

SACC 第八届中国系统架构师大会
2016 SYSTEM ARCHITECT CONFERENCE CHINA 2016

架构创新之路

农银人寿新一代核心业务系统 云平台实践

新核心项目组 王福强



农银人寿保险股份有限公司
ABC LIFE INSURANCE CO., LTD.

前言：让云落地



一边是云技术发展如火如荼，高高在上

对传统公司来说

云能否解决公司的问题？
投入产出是多少？
坚持？观望？试水？推倒重来？



一边是公司现实差距太大，如陷泥潭

本文讲述农银人寿在云平台方面的实践，希望能提供一个有益的参考

目录



一	项目简介
二	新核心系统的云平台
三	实例：批处理平台（Batch PaaS）
四	实例：用户管理（UM PaaS）
五	总结

一、项目简介

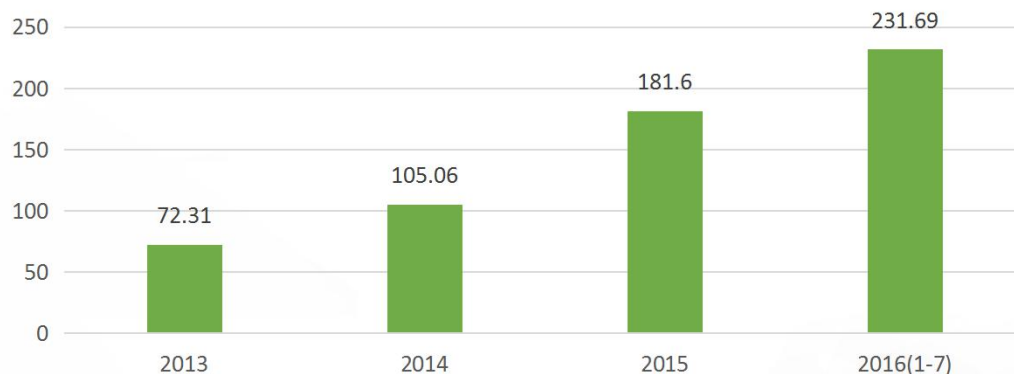
公司情况：

- 农业银行控股
- 中小型寿险公司
- 发展很快（年增长**50%+**）
- 传统金融行业
- 成立10年，更名3年

现状分析：

- 背景、约束
- 资源有限
- IT有点跟不上
- 保守、安全
- 大量遗留系统

保费（亿元）



现有核心业务系统是2007年建设，近几年故障多、性能差、改造困难，无法满足公司业务快速发展需要，技术方面问题：



技术陈旧，集成困难：JDK 1.4.2，目前很多软件无法集成



架构设计不好，扩展困难：JSP+Servlet



运行不稳定，性能差：不定期宕机，紧急补丁多，批处理速度慢

一、项目简介：建设目标

项目建设目标

- 推动公司运营体系、营销机制的创新
- 提高生产化水平和市场响应速度
- 增强公司的市场竞争力和影响力
- 支撑公司未来十年业务发展需要



一、项目简介：保险IT的挑战

唯一不变的是一切在变！

IT方面



业务方面

渠道 | 流程 | 产品 | 规则 | 销管基本法 | 监管

一、项目简介：为何使用云

市场响应速度

快速

快速开发
快速上线

未来十年业务需要

水平扩展

增加服务器就
能提升系统性能

资源有限

共享复用

复用能带来生
产力提升和成
本降低

安全稳定

可用性

无单点故障
故障自动转移
在线增减资源

快点下班！

IT人做梦都想这样！节省的发奖金多好！

又好又快才有意义！

目录



一	项目简介
二	新核心系统的云平台
三	实例：批处理平台（Batch PaaS）
四	实例：用户管理（UM PaaS）
五	总结

二、新核心系统的云平台

基本特性

快速弹性

多租户

按需自服务

可计量服务

资源池

服务模式

软件即服务
SaaS

平台即服务
PaaS (10个)

基础设施即服务
IaaS (3个)

部署模式

公有云

私有云

混合云
(远期规划)

实施模式


商业产品
本地实施 **【7个】**


自主设计
外包开发 **【6个】**


开源产品
自主开发 **【0个】**

二、新核心系统的云平台

SaaS组成

待规划.....



PaaS组成

用户管理
UM

批处理平台
Batch

渠道接入平台
CIP

报表平台
Report

自建
完成

内容管理
ECM

规则管理
IBM ODM

流程管理
IBM BPM

监控平台
MONITA

购买
实施中

产品工厂
PF

分布式事务管理
DTX

自建
实施中

IaaS组成



虚拟机-VMware



数据库-Oracle 12C



中间件-Weblogic 12C

完成
可提高

二、新核心系统的云平台

跟别人有点不一样？

充分利用遗留
应用系统

充分利用已购买
软硬件资产

充分利用现有
人员的知识技能

Why ?

