:57,244 - INFO - start to stop
2017-11-01 09:32:58,581 - INFO - stop_script result code: 0 out: ok
monitor_mail.py: no process killed

###
2017-11-01 09:32:58,484 - INFO - stop end, start to check process
2017-11-01 09:34:00,214 - INFO - monitor_script result code: 1 out: ok
FIN FIN          TIME OK

###
2017-11-01 09:34:00,241 - INFO - check end,update status
2017-11-01 09:34:00,243 - INFO - stop successfully
###real:successcode=0###
alert_channel
2017-11-01 09:34:00,633 - INFO - start to stop
2017-11-01 09:34:00,178 - INFO - stop_script result code: 0 out: ok
alert_channel_mail.py: no process killed
alert_channel_mail.py: no process killed

###
2017-11-01 09:34:00,178 - INFO - stop end, start to check process
2017-11-01 09:34:00,782 - INFO - monitor_script result code: 1 out: ok

```

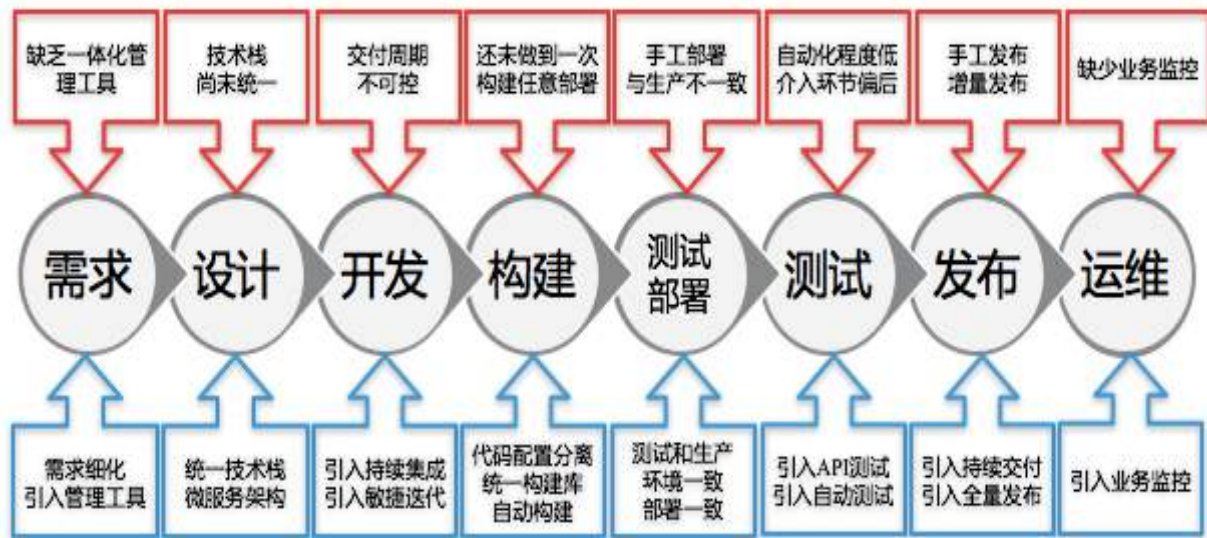

3.IT资源增长迅速，传统CMDB不足以支撑运维体系构建

- 基础资源数据依赖Excel表格维护，运动式人工管理。
- 数据中心过去以基础设施资源管理为主，忽视了上层应用的管理能力。
- 资源维护自动发现能力严重匮乏，维护成本高、效率低。
- 运维系统规划和建设碎片，没有以CMDB为基础构建。

固资卡片						
基本信息	其他信息	财务信息	历史使用情况	维修记录	编辑记录	关联申请单
购置类型:	公司购置	资产状态:	在役			
资产来源:	购建	资产用途:	管理用			
资产类型:	电子设备/电脑主机/服务器	类型编号:	003001			
