OpsWorld 运维世界大会·深圳站

平安云容器服务与运维平台的对接

平安科技 云平台事业部
陈春润

主要内容

运维世界 Ops World

01 平安云及容器服务简介

02 容器服务构建与运维

03 容器服务应用与运维

平安云概貌

云门户

身份管理 | 服务目录 | 产品订购 | 资源管理 | 计费/账单

产品服务

云主机 Elastic Compute Cloud	弹性文件系统 Elastic File System	云备份 Cloud Backup Service	负载均衡 Elastic Load Balancing
对象存储 OBS	块存储 Elastic Block Store	自动化部署 Middleware/VAD	虚拟私有云 Virtual Private Cloud
RDB数据库服务 (MySQL等)	NoSQL 数据库	容器服务 CaaS	其他服务...

公共服务

监控

部署

安全

日志

云数据中心

深圳 

上海 

北京 

源起 - 金融行业用户需求特征

平安集团子公司中包含金融行业的各个类别，不同企业、不同来源、不同开发模式的业务系统对底层资源的需求差异很大。所有这些需求对于平安云来说都是必须要满足的。

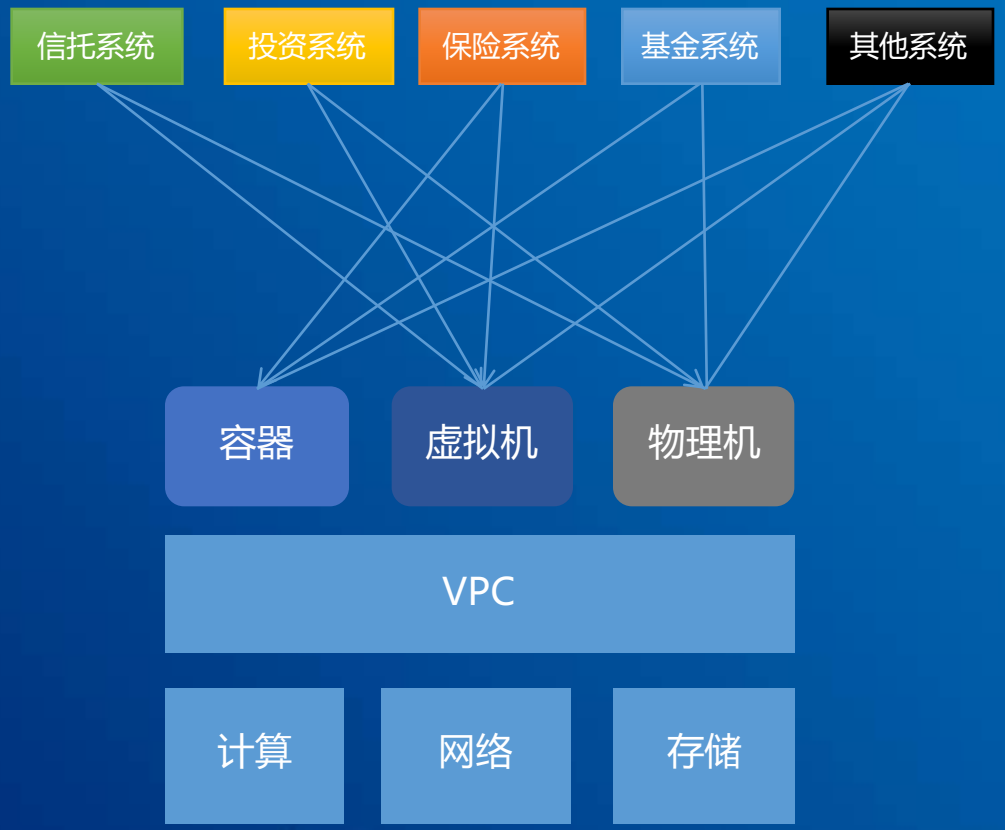
因此平安云会为用户提供不同类型的弹性计算服务，包括：

物理机：高性能，高规格

虚拟机：灵活、安全的共享

容器：灵活、轻量、快速交付

这些不同的计算模式可以共享相同的VPC网络，用户可以根据应用架构选择将一部分应用部署在物理机上，也可以部署在虚拟机上或容器服务中。



容器服务的设计目标——自助服务

对于大多数租户而言，希望能够使用容器服务加快环境部署的速度，提高扩容的效率，降低运维成本，因此平安云提供一套简单有效的容器服务产品，使得用户能够自助完成容器部署工作。

