

金融行业自动化运维的研究与落地

红帽解决方案架构师 魏新宇



目录



IT大咖说
知识分享平台

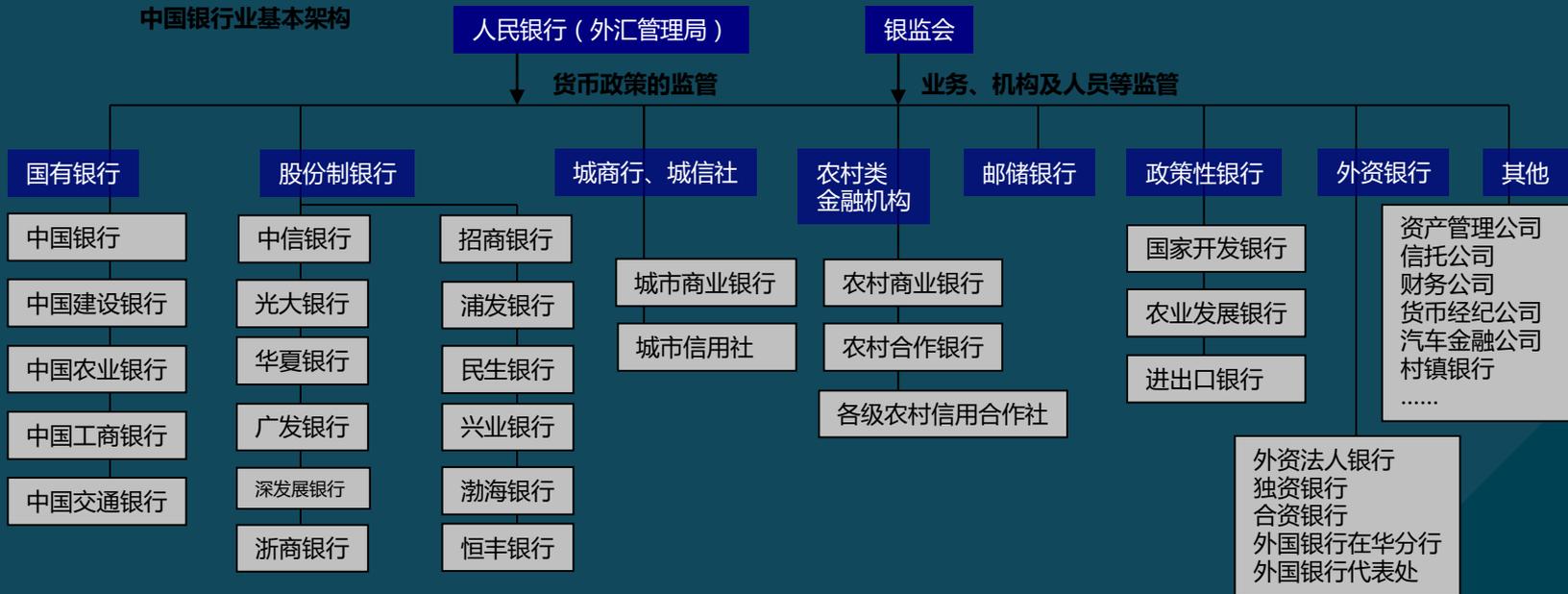
- 金融行业IT运维的现状
- 金融行业IT运维的出路
- 红帽自动化运维解决方案
- 金融行业IT自动化运维实现之旅

金融行业定义



- 中国金融行业自1993年起实施分业经营，金融业主要包括银行、保险、证券三大子行业，多年来随着一行三会监管制度的建立、金融机构改革的稳步推进，中国金融体系架构初步形成。
- 银行业是中国金融行业的主体，受中国人民银行、银监会的双重监管。央行主要负责货币政策的制定，而银监会则负责银行业金融机构及其业务活动的监督管理和行政审批。
- 中国银行业主要包括国有银行、邮政储蓄银行、政策性银行、股份制银行、城市商业银行、城市信用社、农村信用社、农村商业银行、农村合作银行、外资银行及其他非银行类金融机构。

中国银行业基本架构



金融行业IT运维现状

金融行业IT运维现状

- 业务的稳定性、可靠性要求越来越高；
- 业务系统对IT支撑的依赖性越来越强；
- IT架构的复杂度不断加深；
- IT部门工作职责越来越重；
- 人员不足难以应对繁重的运维要求；
- IT事故将直接影响业务，责任重大。

