CCTC 2017 中国云计算技术大会
Cloud Computing Technology Conference 2017

CSDN

走出堡垒，恒丰银行金融云转型实践

刘骁

2017. 5


速度与激情8
4月14日

- 科技投入：约百万-百亿/年
- 建设方式：自建数据中心/租赁机房
- 总分架构：分行有设备
- 运营方式：自营/托管（给大行）/外包
- 环境规模：几百到几万（OS数量）
- 监管要求：两地三中心、等保

国内银行业IT云转型痛点

- 成本中心，资源浪费（向用者付费模式转型）
- 机制体系，太成熟（部门多、分工细、流程长）
- 存量包袱重，上云难（IaaS+、契机、高层决心和推动力）
- 中小金融机构IT力量不足，私有云重复建设，难度大，规模效益低且合规不足
- 难觅外部高端技术人才，只有内部挖潜

国内银行业IT特征

数据的一致性、可用性、实时性、安全性要求高

应用数量多规模小、同步多异步少、云化服务化慢

依赖差异化的IT基础设施实现较多安全可用连续性功能

业务安全性、可用性和连续性等监管合规要求高

- **立足继承发展、自主可控，进行零基设计和系统创新**
  - ✓ 设备/专业高可用、Infra云化 → 架构/服务高可用、应用云化
  - ✓ 开源开放分布式KVM/CEPH + 商业化集中式IOE的融合架构
  - ✓ 构建App Fit Infra的软件定义数据中心（SDDC）解决方案
  - ✓ 以应用系统为中心，规划建设IaaS+应用自动部署管理平台
  - ✓ 面向市场运营，规划建设多租户、服务化、计费计量管理平台