二、新核心系统的云平台

别看广告，看疗效！

保险最易变五要素实现80%

应用开发基础模块实现6个



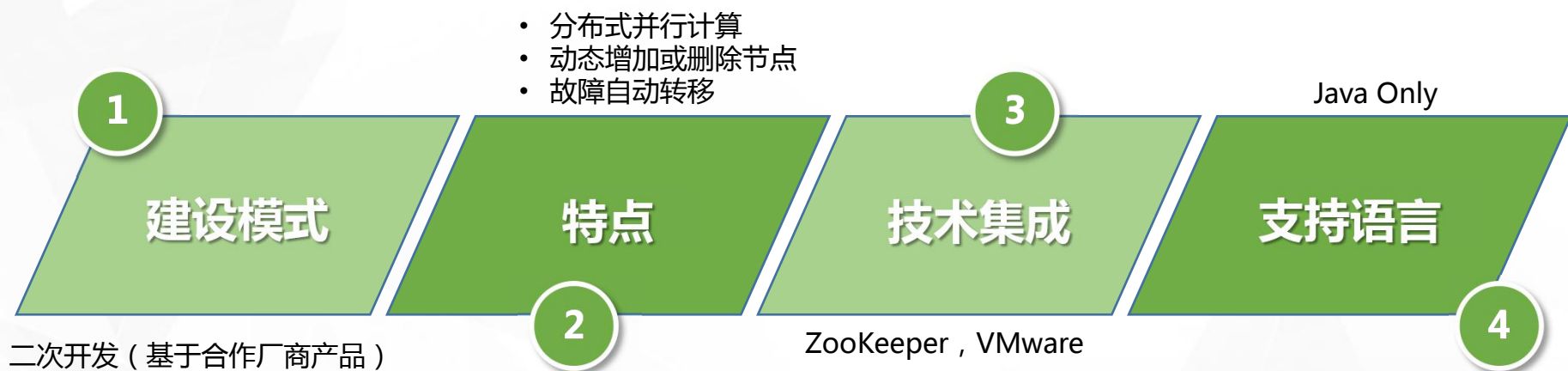
大幅提高上线速度，以及IT应用系统开发的生产力！

目录



一	项目简介
二	新核心系统的云平台
三	实例：批处理平台 (Batch PaaS)
四	实例：用户管理 (UM PaaS)
五	总结

三、实例：批处理平台

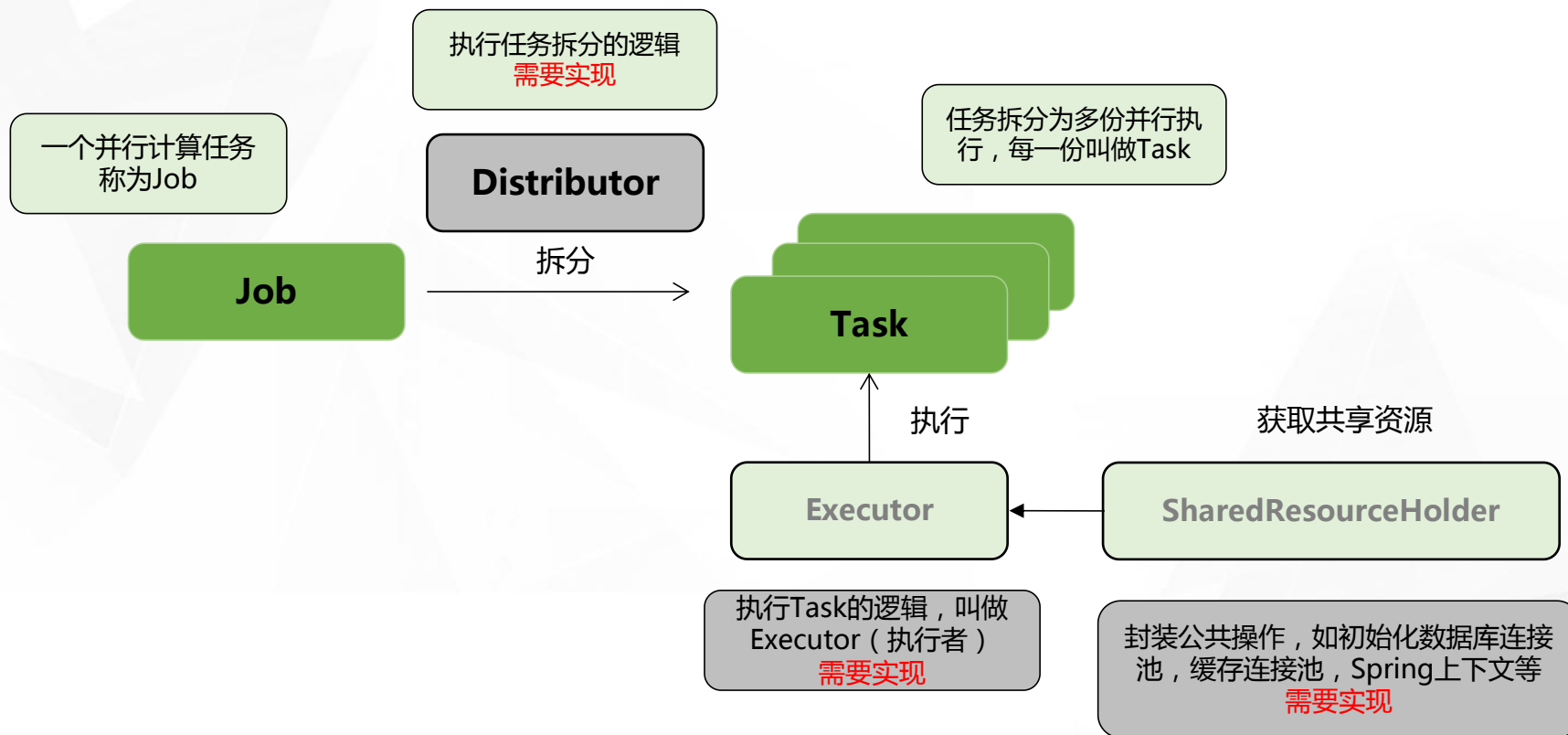


- 批处理平台提供批处理开发、批处理运行管理两部分功能
- 主要用于大批量数据的统一处理，如分红批处理，满期批处理等

三、实例：批处理平台

原开发模式

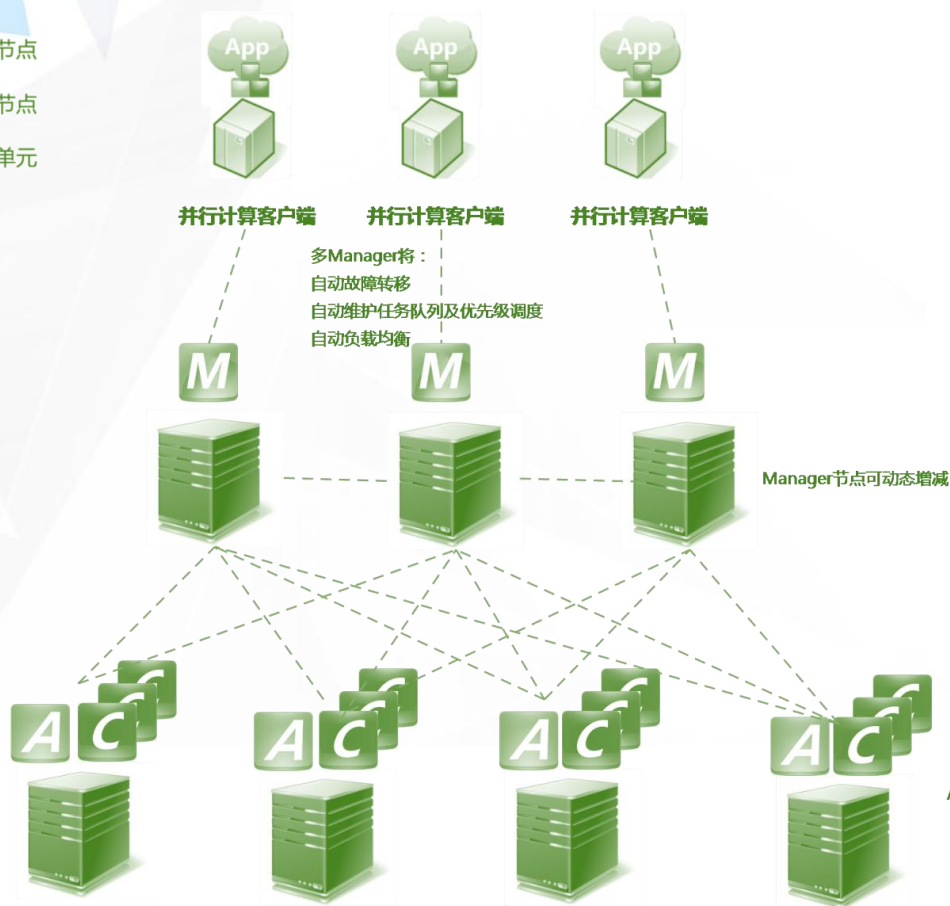
开发人员学习平台的五个基本概念，并开发实现其中3个的子类即可。



三、实例：批处理平台

原部署结构

M 管理节点
A 代理节点
C 运算单元



Zookeeper 高可用集群

ZooKeeper ZooKeeper ZooKeeper

* 必须

PostgreSQL 高可用集群

可替换为任意主流关系型数据库

PostgreSQL PostgreSQL

* 必须

统一日志收集

ELK

* 可选的

平台管理控制台

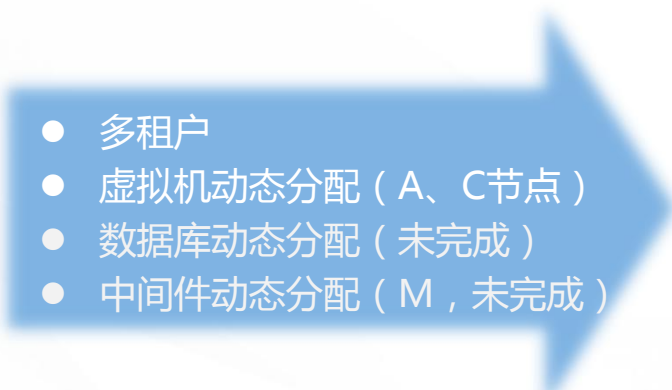
* 可选的