自助式容器服务（私有或公有云服务）

- 用户可定制容器基础架构（*）
- 公共镜像商城
- 私有镜像管理
- 支持混合部署方式（*）
- 兼容平安云基础架构（*）
- 兼容平安应用架构规范（*）

容器服务的设计目标——流水线

对于开发团队而言，希望拥有一套从开发测试到生产部署的流水线，容器服务作为流水线中的实际运行环境，完成最后一公里的工作。

全流程部署自动化（私有云服务）

- 提供API与开发管理平台紧密结合
- 支持开发-测试-生产环境部署流水线
- 用户可定制容器基础架构
- 支持“全容器”和“开发测试容器+生产非容器”型部署需求
- 私有镜像版本管理
- 平台层服务支持

平台构建与运维

产品规划

运维世界 Ops World

租户管理

- 部署容器服务
- 管理运行环境

环境管理

- 环境授权
- 管理主机

应用管理

- 应用编排部署
- 应用管理

服务管理

- 创建服务
- 服务配置

镜像管理

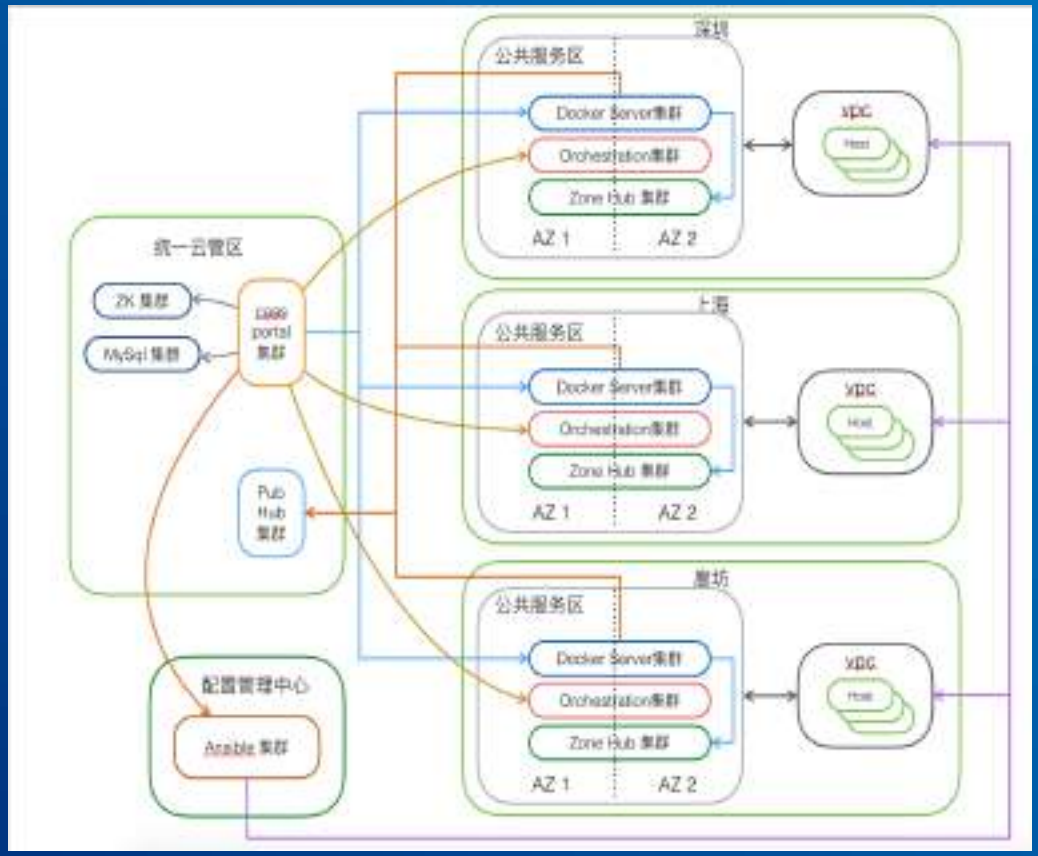