资产名称:	服务器	购入价:				
增值税税率:		不含税价:				
税金:		设备序列号:	D8XFDB2			
品牌名称:	DELL	购买日期:	2016-03-01			
品牌型号:	R730XD	启用日期:	2016-03-02			
主要配置:	2*E5-2698V3/256G/26*300G(2.5"SAS 15K,)/2G Raid卡 /企业级远程管理卡/4*板载intel千兆网卡/增配 1块Inte I350 QP (四口) 1GB 网卡/; DVD光驱; 导轨; 冗余电源; 4年原厂服务 7*24*4; 保留硬盘;		所属部门:	信息技术总部系统运行部		
供应商编号:	00127	使用部门:	信息技术总部系统运行部			
供应商名称:	戴尔(中国)有限公司	责任人:	张浩水 06224			
供应商地址:		使用人:				
资产图片:	暂无附件!	存放地点:	信息技术总部系统运行部			

4. 技术债务多，缺乏端到端高效IT价值流

- 缺乏面向DevOps端到端IT流程，交付流动效率低下。
- 整个IT标准化、持续交付过程规范、工具能力建设、系统架构、组织协作、监控体系等能力需要全面的建设和提升。



目录

1 国信证券及讲师介绍

2 行业特点及挑战

➔ 3 投奔DevOps怀抱

4 平台的建设成果

5 成功经验和总结

DevOps的IT自动化本质——两层交付

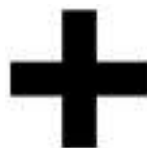


角色：各类运维角色，网络、存储、服务器等等

场景：运维各类自动化、配置、变更等

能力：
面向资源层的自动化能力，包括IaaS和PaaS层自动化

产品：云管理平台CMP



角色：Dev、Test、Ops

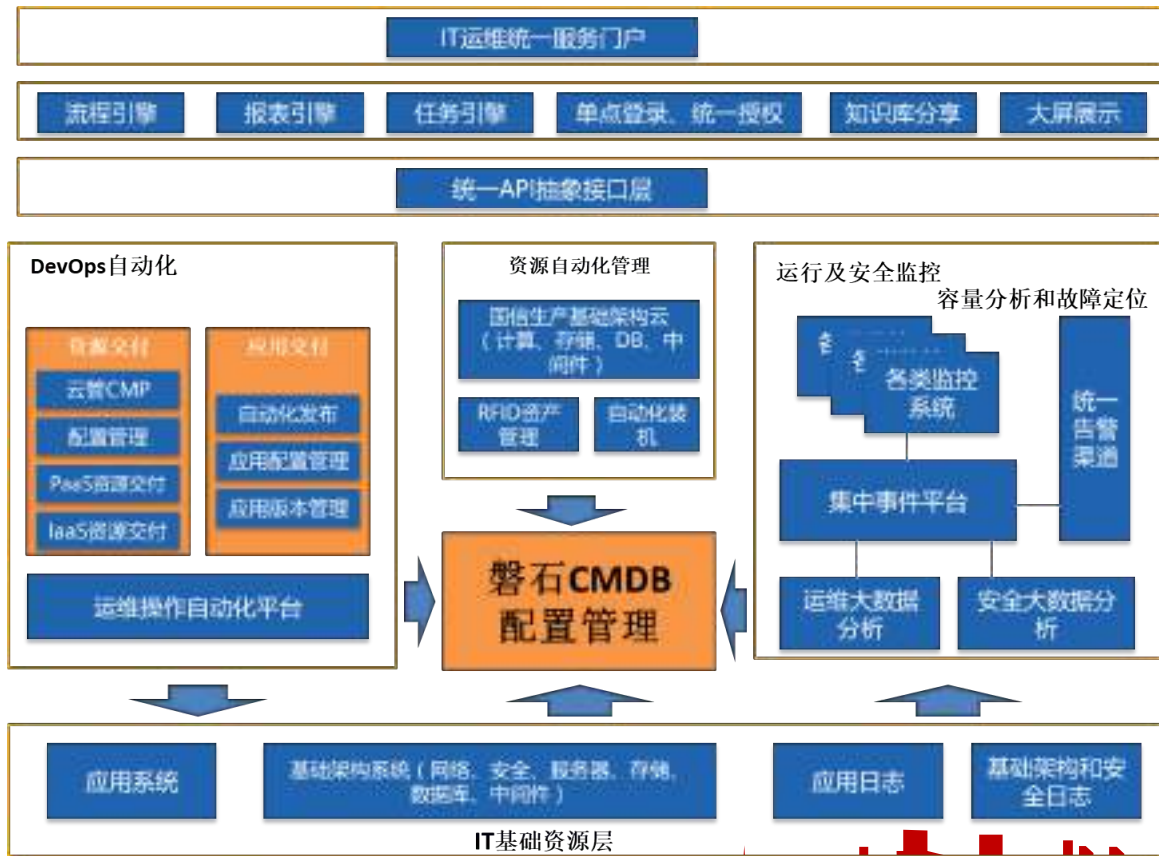
场景：持续部署、配置管理、灰度发布、端到端交付

能力：面向应用的自动化能力，包括持续交付的自动化和运营维护过程自动化

产品：DevOps平台

基于磐石CMDB的DevOps运维平台整体架构图

- 以CMDB为核心基础平台，打通自动化、监控、安全等各种运维平台的能力。在自动化平台部分，打通资源交付和应用交付的自动化能力。
- 国信第一阶段以CMDB为基础，建设统一事件平台、运维大数据平台、混合云管平台、自动化装机平台和运行监控系统，加强数据消费场景。



基于磐石的国信DevOps三步走策略

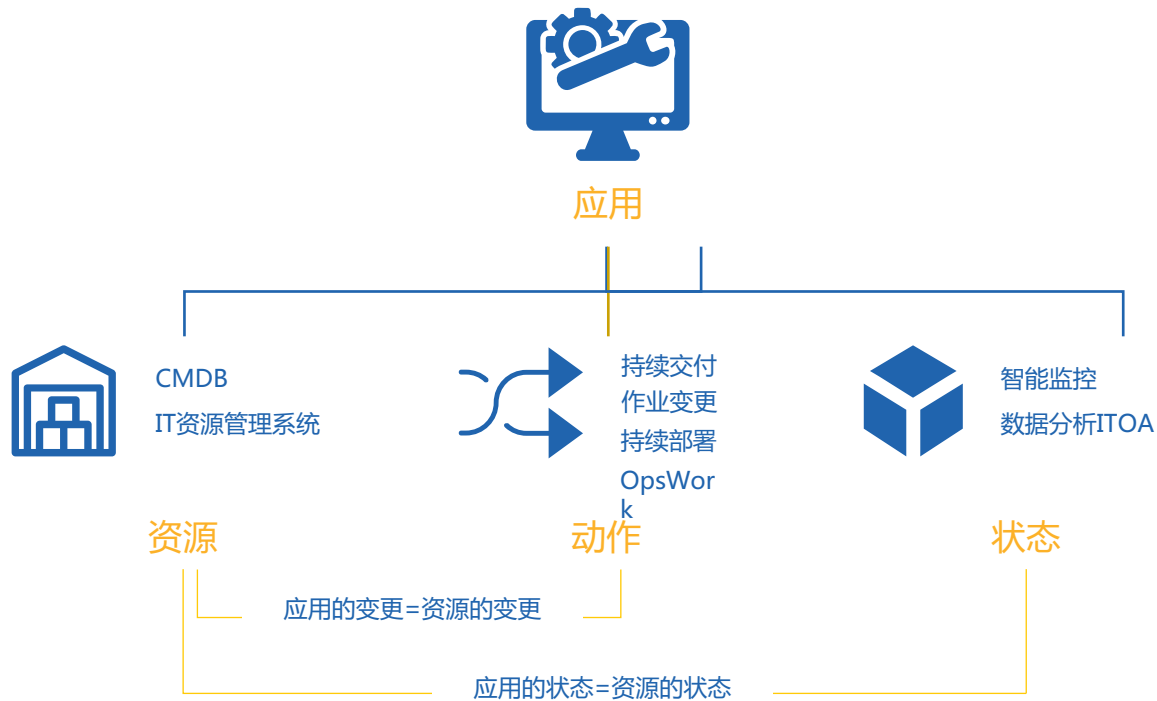