恒丰金融云建设目标

多地多中心

- 平衡应用高可用、连续性、安全性容量性能的SLA等级需求
- 自顶向下零基系统规划设计新一代多活部署架构
- 实现智能监控、准确决策和自动切换恢复

多租户金融云

- 建立大容量、易扩展、虚拟、共享的资源池，提供按需自助、敏捷弹性、高效低价、按量计费的云服务
- 实现多租户设计，为中小金融机构提供云服务

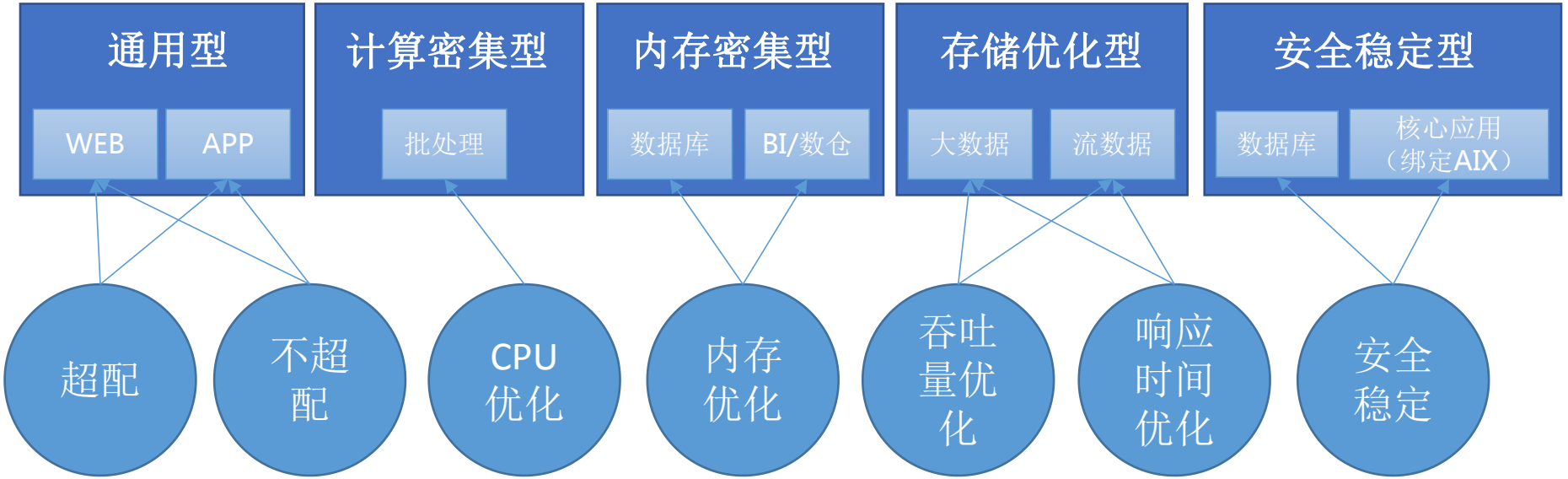
应用云化/自动部署

- 推进应用P-V、LB、SNAT、DNS、GSLB、无状态改造优化
- 实现应用系统建模，建立多中心高可用部署模型
- 实现应用模版化配置和自动部署

可控合规

- 探索开源开放系统最佳实践和管理体系
- 实现租户内和租户间的安全隔离和风险防范
- 符合国内各种安全标准和金融行业监管指引

银行典型计算需求与资源池映射关系



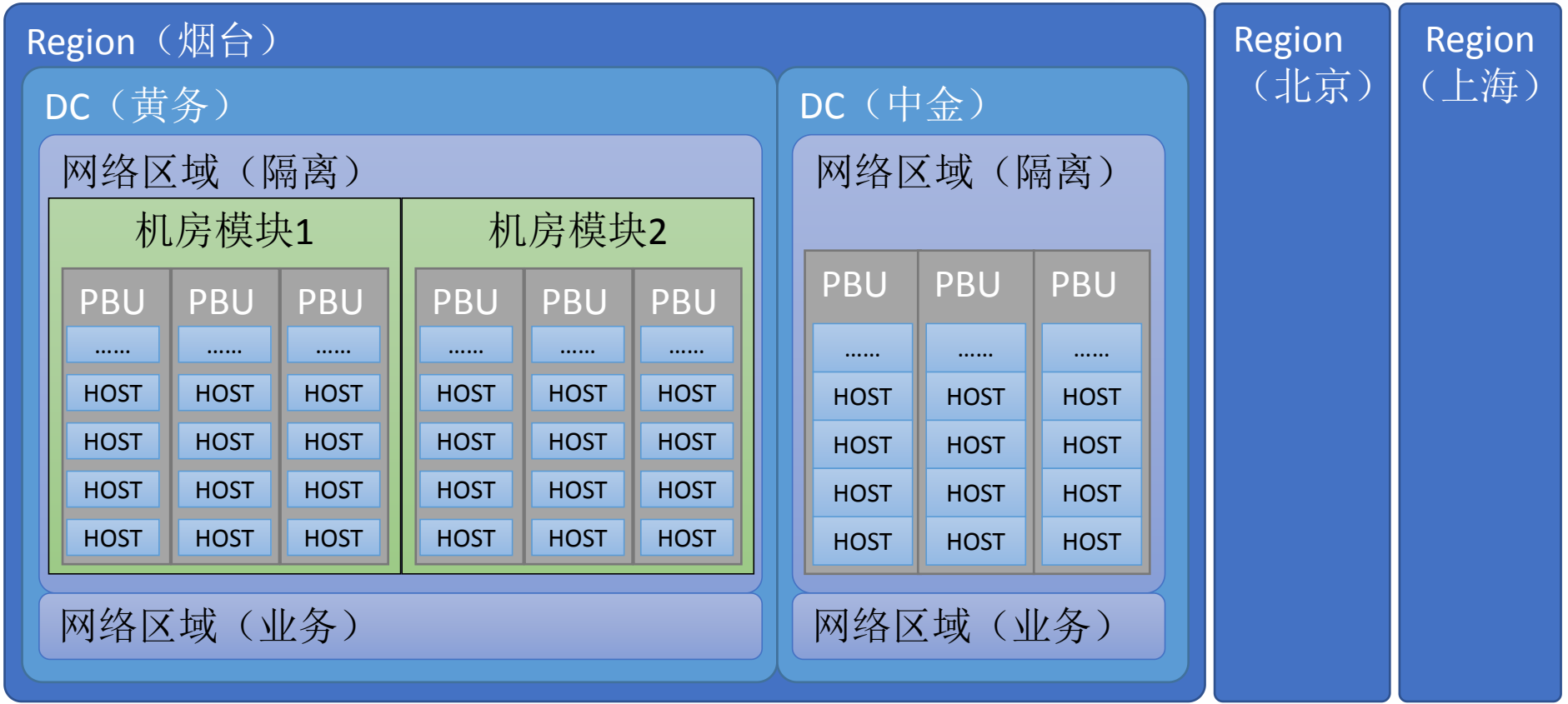
- 由上层管理平台负责Region、DC层的非亲和性调度，并根据网络需求指定具体的网络区域
- 由OpenStack平台负责机房模块、PBU（2个机柜，1对TOR）和宿主机（Host）层的非亲和性调度

Region → DC → 机房模块 → PBU → 宿主机

尽可能分散部署

资源调度策略[2]