- * 无单点故障
- * 支持节点动态增减
- * 自动故障转移

三、实例：批处理平台

我们做了哪些改造使其成为PaaS平台？



- 
- 多租户
 - 虚拟机动态分配 (A、C节点)
 - 数据库动态分配 (未完成)
 - 中间件动态分配 (M, 未完成)



三、实例：批处理平台

1 隔离性

- 数据隔离
- 性能隔离
- 安全隔离

2 适应性

多租户不同需求
(下一个实例)



多租户

不只是在数据库中增加一个区分租户的字段

三、实例：批处理平台

多租户的实现

原系统无多租户

- 用户能够查看和管理**所有**的批处理（安全风险）
- 批处理自动分配到**所有**服务器执行（资源争用）
- 数据库访问由批处理程序**自行设定**（安全风险）

新系统（多租户）

- 用户能够查看和管理**自己**的批处理（安全）
- 用户的批处理自动分配到**自己**的服务器执行（性能隔离）
- 用户仅能访问**自己**的数据库（数据隔离）

新增功能：

- 服务器管理（包括申请，审批，授权使用，授权回收）
- 数据库管理（授权，回收）

三、实例：批处理平台

动态分配的实现

原系统 (无动态分配)

- 所有用户能够使用的服务器是预先安装配置好的
- 如果需要增加资源，需要走审批流程（甚至采购流程）

新系统 (动态分配，目前针对运算单元的服务器)

- 当计算资源不足时，用户申请计算节点
- 虚拟机管理员审批后，系统自动调用vmware接口，按需创建虚拟机