第一步：IT资源自动化管理（磐石系统）

建设目标：

- 解决资源人工管理的问题
- 提升资源交付的效率
- 支持各种差异化的物理和逻辑资源，实现统一管理
- 透明资源的使用信息，提高资源利用率和运行可靠性
- 实现资源管理能力服务化（持续交付的资源服务支持）
- 构建可视化的资源自动管理能力（流程驱动、集中分析、智能调度）

磐石系统的核心设计理念——以应用为中心



- **应用管理**：应用的生命周期管理，是其资源、动作和状态管理的抽象。
- **IT资源管理**：面向应用的IT资源管理，实现全局并分层的资源地图，为各个场景提供数据支撑。
- **动作、状态**：结合应用的管理需求，应用的变更是通过各种场景化动作来完成的，状态的变化是通过对应用的全面监控来完成的。

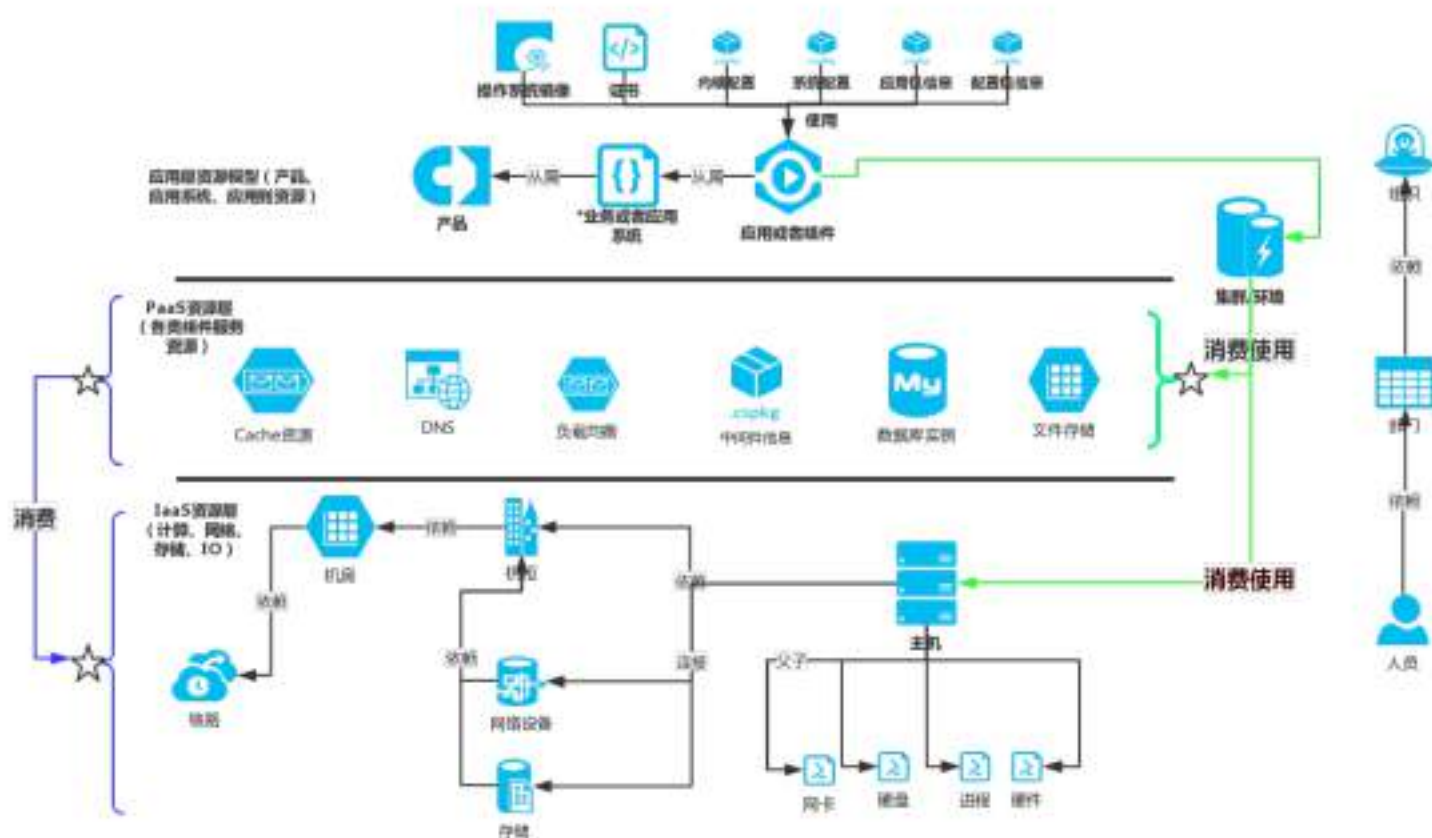
磐石系统之基础CMDB建设五原则

- 1 面向IaaS和PaaS设计，能够管理底层的一切资源
- 2 状态控制借助运维流程自动化完成
- 3 CI的维护要深度使用自动发现，而不是人工维护
- 4 资源信息必须能为上层应用提供服务
- 5 必须满足基础资源的CI管理需要

磐石系统之应用CMDB建设七原则

- 1 → 提供统一的应用元数据管理能力，和应用类型无关
- 2 → 核心诉求是应用生命周期管理
- 3 → 以应用为中心，而非以基础资源为中心
- 4 → 从应用的角度构建起与IT资源的弹性关系
- 5 → 为应用资源、动作、状态的统一管理提供支撑
- 6 → 以统一的基础资源层CMDB作为基础
- 7 → 核心场景就是持续交付

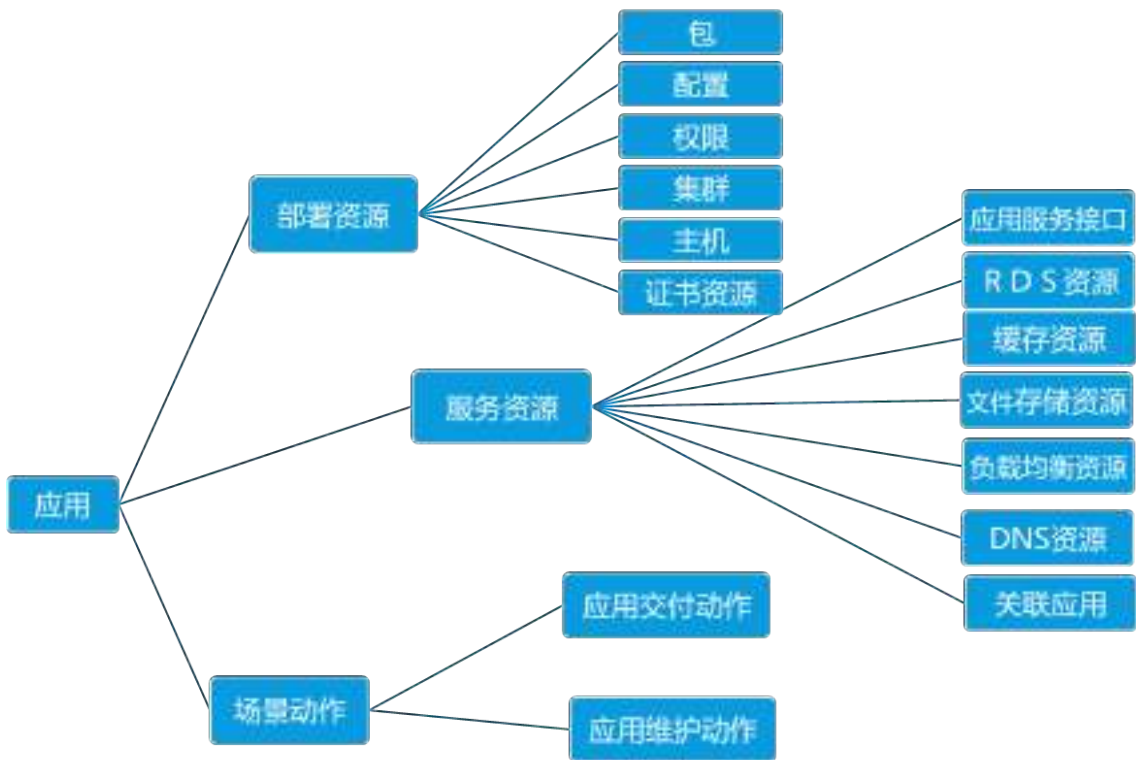
磐石系统的资源模型框架



IaaS层、PaaS层提供面向应用的资源支撑

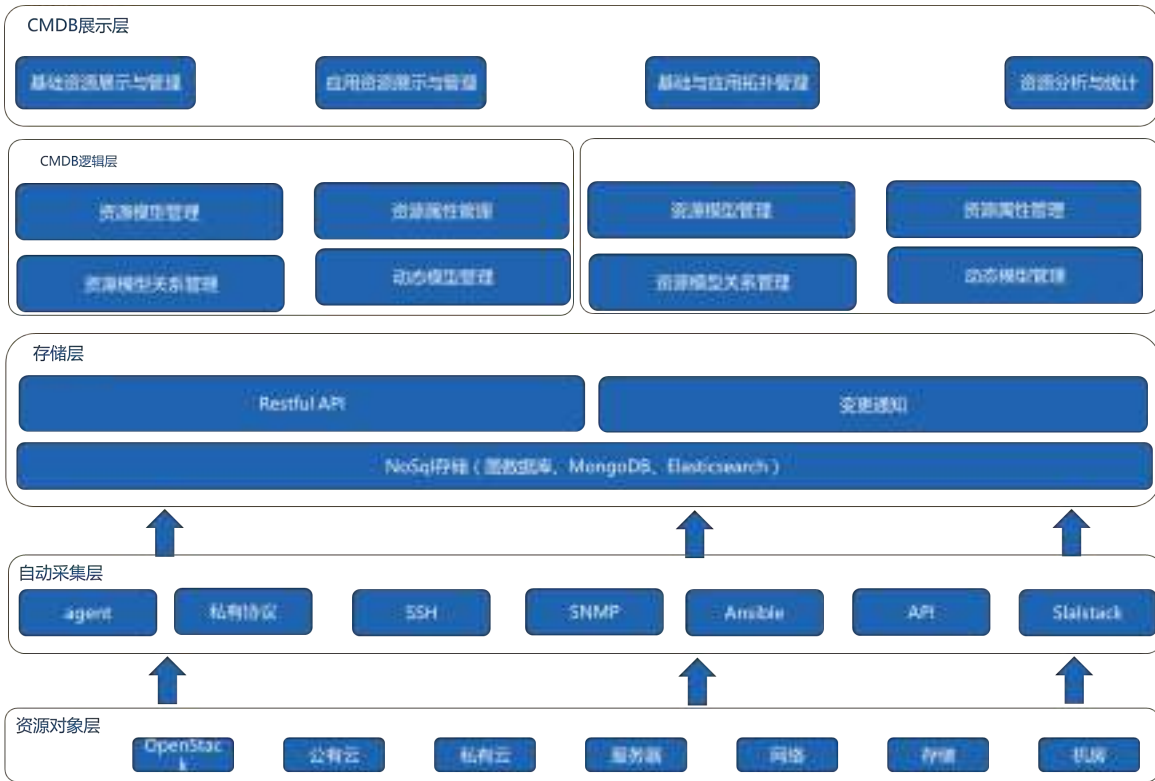
应用强关联各类资源的信息，比如说基础设施资源、外部服务资源以及本地部署资源等。

磐石系统的资源层次模型分解



- 应用CMDB是面向资源的完整描述，应用的资源分成应用的部署资源、服务资源和动作资源。
- 部署资源是一次应用部署所依赖的资源，一般又称本地资源，比如说主机Host、程序包等等
- 服务资源是应用运行依赖的资源，一般称之为附加资源（来自于12factor），比如说应用的服务接口、应用依赖的PaaS资源、应用依赖的应用资源等等。
- 场景动作是资源其上附加的动作描述，是资源的管理方法。

磐石系统的技术架构