1 2 3 4 5 6 7 8



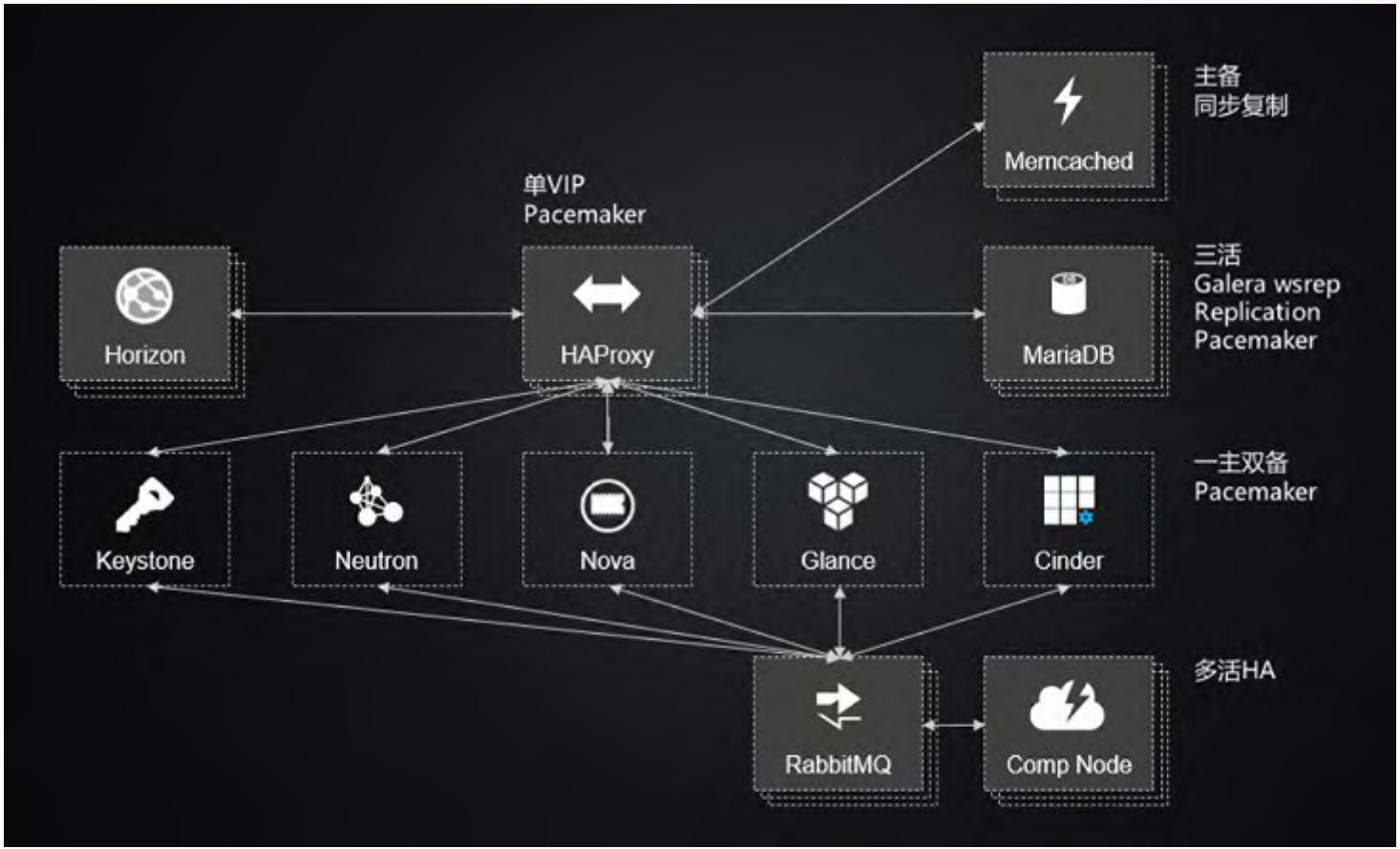
- 库存管理：
  - ✓热库存：资源池余量，应对扩容周期
  - ✓冷库存：库房设备，应对供应链周期
- 预测算法：线性拟合
- 定期评估：季度
- 标准PBU上架（机柜、电源、TOR、布线、服务器、存储等，隔离的网络、连线规则的校验等）

国内银行业率先采用开源OpenStack/KVM/CEPH构建金融IT基础设施云平台，近140个应用的全部研发、测试、生产环境均由OpenStack开源云平台提供（数据库及大数据平台除外）。

自行开发实现了包括虚拟机/宿主机HA，宿主机/虚拟机监控，存储服务探测，基于机柜的非亲和性调度等，针对金融云中应用的特点，对OpenStack及CEPH在高可用及连续性方面的功能增强

开源技术使用的管理体系和最佳实践，有效控制开源技术风险（防止厂商绑定：不使用发行版，与社区版本同步基线版本代码；取各供应商所长：选择引入各供应商有益的代码模块或片段以补充社区没有的特性和功能，自己管理内部的代码基线，有选择的同步社区patch）

OpenStack服务高可用



- 计算节点：400+
- 存储节点：400+
- 实例（虚拟机）：10000+
- 承载应用：140+（全部）

IaaS Plus

首创IaaS+服务，应对金融行业传统应用自助上云和云上自动运维难题

首次建成多租户的金融行业公有云，金融云服务满足等保、两地三中心等监管要求

恒丰金融云技术创新

国内银行首家全面投产OpenStack

国内银行首家全面使用SDN软件定义网络

创造性地融合了传统优势技术与开放开源技术的特色云平台

一群平凡的人做卓越的事

让金融IT云化更简单