- 批处理管理员授权给用户使用
- 用户的job就可以使用这些计算节点了，批处理马上提速
- 当然，如何管理员预先给用户分配虚拟机，就不需要申请了。

注：管理节点一般不是性能瓶颈，动态分配Oracle DB、Weblogic尚未实现

三、实例：批处理平台

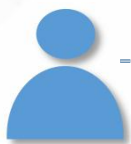
Batch PaaS总图



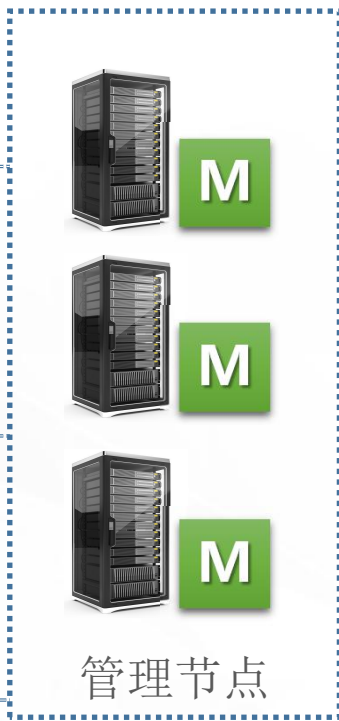
A应用



B应用



管理员



管理节点

vmware虚拟机
weblogic集群
Zookeeper

授权使用

授权使用



A计算节点



B计算节点

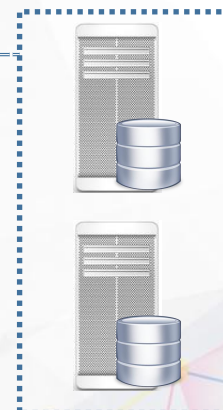
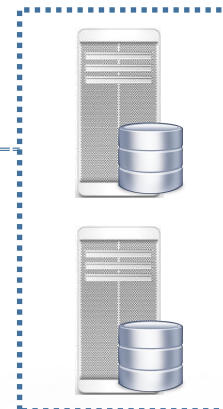


资源池

vmware虚拟机
Zookeeper

授权使用

授权使用



oracle集群
(CDB , PDB)

三、实例：批处理平台

Batch PaaS通过引入产品和二次改造实施，最终效果如下：

- 屏蔽了分布式并行计算的复杂性，实现高性能和高可用
- 屏蔽了批处理开发的复杂性，实现复杂模式（暂停，恢复，重跑，补跑，任务序列，手工调度，定时调度等），开发和部署简单
- 多租户实现资源的共享和复用，资源隔离、计算隔离、安全隔离
- 实现快速弹性，资源动态分配