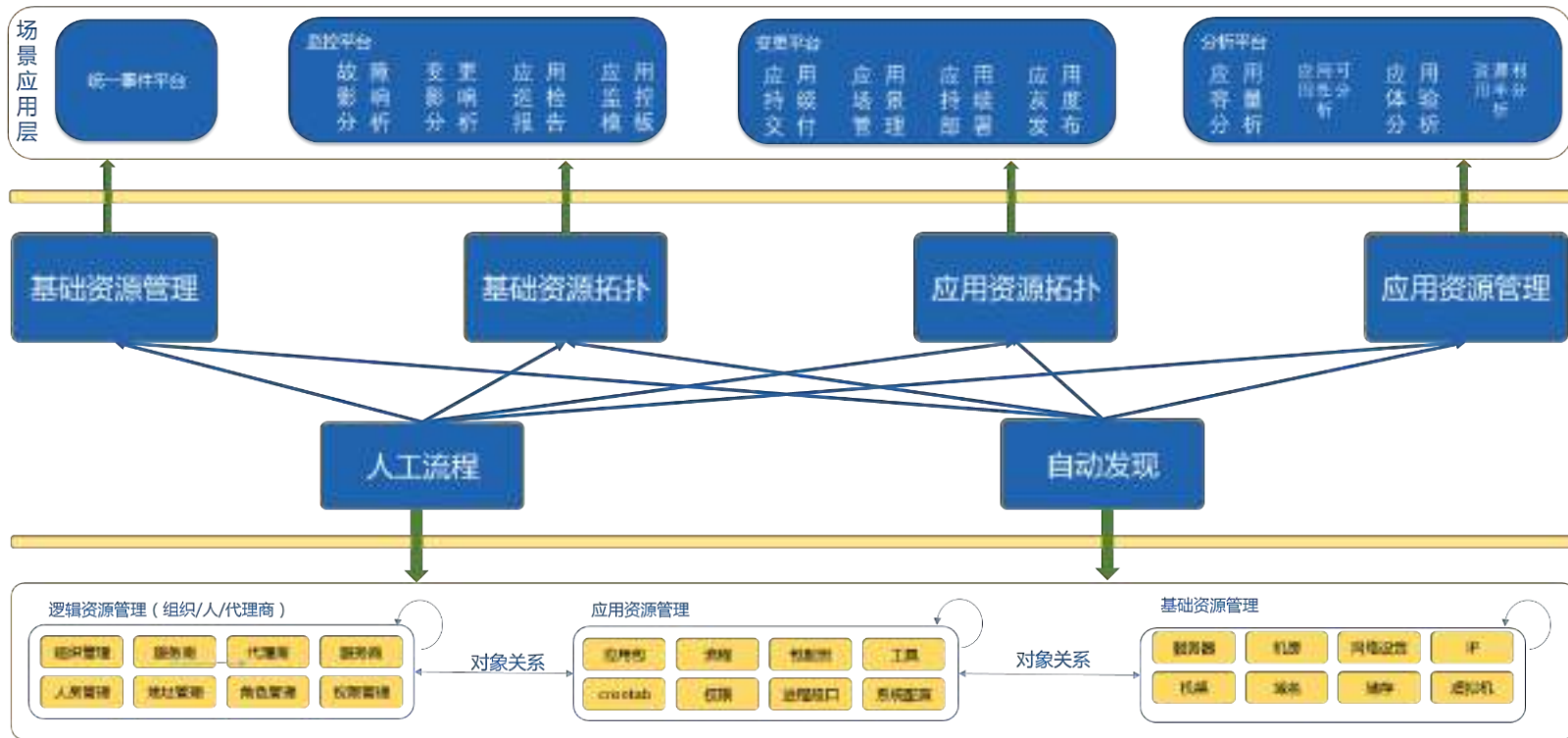
- 自动采集层。支持多种通道的数据采集能力
- 对象存储系统。NoSql与图式数据存储能力，确保数据模型的动态扩展性。
- RestFul API接口。提供IT资源数据的入库能力，同时也确保上层的资源消费能力。
- CMDB展示层。提供面向用户的CMDB管理能力：模型管理、资源管理等等能力。

磐石系统的功能框架



- 资源模型管理主要为定义配置模型，包括配置项、属性、关联关系。
- CI对象管理分成基础设施对象管理、PaaS对象管理及应用的管理等。
- 拓扑的管理是CI对象之间的关联关系管理，从架构拓扑、部署拓扑到基础架构拓扑是一个分层的拓扑Overlay。
- 对于实例和关系的维护有两个重要的手段，一个是自动发现，另外一个就是基于运维流程的生命周期管理与场景化的自动化变更管理等等。

基于磐石系统的场景化规划



磐石系统的落地实施框架

现状评估

- 资源状况
- 流程架构
- 技术架构
- 组织架构

CMDB项目启动

- CMDB项目启动会
- CI模型及关系整理
- CMDB场景整理
- CI模型数据来源方式整理
- 确定CI维护Owner及其管理流程

CMDB数据实例化

- 搭建CMDB测试环境和生产环境
- 导入CI模型
- 编写自动发现程序生成数据
- CI数据实例化人工生成

CMDB数据校验

- 检查CMDB数据导入情况
- Owner确认数据的准确性
- 导入生产环境

数据场景消费

- IT资源管理流程构建
- 周边运维平台与CMDB平台对接（如IT事件平台、日志分析平台）
- 自动化运维平台与CMDB平台对接
- 持续交付平台与CMDB平台对接

磐石平台建设过程

- 2016年5月启动平台建设，项目成员10人
- 2016年9月完成CMDB平台建设和自动采集脚本的开发
- 2016年10月CMDB平台上线试运行
- 2016年12月完成流程平台开发，并启用物理机上架流程
- 2017年1月东莞新数据中心上线，第一个100%对接IT资源管理平台的数据中心
- 2017年4月启动持续集成与持续交付项目，预计18年3月前上线

目录

1 国信证券及讲师介绍

2 行业特点及挑战

3 投奔DevOps怀抱

➔ 4 平台的建设成果

5 成功经验和总结

平台技术特点1：从资产到资源的管理升级

一切IT都是资源，把资源的管理边界确定下来，进一步给CMDB瘦身，确保CMDB成功。

- IaaS层是面向基础设施的资源
- PaaS层是平台服务资源
- 最终的目的是面向应用管理所有资源