- 镜像商城
- 公共镜像
- 私有镜像

系统架构

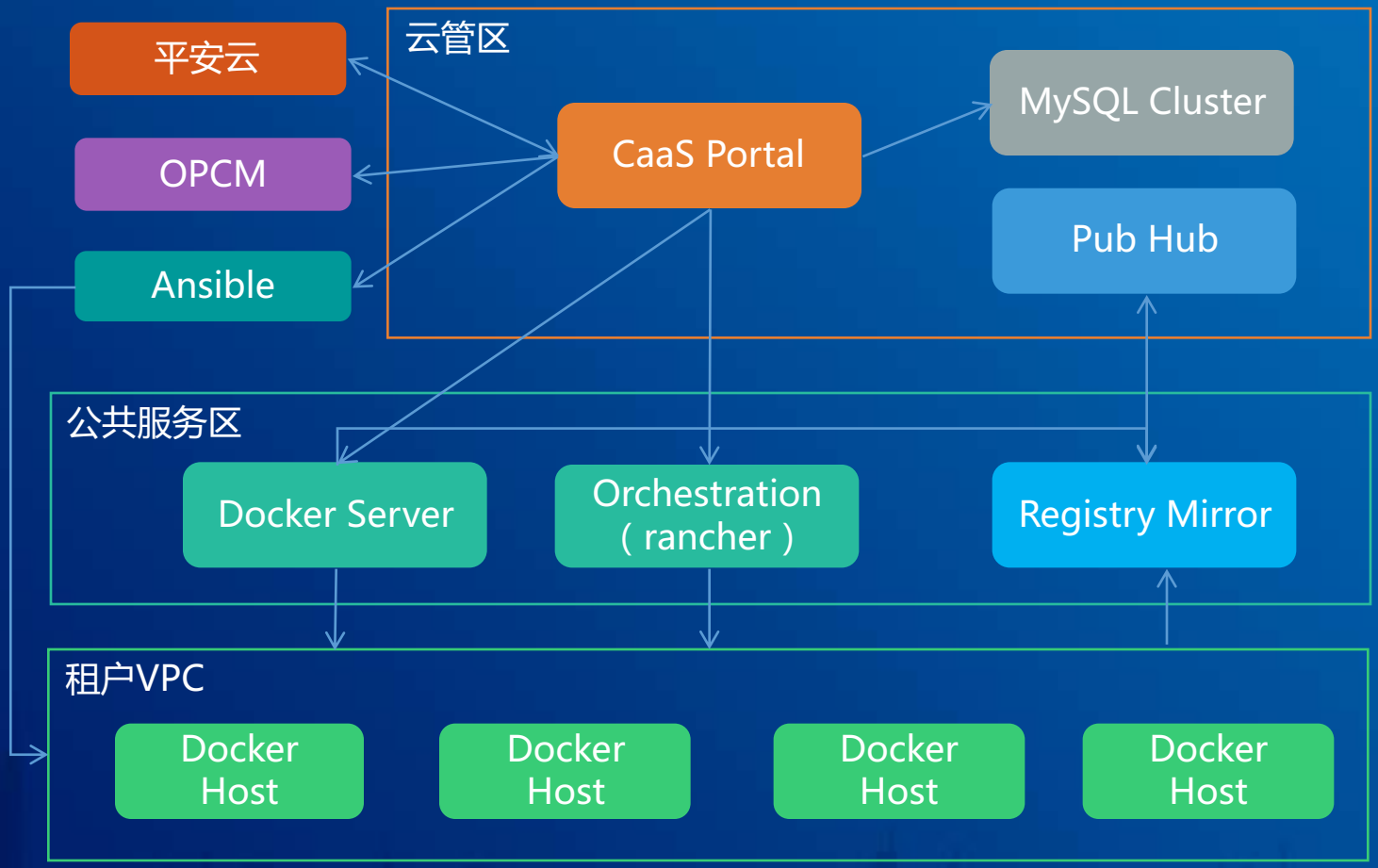
运维世界 Ops World

架构约束

- 同时支持物理机和虚拟机，支持动态添加计算资源
- 优先使用IaaS的弹性计算资源
- 支持多区域数据中心分层架构，统一入口
- 容器平台无法解决的服务需要借助于外部服务，例如防火墙，ADC等
- 容器平台与运维平台（ITIL，监控平台）的集成
- 兼容VPC网络，因此需要采用简易的网络模型
- 利用基础的存储服务实现可靠的弹性存储，例如DNAS



系统架构


平安云
OPCM
Ansible
云管区
CaaS Portal
MySQL Cluster
Pub Hub
公共服务区
Docker Server
Orchestration
(rancher)
Registry Mirror
租户VPC
Docker
Host
Docker
Host
Docker
Host
Docker
Host