过分依赖人工操作，效率低、风险大

- 操作的效率和准确性依赖于人员的技能；
- 操作周期较长并存在误操作的风险；
- 一旦业务中断，将带来巨大损失。

占用大量人力资源，成本偏高

- 不同的系统均由专人负责，运维人员的数量会随着信息系统的增加而不断增加。

将日常性、流程性的工作交由系统自动完成，以替代人工操作，增强业务运行的可靠性。

金融行业Linux运维管理方面典型问题



- **自动部署**

- 目前大多数金融采用各种开源技术实现了操作系统的批量安装和自动化部署、但是**先前的做法可重复利用化程度很低**，每当有项目需要进行自动部署时都需要针对该项目重新进行配置，**工作量大且效率低下而且没有很好的版本管理和回退机制**，也缺乏一个很好的管理界面来进行管理，希望通过有效的管理工具来实现快速部署海量服务器的问题。

- **软件更新**

- 目前金融客户服务器升级都是去红帽官方网站下载然后**手工进行升级操作**，**实效性、可追溯性差**，管理员只是被动接收来自安全部门和红帽的安全建议，希望通过一个集中展示平台，直观的看到行内所有linux服务器目前运行的软件版本和官方版本之间的差异、升级的类型并直接通过统一的展示界面远程直接对需要升级的服务器升级某一个软件的升级程序。

- **安全更新**

- 金融企业的安全部门以及公安部会定期对所有的Linux服务器进行安全扫描并发布安全整改意见，**这些意见和厂商提供的安全更新建议往往有很大的出入**，迫切的需要一个工具能提供Linux的安全更新以及修复建议并且能结合上述的软件更新功能为系统及时的修补安全漏洞

金融行业Linux运维管理方面典型问题

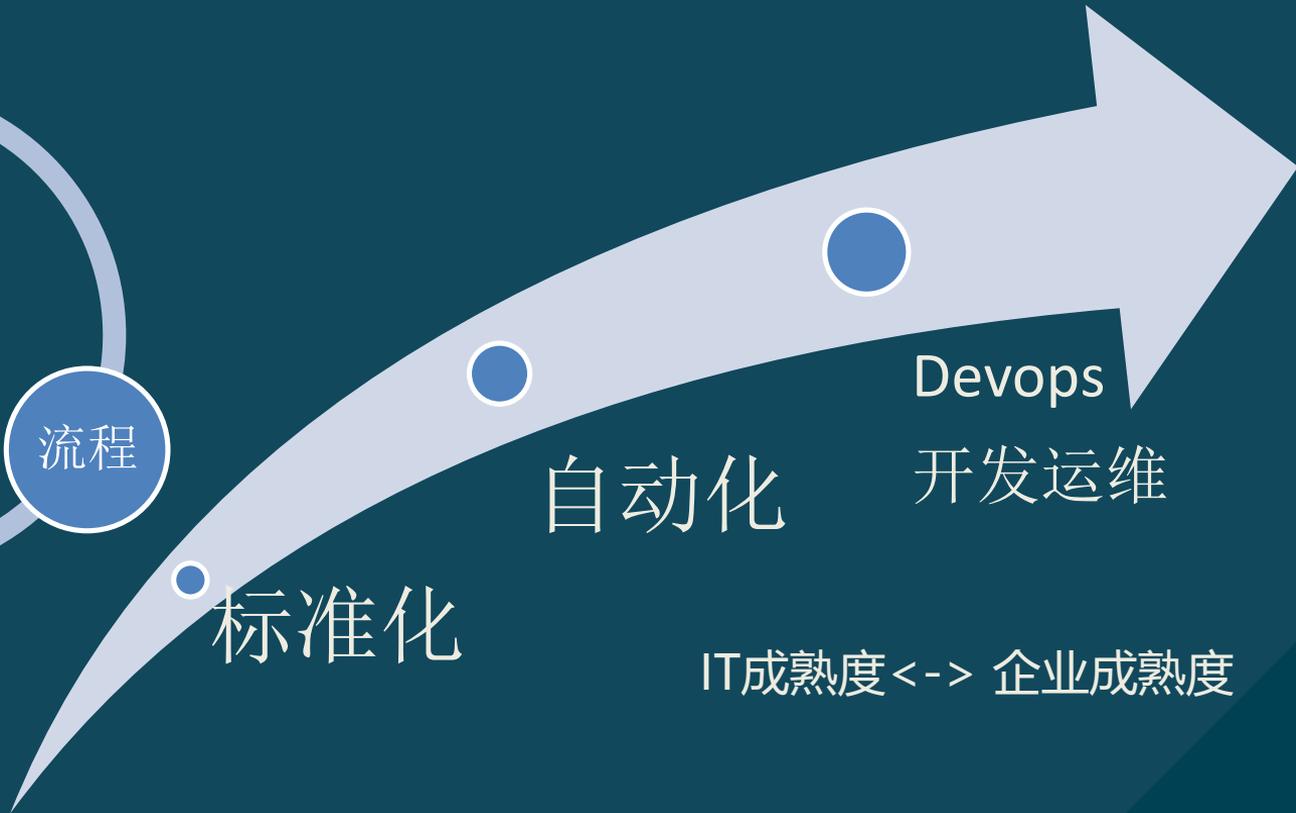
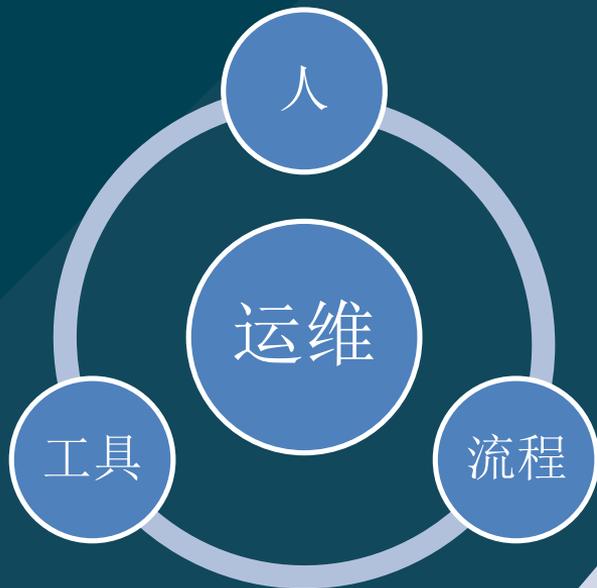