主机管理 + 添加主机 批量编辑 更多操作 -

发现主机冲突，最近是否有机器搬迁或本地重装等情况发生？[请解决冲突。](#)

搜索 按属性、IP、负责人等搜索 克隆匹配 高级搜索 - 显示详细信息

<input type="checkbox"/>	主机名	IP	运维负责人	内存大小	CPU型号	操作系统的发行版本	Agent状态	最近访问
<input type="checkbox"/>	alienwind01	192.168.100.90		125.7 GB	Intel(R) Xeon...	CentOS 6.9 FI...	离线	11小时前
<input type="checkbox"/>	1.1.1.1	1.1.1.1					未安装	
<input type="checkbox"/>	auto_test_hos...	127.0.0.1					未安装	
<input type="checkbox"/>	auto_test_hos...	127.0.0.1					未安装	
<input type="checkbox"/>	auto_test_hos...	127.0.0.1					未安装	
<input type="checkbox"/>	auto_test_hos...	192.168.10.10					未安装	
<input type="checkbox"/>	auto_test_hos...	192.168.10.10					未安装	
<input type="checkbox"/>	auto_test_hos...	192.168.10.10					未安装	
<input type="checkbox"/>	BJ-C00100	192.168.101.1					未安装	
<input type="checkbox"/>	BJ-C00101	192.168.101.2					未安装	

平台技术特点2：动态资源模型，秒级完成。



GOPS2017
Shanghai

任何CI及其属性的调整都可以在秒级之内完成，而这样的调整无需在二次研发的前提下完成，实现用户自助式的能力管理。

- 完全自助式的模型自建和属性任意扩展能力
- 模型即建/即调即所得



平台技术特点3：配置信息自动发现。

从网络、存储到上层应用，提供全面的自动发现能力，降低维护成本

服务器自动发现

- Agent采集资源信息自动录入
- 多协议支持
- 外部API服务的自发现支持

信息自动更新

- 资源信息驱动系统变更
- 变更后信息实时反馈更新

个性化信息采集

