中国光大银行

容器云PaaS平台POC方案

中国光大银行信息科技部

发布版本：V2.0

关键词：信息科技、容器技术、分布式、应用架构

修订记录

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **版本号** | **版本日期** | **版本类型** | **修订人** | **修订说明** | **审核人** |
| V1.0 | 2017-6-14 | 初稿 | 解培 | POC内容框架草拟 |  |
| V1.1 | 2017-6-19 | 修订 | 陈瑶 | 增加测试点 |  |
| V1.2 | 2017-6-29 | 修订 | 陈瑶 | 修订测试点，增加测试案例说明 |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

版本类型：创建/发布/修订

版本：

创建版本：0.1

发布版本：x.0，x为从1递增的整数

修订版本：x.y，x为上次发布版本，y为从1递增的整数

# 目录

修订记录 2

目录 3

一、方案背景及概述 4

二、环境需求（各家补充） 4

（一）主机环境 4

（二）网络需求 5

（三）其它需求 5

三、测试计划 5

四、POC测试案例说明 5

（一）整体架构 6

（二）逻辑架构 6

（三）物理架构 6

五、测试项目列表 7

（一）分布式微服务框架 7

（二）应用管理 7

（三）服务管理 7

（四）平台管理 8

（五）分布式应用组件 9

（六）性能 9

（七）开发测试流水线 9

（八）容器云平台部署 9

（九）多数据中心，混合基础设施管理 9

（十）镜像仓库管理 10

（十一）镜像管理 10

（十二）应用编排及管理 10

（十三）服务目录管理 10

（十四）容器管理 10

（十五）容器网络 11

（十六）容器存储 11

（十七）平台高可用 11

（十八）平台安全 11

# 方案背景及概述

为适应互联网业务创新，探索引入分布式架构进行应用云化，同时利用容器技术提高标准化和自动化能力。面向业界主流解决方案的通用功能点，结合行内针对该类型需求的要求编写本测试方案，做到客观、公正、严谨的横向评测各方案的完整性、技术特点、可靠和可用性，以及平台开放和整合能力。

# 环境需求（各家补充）

## 主机环境

以表格形式展现，下面表格内容是样例，请根据各自方案填写。最后请汇总需要的物理机、虚拟机数量。表格内容可以根据各自方案调整。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 角色 | 功能 | 数量 | 类型 | 配置 | 备注 |
| *平台xx组件* | *集群管理* | *2* | *虚拟机* | Ubuntu 16.04, 8C/32G 80GB硬盘 | *存储容量够用即可* |
|  | *镜像仓库* | *2* | *物理机* |  |  |
| *微服务治理xx* |  |  |  |  |  |

## 网络需求

请描述网络方面需求，比如vlan数量和IP地址段、IP地址数量、防火墙需求（虽然默认我行测试环境无防火墙，详细提供端口需求有助于后续测试中问题排查）

注意：我行不提供任何互联网连接，必须离线安装部署、提供服务！！

## 其它需求

例如：NTP服务、DNS服务等需要我行提前准备的各类基础需求。

# 测试计划

|  |  |  |  |
| --- | --- | --- | --- |
| 时间（天） | 内容 | 对应测试功能点 | 人员安排 |
| 事例：以天为单位，3天 | 安装部署 | 下面测试内容章节的哪部分，比如5.1 | 人员姓名、电话？方便联系 |
|  |  |  |  |
|  |  |  |  |

# POC测试案例说明

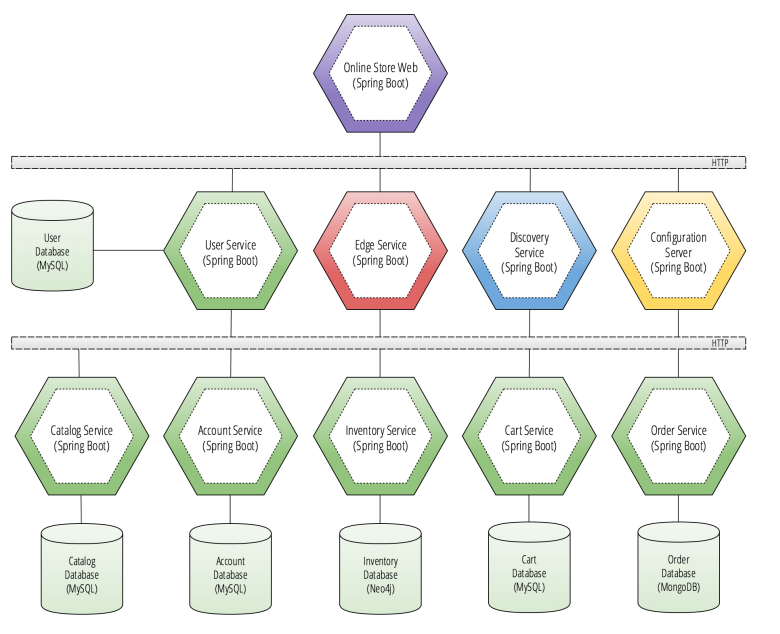
本次POC测试案例需求为模拟电商网站购物过程和秒杀场景。微服务拆分方式如下：

1. 前端页面：用户登录的前端页面，可以查看商品信息，登录后可以下单购买。
2. 用户认证：提供用户登录和认证服务。
3. 商品服务：商品信息
4. 库存服务：商品库存信息
5. 购物车：购物车信息
6. 账户服务：账户信息
7. 订单服务：下单后产生订单信息
8. 付款服务：订单提交后进行付款服务，并修改订单状态等内容。（参考样例中未涉及）付款成功后，调用消息队列模拟发送短信。
9. 服务注册发现中心、服务配置中心、API网关等微服务架构必备的框架。