- **合规**
 - 金融行业内部的合规性标准需要人工来实现以及更，参与Linux运维的人员也很多，每个人的能力、对操作系统的理解程度以及使用习惯的不同会造成Linux服务器的配置存在很大的差异，通过一个集中式管理工具结合行里的运行规范来实现自动化部署并且可以根据已有古规范找出个与规范之间的差异并消除
- **软件生命周期管理**
 - 开发测试运维的环境的不一致导致开发测试环境中可用但到了生产环境会出现问题的风险，自动化工具来统筹管理开发、测试和运维平台上的Linux环境的部署，应用软件的分发以及合规性一致性的检测。
- **多用户、用户组管理以及访问控制**
 - 每个项目都会有相应的软件中心和数据中心的技术人员负责应用软件和操作系统的开发、部署、上线、维护等工作，为了完成这些工作需要给相应的用户赋予相应的权限以避免越权操作，希望解决在大规模Linux使用环境下用户管理和权限划分的问题。
- **服务器组批量操作**
 - 对于一个项目而言，通常几台甚至几十台服务器的配置和运行环境是完全一样的，希望能实现像操作一台服务器那样操作一组服务器，执行一次操作就可以对该组内所有服务器都生效，即对一组服务器可批量进行升级、部署、管理和维护的工作。

目录

- 金融行业IT运维的现状
- 金融行业IT运维的出路
- 红帽自动化运维解决方案
- 金融行业IT自动化运维实现之旅

解决诸多问题之路-运维标准化自动化



IT成熟度 <-> 企业成熟度

IT/OS运维成熟度



IT大咖说
知识分享平台

	Level 1 初级	Level 2 策略	Level 3 执行	Level 4 记录	Level 5 Devops
基础版本 CoreBuild	手动安装	文档标准	自动化安装	Corebuild版本管理	容器分层系统管理
补丁管理	无补丁	手动补丁	软件源, 订阅发布	集中, 定期版本管理	自动管理
配置	独立维护	文档 手工修改	批量脚本	配置管理控制, Git, SVN	自动配置, 自动发现
告警, 日志	无管理	有日志, 有性能统计, 手动检查	批量巡检	日志集中管理	自动修复 自动管理 自动告警
安全, 漏洞	无, 物理隔离	防火墙策略 安全配置	定期执行漏洞检查	安全集中管理	主动防御

