GOPS 2021
Shenzhen

GOPS

GOPS 全球运维大会

2021
-XOPS 风向标

深圳站

中国·深圳

指导单位：

主办单位：

时间：2021年5月21日-22日

GOPS 2021
shenzhen

移（tǎng）动（zhe）运维那些事儿

陈大伟　　华夏银行云计算平台负责人

陈大伟

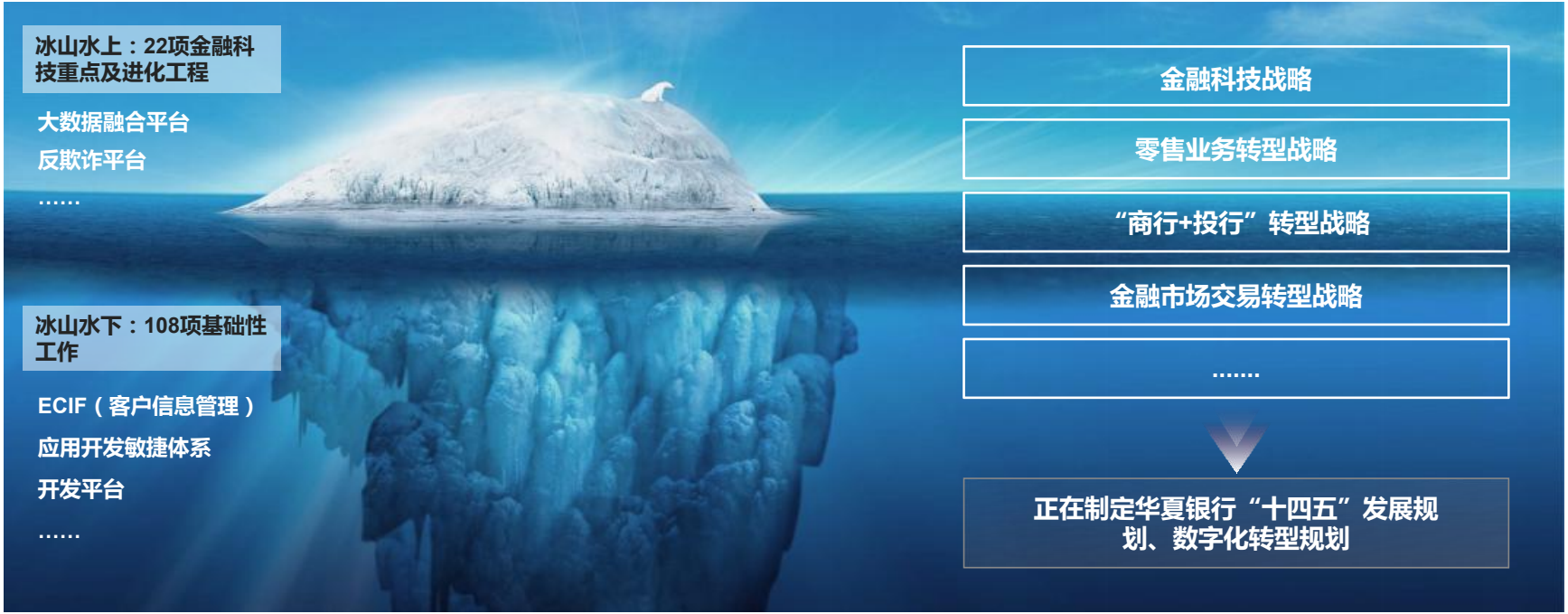
云计算平台负责人

15年来一直从事it基础平台规划、建设及运维相关工作，有着丰富的主机、存储、虚拟化及云平台相关运维经验，目前任华夏银行云计算团队负责人。

原先题目

华夏银行战略

科技战略-冰山工程



- 金融科技战略
- 零售业务转型战略
- “商行+投行”转型战略