- 支持采集插件的扩展
- Agent实现统一插件调度



The screenshot displays the '自动发现' (Automatic Discovery) section of the IT Resource Management system. The left sidebar contains navigation options: IT资源管理, 概览, 业务管理, 应用管理, 基础资源, 基础配置, 模型管理, 模型统计, 自动发现 (highlighted), 基础管理, and 用户管理. The main content area shows a list of discovery rules:

规则名称	最近五次发现状态	最近一次发现时间
规则：网络设备自动发现 所属资源：第十次网发	● ● ● ● ●	2017年7月6日 19:00
规则：存储EMC自动发现 所属资源：lightTestObject	● ● ● ● ●	2017年8月22日 00:52
规则：存储HDS自动发现 所属资源：测试测试	● ● ● ● ●	2017年8月22日 00:52
规则：全网IP自动扫描 所属资源：测试小火车	● ● ● ● ●	2017年7月6日 19:00
规则：FS自动发现 所属资源：lightTestObject	● ● ● ● ●	2017年7月6日 19:00
规则：执行一下沙箱工具 所属资源：应用	● ● ● ● ●	2017年7月6日 19:00

平台技术特点4：面向应用的资源管理画像

构建全面的应用管理画像，从底层的资源到上层的应用配置信息，全面覆盖，建立以应用管理视角的强驱动模式，确保CMDB真正的落地成功

❖ 应用资源的理解

本地资源，支持应用运行的本地资源，比如说服务器、进程、端口等等。

远程资源，支持应用运行的第三方资源，比如说缓存、存储等等。

❖ 应用管理画像

应用画像=应用信息+应用资源信息+应用拓扑信息+应用变更动作。



The screenshot displays the 'APP_cmdb' application management interface. The main content area features a central dashboard with a hexagonal diagram and several data cards. The hexagonal diagram is surrounded by six modules: '基本优势' (Basic