投入

- 改造费用：20人月
- 其他费用：
- VMware (0)
- Oracle (0)
- Weblogic (0)



产出

- 多租户、快速弹性、故障自动转移
- 性能提升：20%~数十倍
- 快速开发：平均节省数天
- 快速部署：数天变为数小时

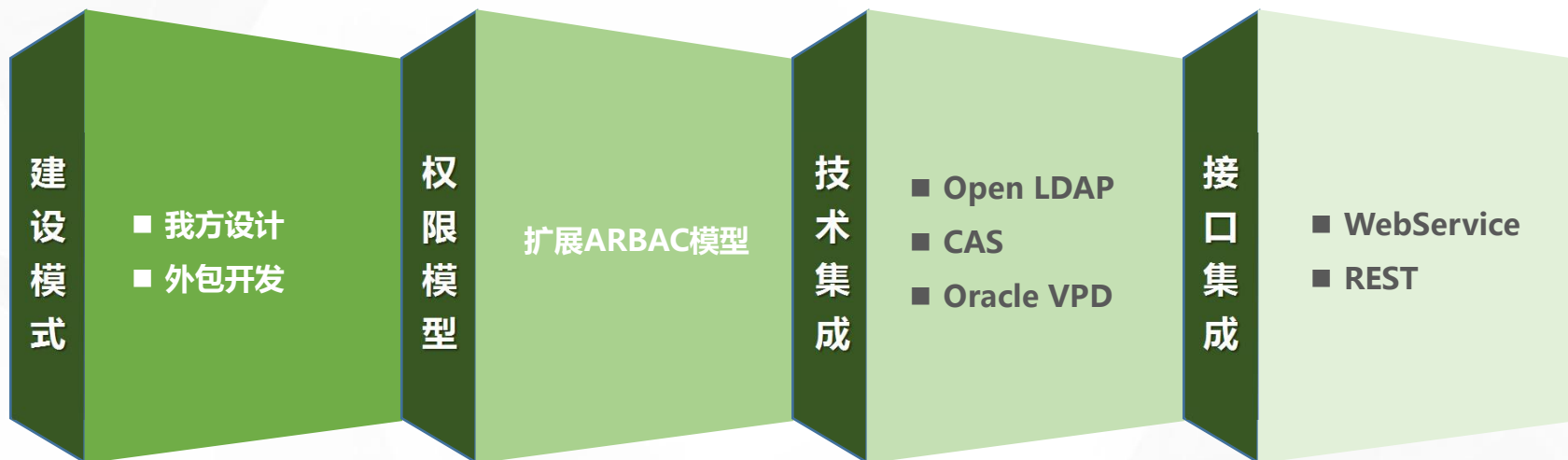
目录



一	项目简介
二	新核心系统的云平台
三	实例：批处理平台（Batch PaaS）
四	实例：用户管理（UM PaaS）
五	总结

四、实例：用户管理

统一用户管理包括用户管理、组织机构管理、权限管理三部分功能。用于所有新核心项目的子系统，进行统一认证和统一权限管理。



四、实例：用户管理

UM系统做PaaS难在多租户的适应性

应该支持RBAC，也应该支持ACL

应该对**开发者透明**，对用户简单明了

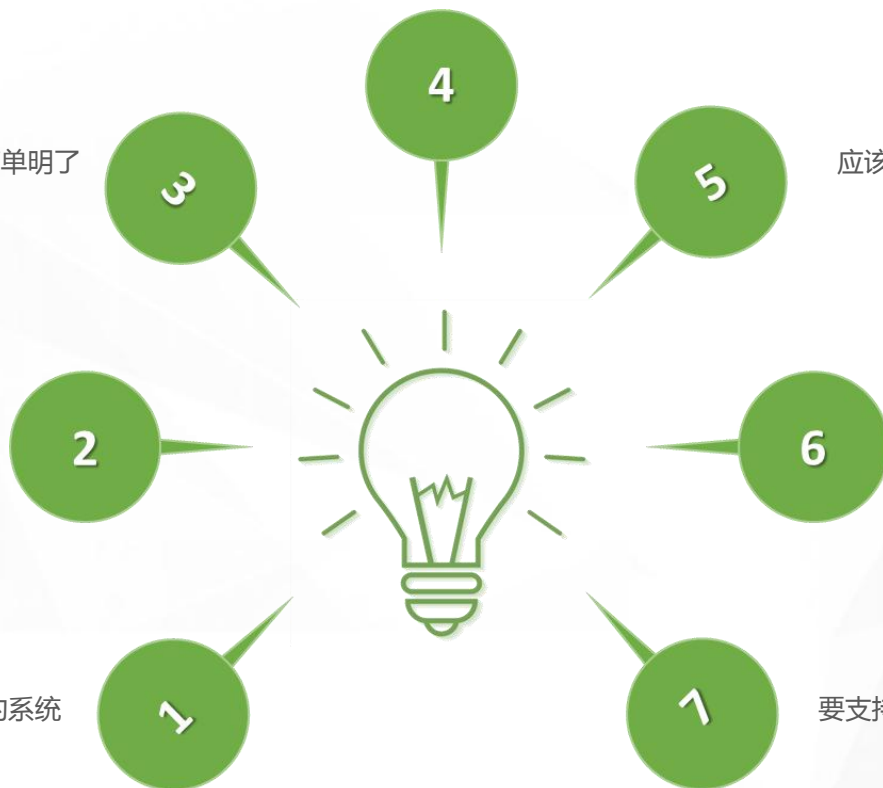