注意：

* 此案例需在付款服务时考虑事务一致性。
* 为应对秒杀场景，提高效率，部分内容（如商品信息）应放入分布式缓存中存储。
* 发送短信的消息队列，需使用分布式消息。
* 请尽可能使用此案例需求覆盖测试点。

参考样例（仅供参考）：https://github.com/kbastani/spring-cloud-event-sourcing-example



## 整体架构

描述贵公司本次POC的方案整体能力组件和功能边界，架构图形式附带简要说明。

## 逻辑架构

方案的逻辑组件关系，架构图形式，附带简要说明。

## 物理架构

所有节点角色的物理拓扑，提供高可用性的部署细节

# 测试项目列表

## 分布式微服务框架

1. 框架搭建：

提供服务注册、服务发现、服务路由、服务调用，轻量级通讯等功能。其中，内部服务间轻量级通讯需支持REST和RPC两种方式（最少支持一种）。

【王霄】：数人云微服务框架年底产品release，暂时不支持。

但可以先用squid基于消息的微服务调度框架测，打个擦边球

## 应用管理

1. 应用生命周期管理

应支持以镜像形式部署，同时支持现有目录或war包形式部署。支持一个应用部署在不同容器集群（包括不同机房和同一机房的不同网络域：例如某应用前端页面、后端服务、数据库分别在互联网域、业务域、生产域；例如某业务域服务需按比例部署在业务域的不同网络区）。支持自动化部署。

【王霄】：war包形式产品不支持，但浦发卡有方案，测试时需要补充这部分。其他支持

1. 应用升级回滚

混合云不同底层介质提供不同升级策略。支持灰度发布、滚动升级、升级回滚等。

【王霄】：支持

1. 应用配置中心

提供应用级的配置中心和配置项变更能力。

【王霄】：配置中心10月release

1. 自动伸缩管理

应支持不同容器集群间弹性伸缩策略配置（例如AB两机房/网络区可按百分比扩容，可分别设置AB各自的扩容数量，可跨故障域扩容）。

支持对应用中部分服务的弹性伸缩。

支持机房/网络区/宿主机亲和和反亲和策略。

所有应用部署形式均支持自动伸缩。

【王霄】：3.5版本无自动伸缩

1. 应用健康检查

提供应用和服务的健康检查机制，用以判断当前的应用/服务实例是否正常运行，当实例异常时，可进行相应故障处置（支持故障处置策略和自动化运维），避免终端客户访问异常。

【王霄】：支持

1. 应用多版本管理

【王霄】：支持

1. 应用依赖关系管理

可对租户空间内的所有应用或者指定应用进行扫描，发现应用依赖和被依赖的应用和微服务，并提供报告。帮助应用开发者和应用运维人员对应用的内部情况进行更多的了解。

【王霄】：调用链跟踪功能，后续会和听云或oneapm合作，放入微服务框架，所以暂时也不支持

1. 故障处置

故障通知、报警、定位、隔离、恢复等。

【王霄】：支持

## 服务管理

1. 服务生命周期管理

提供服务发布（内部服务/外部服务）、删除、查询（服务列表）、升级、多版本、多租户服务隔离等功能。

1. 链路跟踪[依赖关系管理]
2. 服务限流=》APACHE
3. 服务降级=》APACHE
4. 服务依赖关系管理【依赖关系管理】
5. 服务访问控制

对外：私有服务、公共服务；对内：服务间调用权限设置；包含申请流程。

1. 服务调用分析
2. 服务配置中心
3. 服务容错保护=》SQUID
4. 服务列表

提供发布的服务列表和消费的服务列表

【王霄】：产品12月底release，暂时不支持。可以先用squid测。

## 平台管理

1. 租户管理

平台支持多租户，并提供租户管理功能。

【王霄】：支持

1. 用户管理

用户增删改查，用户分组等。

【王霄】：支持

1. 角色管理

【王霄】：支持

1. 权限管理

菜单权限、服务访问权限等。

【王霄】：支持

1. 操作审计

用户操作记录、操作日志查看和检索。

【王霄】：支持

1. 集群管理

支持并可以管理多个容器云集群。可设置并调整平台资源、集群资源、应用/服务可用资源。对应用/服务的弹性伸缩进行资源限流，避免平台瞬间过载。

【王霄】：支持

1. 日志管理

平台提供或集成高效可靠、自动化的日志管理服务，实现对应用和平台自身日志的收集、存储、检索、整合分析、查询、导出、告警服务。

【王霄】：支持

若日志管理服务为平台内的服务，平台应对日志管理服务提供在线资源调整等管理功能。

1. 监控管理

平台提供监控管理页面，可展示/输出应用指标（交易流量、负载、TPS、应用访问量等业务指标和应用对资源的使用情况等）、服务指标、平台资源指标（CPU、内存、磁盘、容器等）、集群/单机指标、操作指标、性能指标等。为应用稳定运行，容量规划，升级，扩容等提供数据指标支撑。