IT成熟度 < - > 企业团队成熟度



金融行业理想自动化运维平台



IT大咖说
知识分享平台

合规管理人员

服务台人员



现场支持人员



专家组



系统管理员



领导



业务部门



合规管理人员



数据展示

统一展示平台

统计分析平台

服务管理

服务流程管理平台

服务台

- 事件管理
- 问题管理
- 知识库
- 变更管理
- 配置管理
- 值班管理
- 绩效管理
- 安全管理

基础架构管理

集中监控平台

- 应用层面
- 平台层面

运维自动化平台

- 作业调度
- 自动巡检
- 批量发布
- 容灾管理

内控平台

- 合规管理
- 风险管理
- 用户管理
- 访问控制

IT环境

- 设备
- 介质
- 软件
- 文档
- 操作
- 数据
- 流程
- 安全

目录

- 金融行业IT运维的现状
- 金融行业IT运维的出路
- 红帽自动化运维解决方案
- 金融行业IT自动化运维实现之旅



IT大咖说
知识分享平台

金融行业IT运维自动化运维的左膀右臂



IT大咖说
知识分享平台



左膀：自动化

RED HAT®
CLOUDFORMS

云管平台

RED HAT®
SATELLITE

右臂：标准化

ANSIBLE

AUTOMATE YOUR
I. T. PROCESSES & DEPLOYMENTS

Provisioning功能如下：

- 可在裸金属，虚拟化和基于云的环境中进行操作系统以及应用的部署
- 联邦式的内容分发
- 支持基于build以及基于镜像的部署
- 发现还未被部署的主机

订阅管理的功能如下：

- 集中的管理订阅使用
- 维护准确的库存和利用率的相关信息
- 按小组为单位的订阅消耗报告



软件管理的功能如下：

- 定义和管理标准的操作环境
- 针对安全漏洞（Heartbleed/shellshock）快速的相应
- 遵守组织内部的相关安全策略
- 部署所有红帽相关的基础设施以及第三方软件