应该支持功能权限，也应该支持数据权限

对简单系统使用必须简单

应该支持到最细粒度，但是也能粗粒度使用

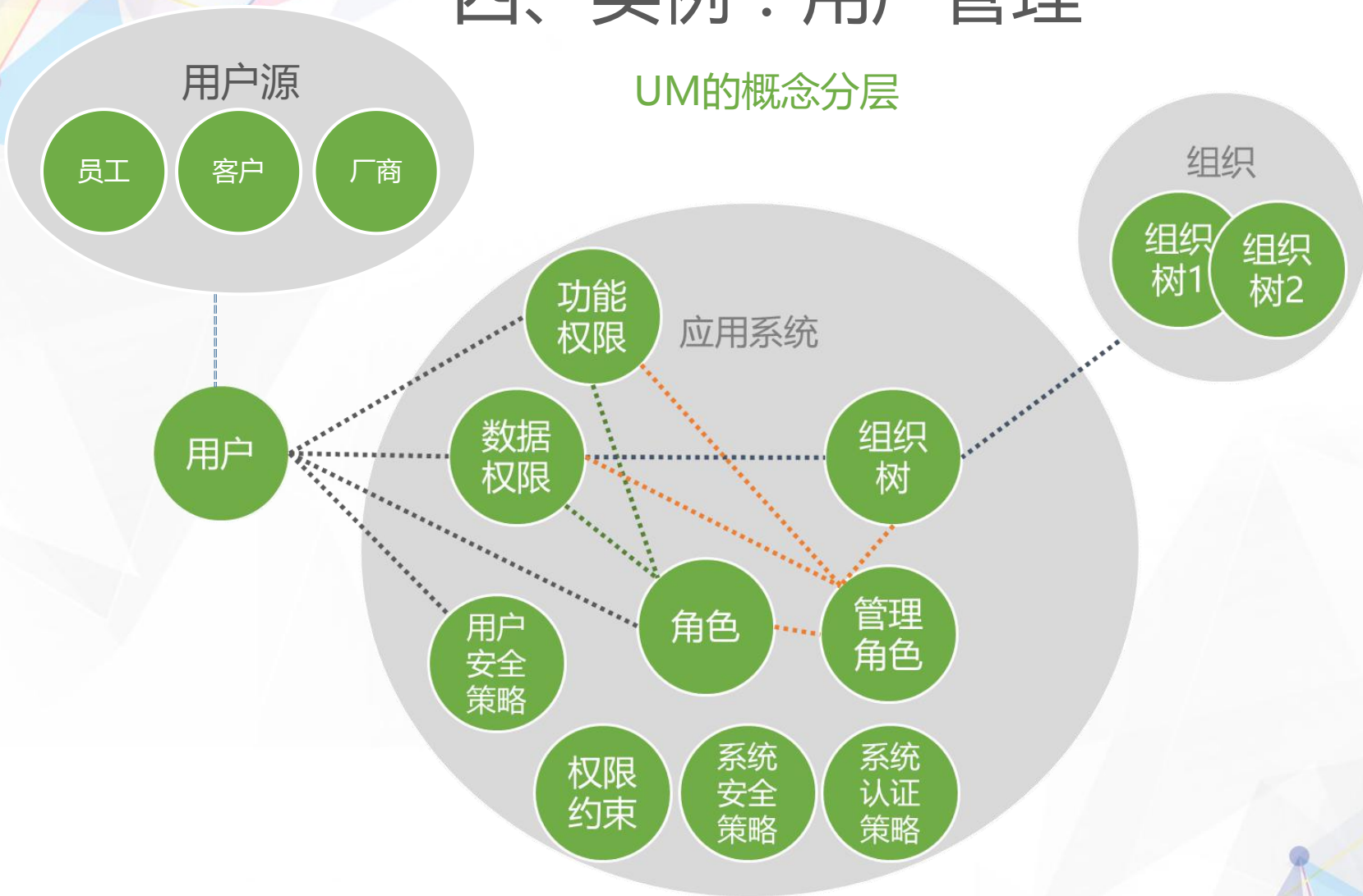
必须能够适应简单的系统，以及复杂的系统

要支持更复杂的认证和安全方式和策略



四、实例：用户管理

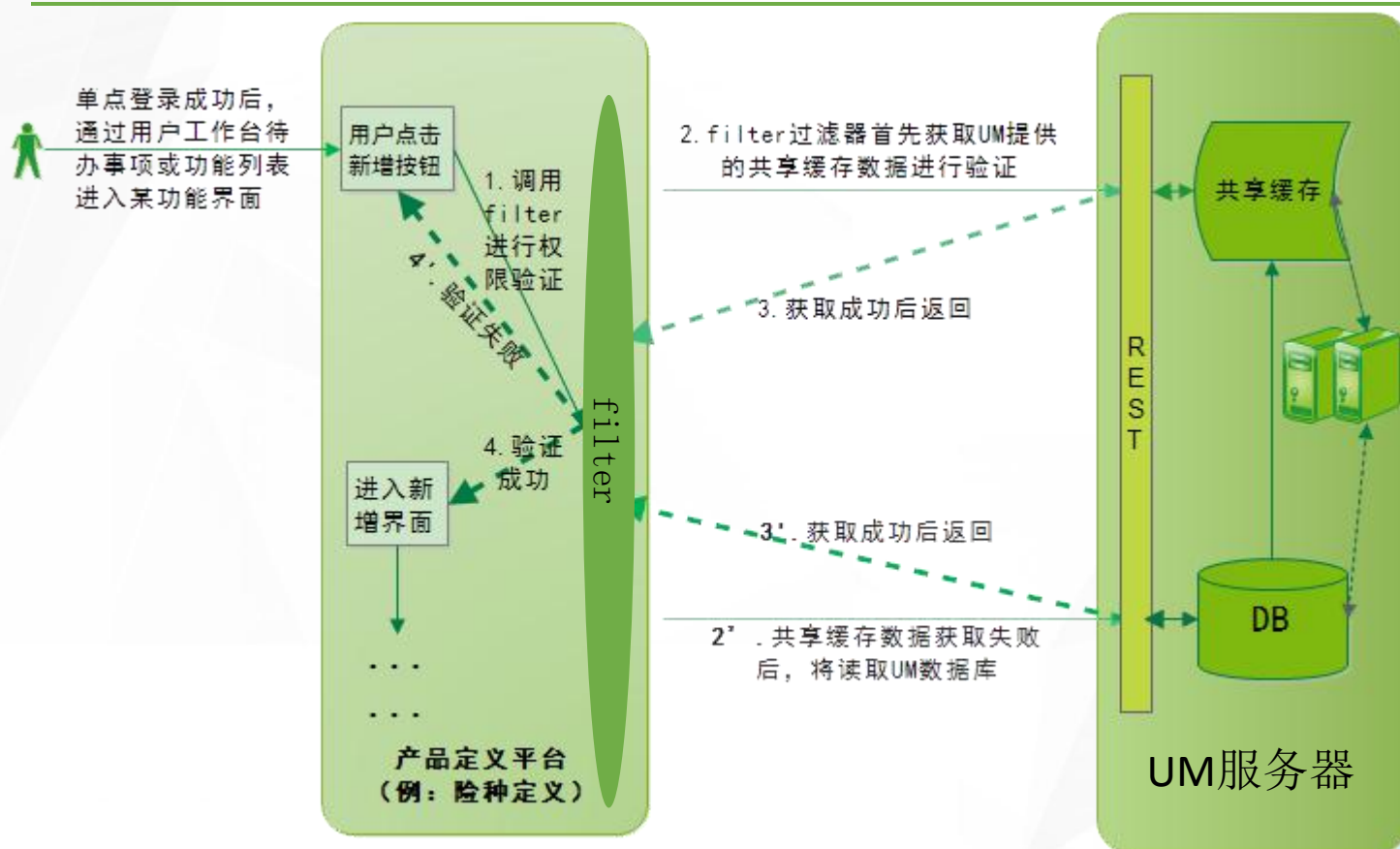
UM的概念分层



四、实例：用户管理

功能权限的实现

提供通用权限认证过滤器Filter，以实现灵活进行子系统集成



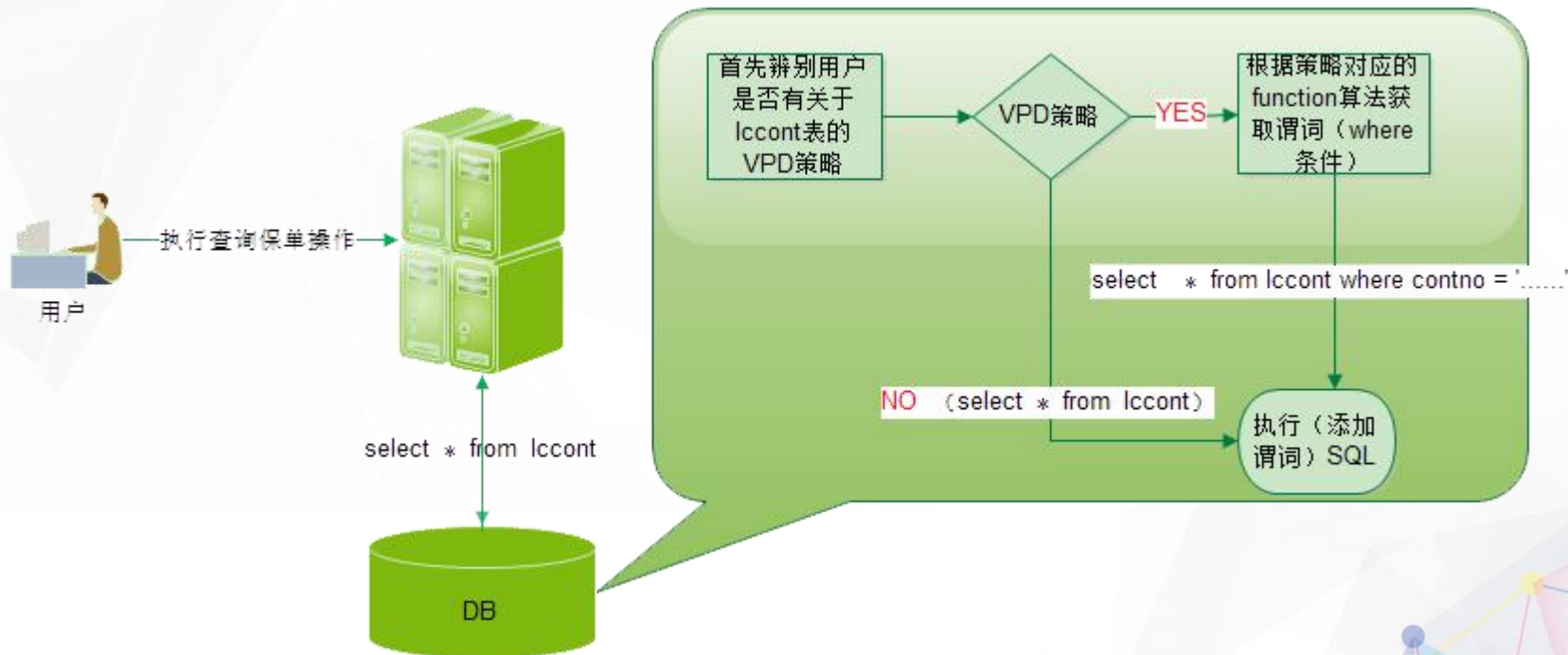
四、实例：用户管理

数据权限的实现

使用ORACLE 企业版VPD (Virtual Private Database)

从数据库层面实现数据访问控制的一种成熟技术 (能够实现行级、列级访问控制)

性能高：每次SQL平均时间损耗 0.2ms