【王霄】：应用指标没有，其他满足

1. 定时任务支持

平台可支持一次性运行类型的任务，用户可以按正常间隔或固定时间运行任务。可在线查看和管理任务。

【王霄】：满足

1. 管理工具支持

提供开放的API，API应该功能丰富、使用简单明了，对不同用户（管理员、普通用户等）有权限控制，分别支持对PaaS平台管理、应用管理、服务和应用组件管理。可封装成常用命令行工具对外提供。支持常用编程语言和通讯协议。

【王霄】：满足

1. 平台升级

平台提供升级功能，应不影响平台上的应用/服务且不会导致业务停顿。

【王霄】：可以答满足，要看平台架构是否大动，还要看是什么应用

1. 云中间件服务升级

云中间件服务提供不影响业务的升级方式。

【王霄】：满足

1. 平台备份恢复

支持对整个PaaS平台做备份和恢复，整个备份和恢复的过程不影响平台业务的访问。

【王霄】：支持，但是为手动

## 分布式应用组件

1. 分布式缓存管理和高可用
2. 对象存储服务管理和大文件传输支持
3. 分布式数据库管理和高可用
4. 分布式事务处理机制
5. 软负载均衡服务管理

支持7层和3层负载均衡管理。

1. 分布式消息服务管理

消息发送、消费、订阅、定时消息、事务消息、运维功能、高可用、可扩展、负载均衡

1. API网关服务管理

【王霄】：以上暂时都不支持

## 性能

平台自身性能，上述功能的高可用+弹性伸缩速度。PS：应用的性能，后续在统一环境下验证。

## 开发测试流水线

1. 与容器云PaaS平台集成

DevOps全流程演示（编译、打包、部署），支持镜像和war包两种方式。

Ps：CI/CD流水线使用厂商自带的产品。

【王霄】：满足，但测试时需要补充war包的方案

## 容器云平台部署

容器云平台快速部署

【王霄】：满足，1小时内安装完成

## 多数据中心，混合基础设施管理

1. 多数据中心主机接入管理
2. 混合基础设施的主机接入和网络适配
3. 主机统计信息展示
4. 主机监控报警

【王霄】满足，通过grafana页面查看主机监控

## 镜像仓库管理

1. 镜像仓库创建和管理
2. 镜像仓库镜像批量下发
3. 镜像搜索
4. 管理外部镜像仓库
5. 镜像仓库安全管理

【王霄】满足

## 镜像管理

1. 镜像管理，列表及详情显示

【王霄】满足

1. 镜像分布和关联容器查询

【王霄】暂时没有

## 应用编排及管理

1. 应用资源配额设置
2. 应用调度策略设置
3. 服务依赖关系定义
4. 配置文件管理
5. 编排模板版本化管理
6. 编排模板导入导出
7. 跨容器集群的应用编排能力

提供跨机房、跨网络域（例如：生产域、业务域、互联网域）、跨网络区（每个网络区属于不同的容器集群）的应用编排能力。

【王霄】可以答满足，但目前支持的不好，需要写编排文件和调borg API的脚本，暂时没有整合在一起

## 服务目录管理

1. 共享服务目录上架和管理
2. 共享服务应用部署
3. 共享服务导入导出

【王霄】满足

## 容器管理

1. 容器生命周期管理
2. 容器列表和详细信息展示
3. 容器统计信息展示
4. 容器监控报警
5. 容器日志查看和收集
6. 容器文件上传下载
7. 容器web终端

【王霄】满足

## 容器网络

1. 容器跨主机通信
2. 容器网络隔离
3. 容器IP生命周期管理
4. 容器静态IP设置
5. 容器网络吞吐量和延迟测试

【王霄】满足

## 容器存储

1. 容器挂载主机数据
2. 容器对接外部存储

【王霄】满足，外部存储是接客户已有的存储还是要我们带进去？如果需要我们带的话，就要找一家分布式存储，例如xsky

## 平台高可用

1. 管理节点高可用测试
2. 计算节点高可用测试

【王霄】满足

## 平台安全

1. 提供安全检查功能：

平台安全性主要指PaaS平台能够防止非法访问，确保只有有权限的用户才能访问平台提供的相应服务。

安全检查主要面向容器运行环境，检查其是否合规，包括以下几个方面：容器宿主节点合规性、容器合规性；

容器宿主节点合规性主要检查：内核安全、拒绝服务攻击、防火墙规则、用户权限、安全策略等；

容器合规性主要检查：容器是否正确部署、CPU、内存、磁盘是否超限等；

【王霄】这个需要和安全设备配合，可以答满足