服务交付

运维世界 Ops World

镜像仓库

1. 镜像商城：提供多种官方镜像，所有租户均可使用
2. 公共仓库：每个租户拥有自己的公共仓库，租户内用户共享租户内镜像
3. 个人镜像：支持将容器提交成镜像，下载官方和公开镜像

服务管理

1. 详细的服务管理：服务信息、服务事件、服务配置
2. 支持shell、文件上传、镜像制作等扩展功能

新建应用和服务

1. 应用：包含一系列相互关联的服务，这些服务组成一个系统，与RSMS对接
2. 支持Docker ComposeV1编排方式创建
1. 丰富的服务创建配置：支持服务连接、端口映射、环境变量、目录挂载等多种策略等配置。

启动容器服务

1. 对接平安云门户，用户可以一键启用容器服务，在私有的VPC内完成部署。
2. 支持多租户、多数据中心，租户可以选择指定的数据中心启动服务
3. 租户亦可以使用容器平台提供公共租户，也可以单独部署容器服务。

创建容器环境

1. 用户可以根据需求创建多套容器环境，并将自己的计算节点添加到环境中，实现底层资源的弹性扩容。
2. 环境之间资源、服务等完全隔离，仅在管理态存在关联。

使用容器编排

1. 提供常见的编排方案，一键式部署应用
2. 应用和编排相互转，个人编排发布到应用商城

服务交付过程

平台运维

运维世界 Ops World

监控管理

容器底层的主机监控依赖既有的基于zabbix和open-falcon的监控，监控数据推送到EMP上。
容器的运行状态数据直接展现给用户，方便快速诊断，应用层的监控由部署在主机上的监控agent来采集。

日志管理

容器的日志直接展现给用户，容器内进程的日志输出到指定目录，由主机端负责归档和处理。

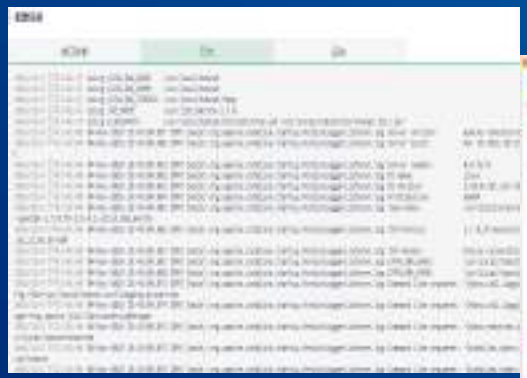
服务管理

容器的增删改查等功能开放到门户上，由用户直接操作，同时提供了SSH可视化。
同时在主机层也提供了一键登录的功能，使用户可以从主机层面通过CLI控制服务。

事件响应

容器服务包含的事件分为平台层和应用层，均通过case系统进行上报处理。

平台运维 - 日志与监控



容器日志

- 容器服务平台日志：本地+云平台ELK日志服务
- 容器自身运行日志：本地云磁盘+云平台ELK日志服务
- 容器内应用日志：业务自行规划，已经提供目录挂载

主机监控

- 主机监控可以通过统一的emp汇总报警信息并查询监控数据
- IaaS层主机则可从云门户直接查看相应的监控项

容器监控

- 容器监控：自研发脚本，提供容器本身的性能监控(cpu/mem/network/storage)，监控平台定时获取，同时，能够在portal上查看
- 中间件监控：提供常见中间件的性能监控(weblogic/tomcat/nginx等)，为中间件镜像制作脚本，中间件监控程序整合到docker镜像中，容器一启动，就能即时上报性能数据到监控平台，无需任何外部干预