四、实例：用户管理

UM PaaS通过自主设计和外包实施，最终效果如下：

- 应用透明：屏蔽了用户、机构和权限的管理，集中统一管理，其他应用不考虑
- 开发透明：屏蔽了认证和权限的开发，普通开发者不考虑
- 多租户：实现资源的共享和复用，满足各种安全级别和安全管理需求

投入

- 外包费用：70人月
- 其他费用：
Oracle VPD (0)
Weblogic (0)



产出

- 开发更高效，开发者透明
新核心系统30多个系统不开发用户和权限管理（节约2人月/系统以上），集成只需1-2天
- 管理更方便
员工所有权限集中管理，一览无余；调岗、离司处理方便
- 随需而变
应用的安全级别可随时修改；应用的安全策略可随时修改
- 更安全
安全策略可定制；最细粒度的功能权限控制（每一次请求/点击）；最细粒度的数据权限控制（行级和列级）

目录



一	项目简介
二	新核心系统的云平台
三	实例：批处理平台（Batch PaaS）
四	实例：用户管理（UM PaaS）
五	总结

五、总结

我们下一步工作：

- (1) 内部推广，创造服务价值：服务的应用系统从20+增至100+
- (2) 继续完善，提升服务能力：去中心化、标准化



通过加强这两项，还能够实现：

- ✓ 更简单和快速的资源管理
- ✓ 更简单的部署，更少的人工干预

五、总结

农银人寿新一代核心业务系统结合公司实际，实现了部分IaaS和PaaS平台，经过实践检验，取得比较不错的效果。

我们的一点实践经验



技术是为业务服务

创造业务价值才是传统公司IT最大的价值



没有最好只有最合适

结合公司实际选用合适的云技术，不要完美主义



别纠结太多概念

云技术还不算特别成熟和具有公论，根据效果选择

THANKS

SequeMedia
盛拓传媒

IT168.com
6 3 0 9 10 9

ChinaUnix

ITPUB
www.itpub.net