Advantages), '配置管理' (Configuration Management), '应用管理' (Application Management), '拓扑管理' (Topology Management), '性能管理' (Performance Management), and '外部依赖' (External Dependencies). Below the diagram are three data cards: '设备管理' (Device Management) showing 2 servers and 2 hosts; '人员信息' (Personnel Information) listing 'jeason2' as the administrator, developer, and tester; and '资源信息' (Resource Information) showing 0 instances for various resources like '程序包' (Packages), '数据库' (Databases), '中间件' (Middleware), '缓存' (Cache), and '文件库' (File Storage).

磐石系统技术特点总结

❖ 全开放式API接口，Restful风格

CMDB的开放才能让数据被全面消费，才能让CMDB数据鲜活性得到保障。

❖ 全开源技术栈、NoSql和图数据库存储

开放式的底层技术设计，新一代的存储选型，让CMDB的实施成本大大降低，可以快速满足新的需求实现，甚至自助式的完成业务需求的开发。

❖ 与流程平台/变更/监控平台的深度集成

“任何资源及服务”的业务要求下，加上开放式API的设计，确保了资源真正的能被全面的消费，有来自于流程平台的消费、有变更场景的消费，有状态监控平台的消费。

❖ 微服务架构

运维平台微服务化，让后续的升级、维护等可以低成本的进行，确保CMDB模块可以动态扩展架构。

❖ 应用资源的柔性管理能力

每个应用需要管理的资源不同，管理能力需要柔性化，自动化，精确应用的资源管理画像。

基于磐石的IT资源自动化管理建设成果

资源模型

三层简化结构：



资源项 **43**

属性 **750**

流程制度


5 维护动作

录入、修改、删除、人工
变更、自动发现

34 个关联流程

4 个关联系统

系统建设

 即搜即得

100% 自动采集



标准化实时接口



与流程对应的
维护权限控制

业务系统 覆盖

业务系统 **全覆盖**