平台运维 - 智能化尝试

资源池管理

即时通讯与客服机器人

图式配置信息展示

监控分析与初步诊断

持续优化 - 待完善项

功能优化

编排功能的优化，将架构师输出的架构信息转换为compose文件

图形化编排

应用商城

计费模式的改进

监控检查的准确度和自动处理机制

流程优化

租户自我管理功能强化

与外部流程的对接，固定流程的简化

容器服务应用与运维

01 配置管理

在底层资源实现配置管理的基础上，配置管理主要实现用户应用信息的配置管理

02 扩容缩容

容器服务对运维最大的价值点莫过于可以快速部署、快速扩容，但针对于不用的应用架构，快速扩容的实现方法不同

03 版本发布

基于文件和基于镜像两种部署方式，兼容用户习惯和容器特征

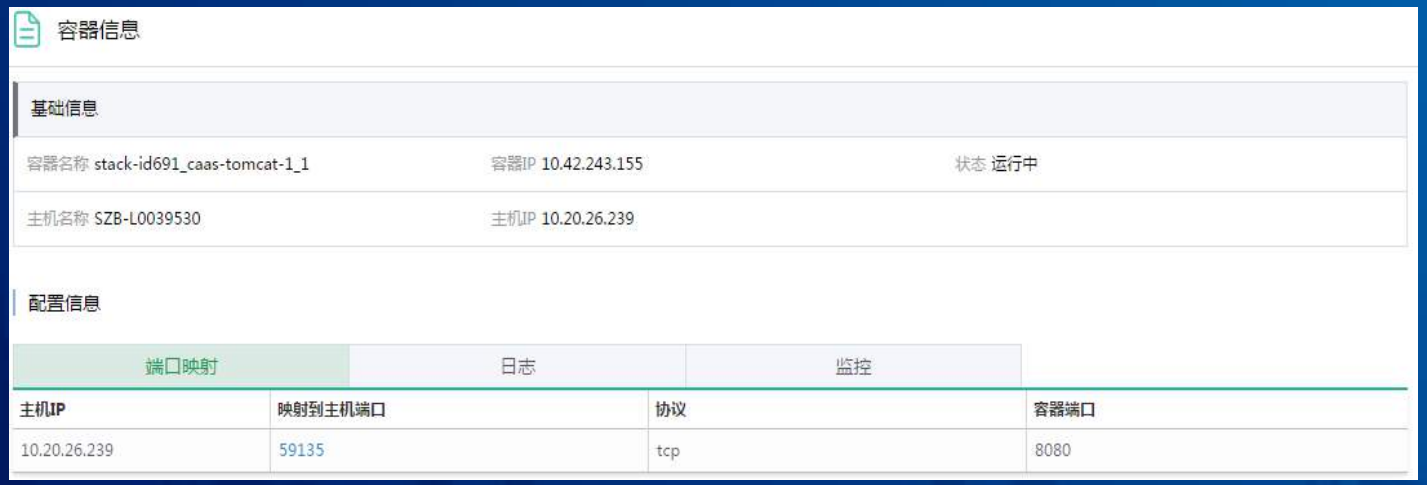
容器服务应用与运维

背景 - 网络方案

容器支持的网络方案有很多种，而且在快速发展中。由于平安云已经有较好的VPC实现，且容器服务作为计算三剑客的一员，需要适配VPC网络，因此在网络方案选择时我们选择了较为成熟和简单的做法。