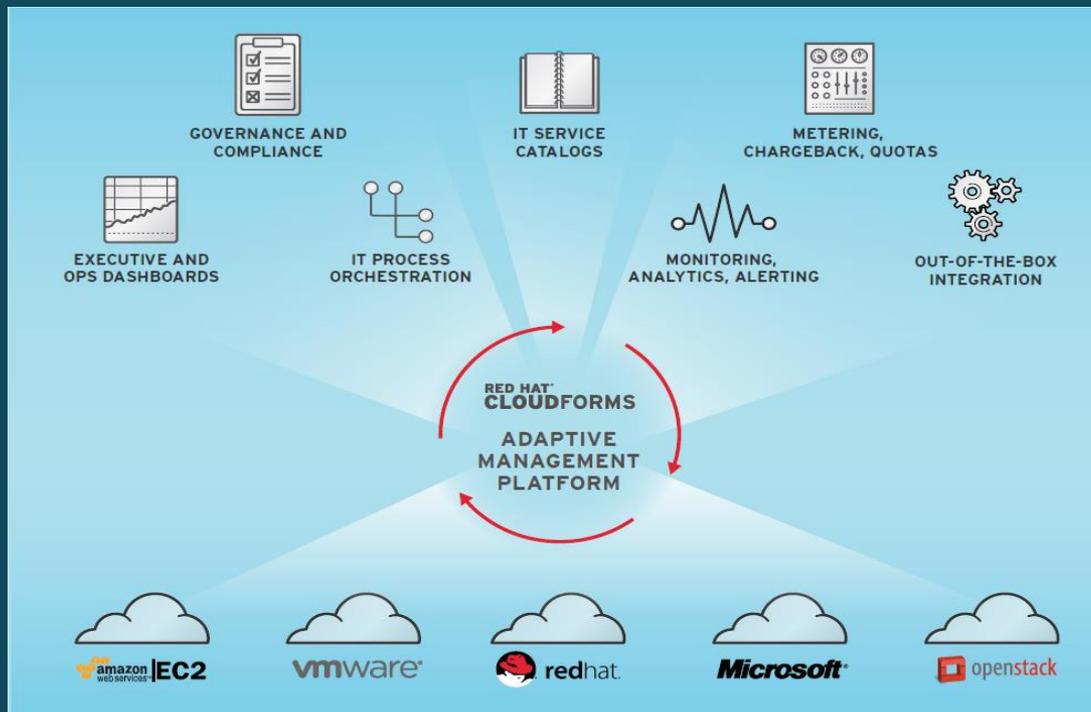
配置管理的功能如下：

- 定义系统所需的状态
- 管理和修复配置状态漂移
- 变更时的审核及报告

CLOUDFORM管理能力



IT大咖说
知识分享平台



目录

- 金融行业IT运维的现状
- 金融行业IT运维的出路
- 红帽自动化运维解决方案
- 金融行业IT自动化运维实现之旅



IT大咖说
知识分享平台

金融行业理想自动化运维平台的实现



IT大咖说
知识分享平台

服务台人员

现场支持人员

专家组

系统管理员

领导

业务部门

合规管理人员



数据展示

Cloudforms + UI定制化开发

析平台

服务管理

服务流程管理平台

Jboss BPM + ITIL + 专业服务

事件管理

问题管理

知识库

变更管理

配置管理

值班管理

绩效管理

安全管理

基础架构

集中监控平台

运维自动化平台

内控平台

Cloudforms+Zabbix + 专业服务

Ansible Tower + 专业服务

Satellite+专业服务

IT环境

设备

Redhat解决方案 + 其他软件厂商方案 + 硬件设备厂商方案 + 专业服务

安全

自动化运维管理平台应用场景



IT大咖说
知识分享平台

1、批量作业调度自动化

- 1、跨平台、跨作业段的**批量作业协同调度操作**。
- 2、作业执行结果实时巡检监控管理。

2、软件批量分发部署

- 1、建立**应用软件基线库**，实现部署软件版本的统一管理；
- 2、实现应用软件从分发、安装、运行的全过程自动化、智能化动态管理。

3、配置与版本管理

实现对生产应用配置文件，系统文件夹，重要数据文件的实时监控，实现对**关键文件的安全保护**。

4、自动巡检

通过定时或人工触发方式的自动调度执行。实现对管理设备、业务应用执行状态的**实时检查**。

5、应急故障检查

- 1、建立**应急分析模型**；
- 2、实现应急快速巡检，故障数据采样；
- 3、实现故障快速分析定位。

6、容灾管理

- 1、容灾切换流程批量自动执行，一键切换启动；
- 2、生产系统及容灾系统**一致性管理**；
- 3、容灾切换演习管理；容灾切换导航管理。

自动化运维实现步骤



运维自动化实现步骤	运维自动化实现内容	实现方式
标准运维操作自动化	批量作业自动化 + 自动巡检	Ansible Tower+专业服务实现
	软件批量分发部署+ 配置与版本管理	Ansible Tower + Satellite + 专业服务/其他开源工具实现
ITIL流程工具化	应急故障检查和容灾管理	Ansible Tower + Satellite + ITIL + BPM + 专业服务/其他开源工具实现
自动化运维平台化	构建自动化运维平台	Ansible Tower + Satellite + ITIL + BPM + CloudForms专业服务/其他开源工具实现

中国金融案例

云计算开源产业联盟
OpenSource Cloud Alliance for Industry/CloudIT大咖说
知识分享平台兴业银行
INDUSTRIAL BANK CO.,LTD.招商银行
CHINA MERCHANTS BANK深圳证券交易所
SHENZHEN
STOCK EXCHANGE上海證券交易所
SHANGHAI STOCK EXCHANGE交通銀行
BANK OF COMMUNICATIONS中國銀行
BANK OF CHINA中国建设银行
China Construction Bank上海清算所
SHANGHAI CLEARING HOUSE大新銀行
DahSingBank上海农村商业银行
Shanghai Rural Commercial Bank

广发银行|CGB

大连商品交易所
DALIAN COMMODITY EXCHANGE中国金融期货交易所
China Financial Futures Exchange

citibank



浙江农信



东莞农商银行



上海期貨交易所

Shanghai Futures Exchange

Standard Chartered

浙商银行
CHINA ZHESHANG BANK上海銀行
Bank of Shanghai广东华兴银行
GUANGDONG HUAXING BANK上海黃金交易所
SHANGHAI GOLD EXCHANGE

HSBC

中国平安 PINGAN
保險·銀行·投資广州銀行
BANK OF GUANGZHOU中国外汇交易中心
全国银行间同业拆借中心HKEx
香港交易所

谢谢!