组件 **近千个**

实例信息

核心资产信息：

- 机房
- 机柜
- 网络
- 存储
- 主机
- IP
- 应用
- 服务

目录

1 国信证券及讲师介绍

2 行业特点及挑战

3 投奔DevOps怀抱

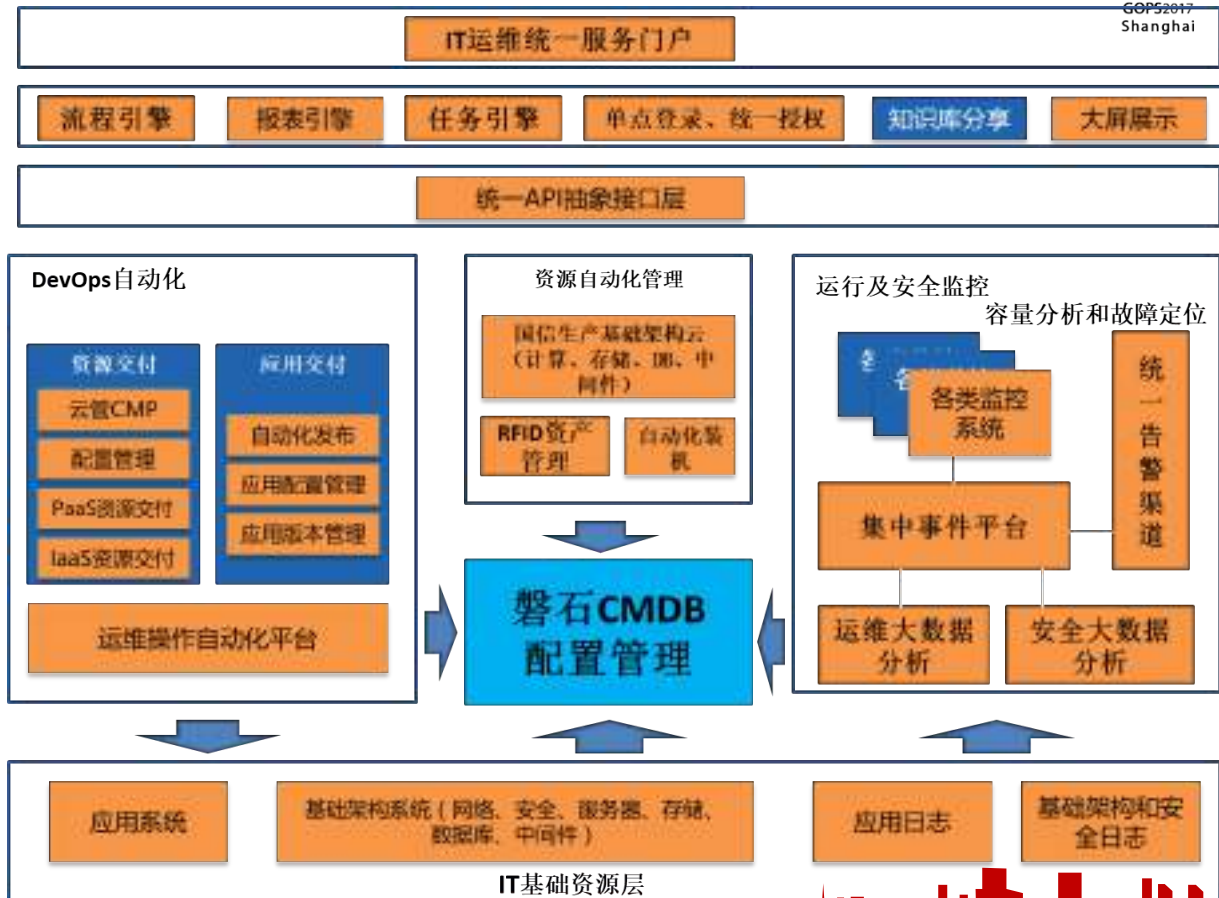
4 平台的建设成果

➔ 5 总结

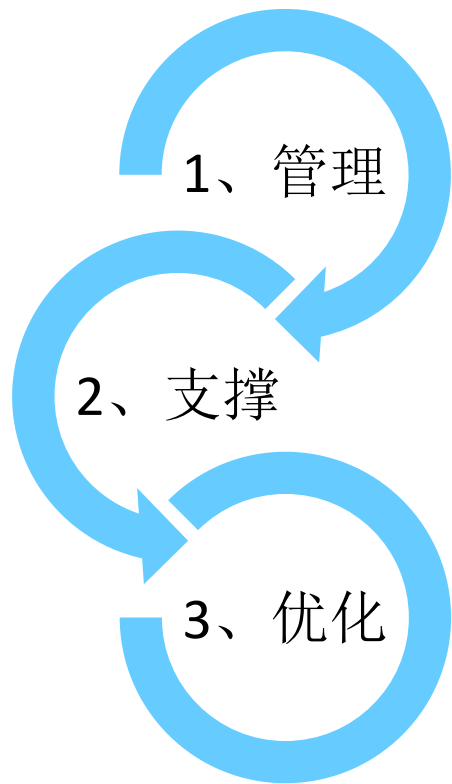
国信基于磐石的DevOps运维管理平台建设情况

建设已完成

- 磐石CMDB在国信全面落地，包括自动发现、应用组件管理等等。
- 资源交付自动化平台初步建设完成，基本实现了资源交付自动化（一键上线主机），应用部署自动化（持续部署）目前正在建设中。
- 整个运维管理平台以磐石CMDB为核心，通过磐石的数据全面开放能力，驱动周边所有平台与其集成，



国信基于磐石的DevOps运维管理平台建设成果



- 管理

- 集中管理所有的资源及其资源的拓扑关系，实现**资源全生命周期管理**；通过**自动化发现技术结合运维变更流程**，有效降低资源维护成本。

- 支撑

- 作为元数据平台，给周边平台提供数据支撑，第一阶段就与集中事件平台、运维大数据平台、混合云管平台、自动化装机平台等集成，周边平台场景消费，确保CMDB数据的准确性和鲜活性。

- 优化

- 基于CMDB实现了IT变更服务流程能力再造，把流程和自动化做了结合；
- 基于应用CMDB，实现了多环境的自动化部署，提升变更能力。

国信DevOps运维管理平台实施经验分享

01

领导支持且参与
自上而下的推动支持

02

理念与意识先行
社区、培训、咨询三位一体

03

以CMDB为基础
其他平台与其关联建设

04

持续交付
打造端到端IT效能提升

05

核心痛点优先
自动化解决效率和成本的痛点

06

运维大数据
精细化运营，数据驱动

磐石CMDB系统创新总结

自动化采集+外围工具平台提供为主
流程自动化为辅



01



复杂业务访问关系拓扑图的动态展示

02

以应用为中心的资源管理全视图

04

以CMDB为核心的运维生态圈

03



国信证券诚聘英才

- 运维开发岗/互联网应用运维岗
 - 老板好
 - 待遇优
 - 假期多
 - 不熬夜
 - 不背锅
 - 团队氛围融洽





Thanks

高效运维社区
开放运维联盟

荣誉出品



想第一时间看到
高效运维社区公众号
的好文章吗？

请打开高效运维社区公众号，点击右上角小人，如右侧所示设置就好