- 对外：Container Bridge，与外界通讯采用端口映射
- 对内：容器之间采用实现的IPsec隧道实现

每一个容器均可以将其内部端口映射到主机端，容器服务平台负责管理和分配服务端口，确保容器端口不会冲突。目前对于一个服务的多个容器实例，只能有一种端口映射方案。



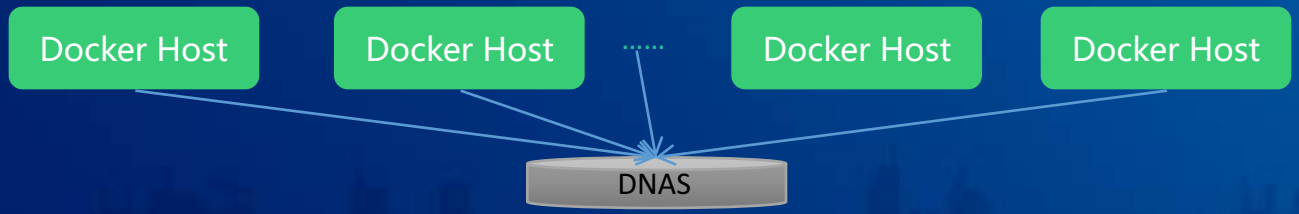
容器服务应用与运维

运维世界 Ops World

背景 - 存储方案

- 镜像容器：采用分层文件系统的方式。考虑到我们需要支持的操作系统类型和文件系统的成熟度，使用devicemapper（direct-lvm）

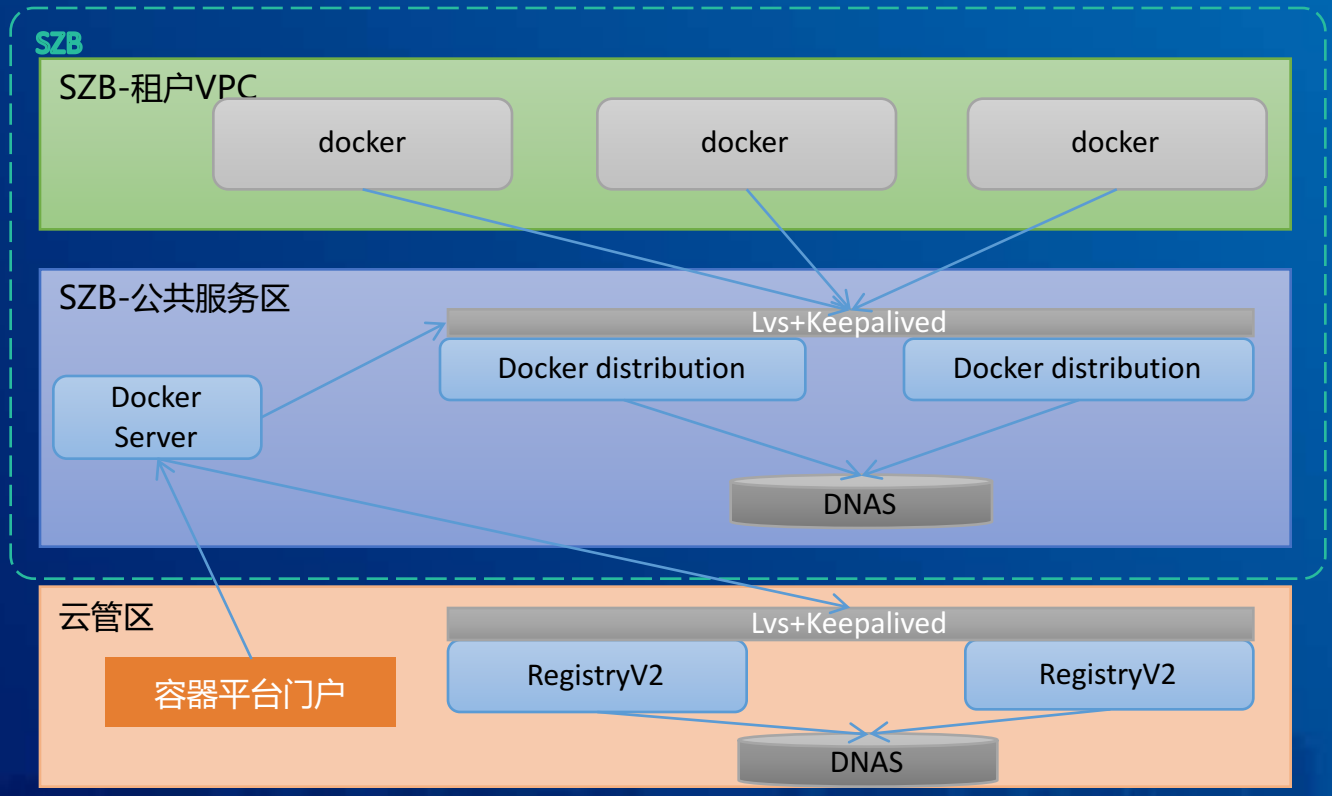
- 应用数据：采用了Volume接口或者直接Volume映射。包含应用包目录，日志目录，应用文件目录。在生产环境，我们将应用包目录部署在高冗余度的DNAS设备上，支持容器迁移和扩容。不需要迁移的目录在落在主机本地磁盘上。



容器服务应用与运维

背景 - 镜像库方案

- 由于平安云容器服务是跨机房部署的，因此分为两个管理层级，在镜像库管理和镜像更新过程中，会按照区域和镜像类型、活跃度进行提前推送以节省空间和时间，



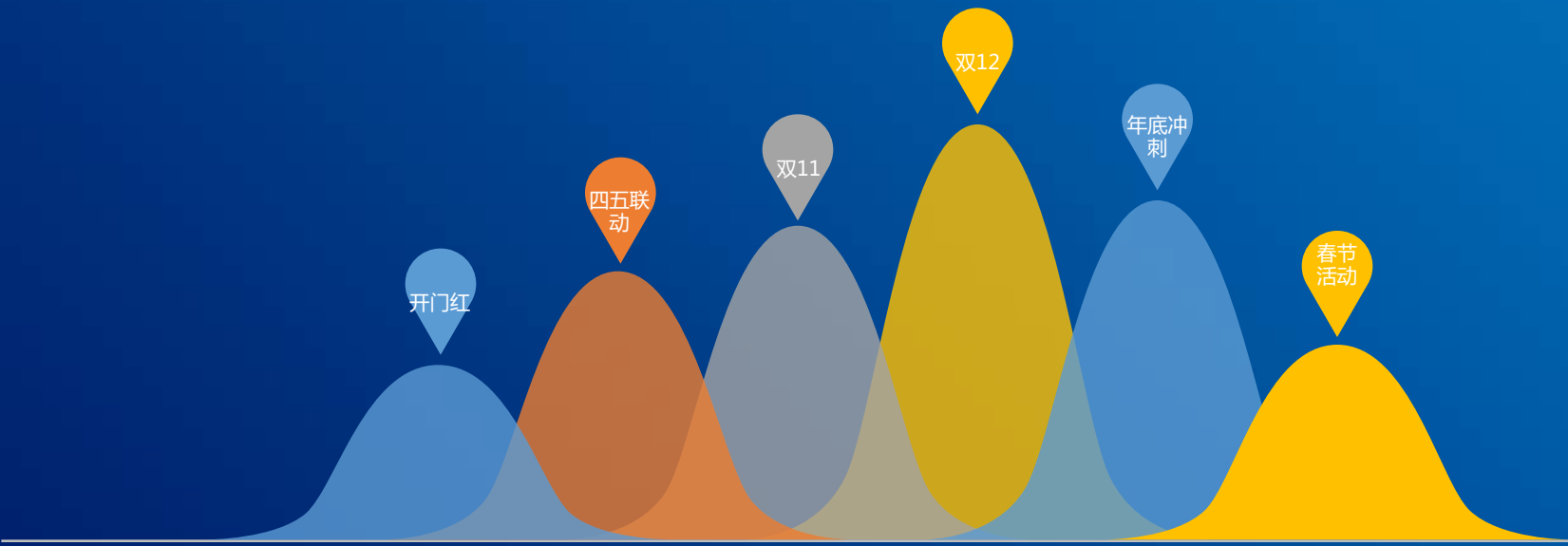
应用运维 - 配置管理

容器实例是最小的配置项

在容器实例创建时统一命名且终生不变。由于容器必属于服务，且一个服务下的容器具备相同的功能，因此服务共同的属性记录在服务配置项中。
对服务的修改不影响容器实例的配置更新，容器实例仅在新建、删除时存在变化。

所有这些配置信息以容器服务平台纪录的为准，但会把与非容器有关的部分同步到CMDB中供其他用户和平台查阅。

应用运维 - 扩容缩容



金融业务系统大多数情况下负载稳定，具备典型的双驼峰特性。但随着部分业务系统的互联网化，在每年的若干高峰期会存在非常迫切的扩容需求。

如果应用架构不做调整，扩容最直观的方式就是针对负载均衡后的集群增加实例，由容器编排平台进行新实例创建和负载均衡配置调整。为了简化步骤，新实例外调防火墙需要提前开通或者通过NSP平台开通。

简化的做法还包括不实用DNS（如何DNS服务没有自动化的话），避免weblogic等中间件运行后修改配置，启动热部署等做法。

扩容的另一个关键性用途包括服务克隆功能和灰度发布、流量路由功能。

应用运维 - 版本发布

基于文件

容器服务允许用户向已经部署好的服务中上传应用包并远程执行命令，容器所在的主机也具备完整的目录结构可供部署平台推送应用包，因此基于文件的版本发布流程可以和非容器流程完全相同，通过DPM平台启动版本发布。

用户也可以针对开发环境直接上传文件到主机并映射到容器内，通过此种方式，容器更像是一个普通的进程。

基于镜像

自动化部署流水线支持自动打包和制作镜像，通过此种方式，可以一次性部署完整的服务，版本以镜像的形式存在。其他用户则可以在容器服务门户中选择编排，重新部署一套完整的应用。

用户也可以通过上传文件完成调试后提交镜像，将改动更新到镜像库中。

运维世界
Ops World

THANKS