- 金融市场交易转型战略
- ……

正在制定华夏银行“十四五”发展规划、数字化转型规划

目录
CONTENTS

1 站着运维

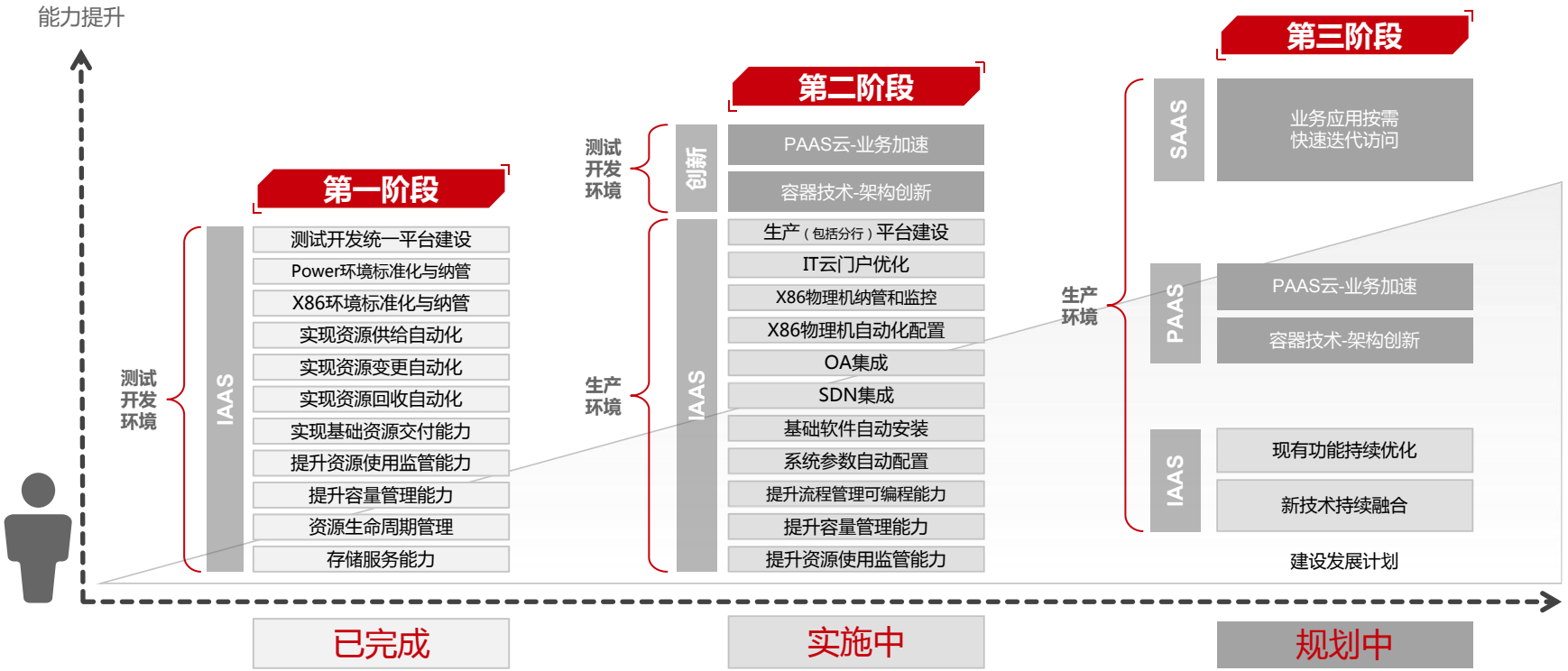
2 坐着运维

3 躺着运维

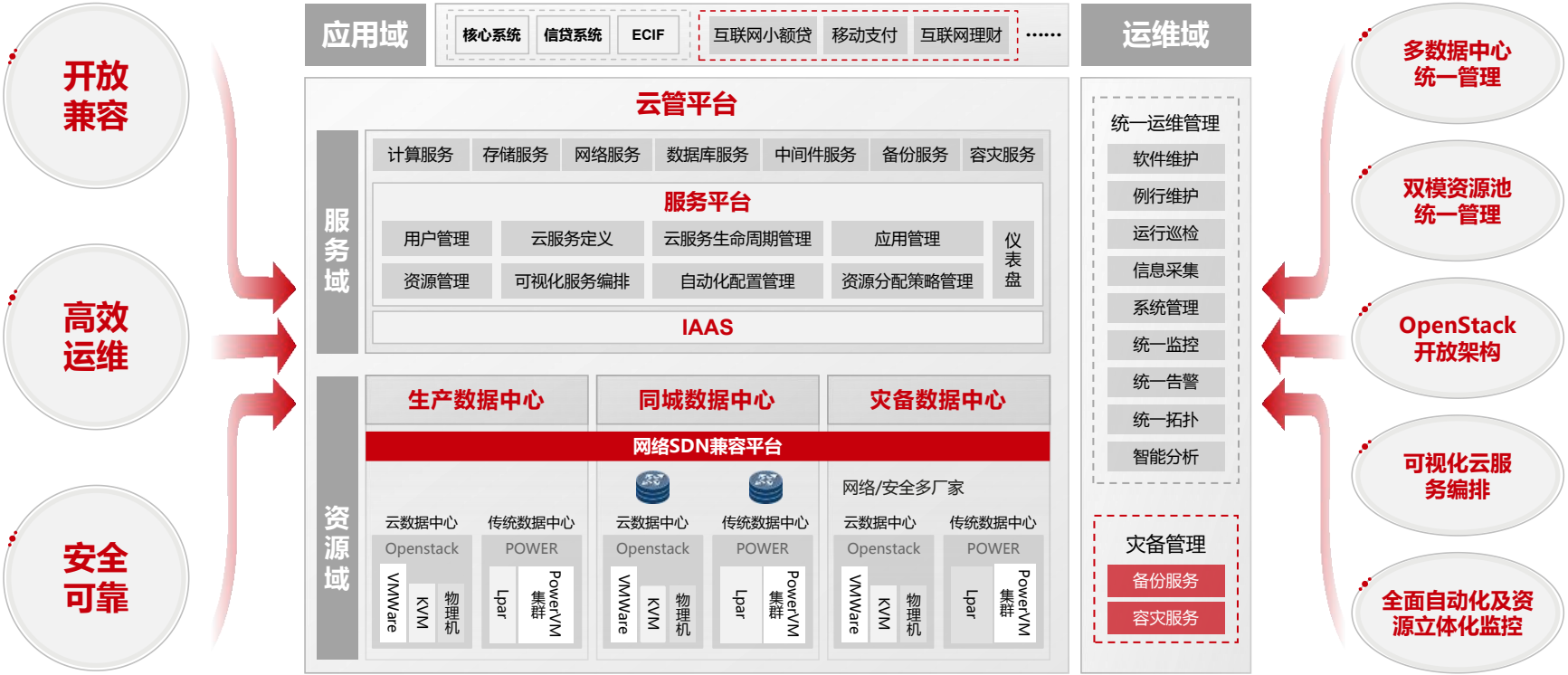
站着运维

01

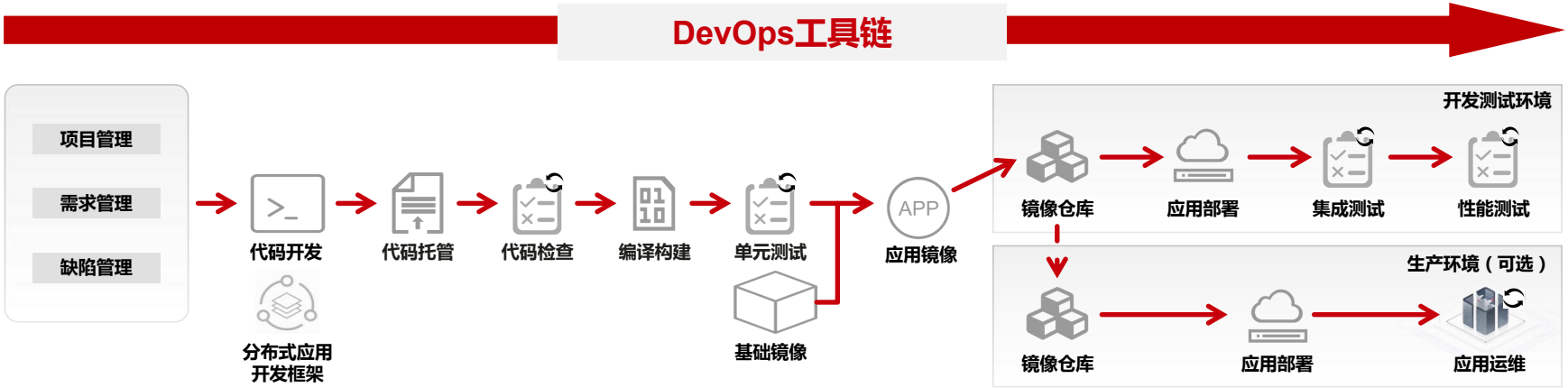
华夏银行的金融云建设之路

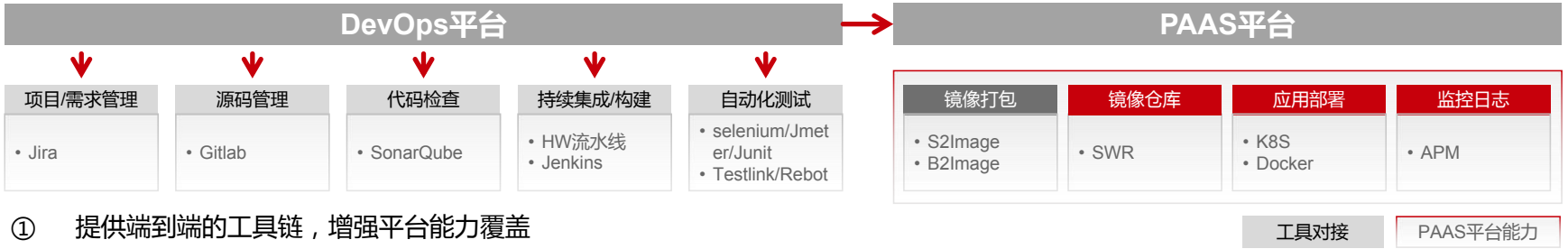


华夏银行金融云全景图


开放兼容
高效运维
安全可靠
应用域
核心系统
信贷系统
ECIF
互联网小额贷
移动支付
互联网理财
……
运维域
云管平台
服务域
计算服务
存储服务
网络服务
数据库服务
中间件服务
备份服务
容灾服务
服务平台
用户管理
云服务定义
云服务生命周期管理
应用管理
仪表盘
资源管理
可视化服务编排
自动化配置管理
资源分配策略管理
IAAS
资源域
生产数据中心
同城数据中心
灾备数据中心
网络SDN兼容平台
网络/安全多厂家
云数据中心
传统数据中心
Openstack
POWER
VMWare
KVM
物理机
Lpar
PowerVM集群
统一运维管理
软件维护
例行维护
运行巡检
信息采集
系统管理
统一监控
统一告警
统一拓扑
智能分析
灾备管理
备份服务
容灾服务
多数据中心统一管理
双模资源池统一管理
OpenStack开放架构
可视化云服务编排
全面自动化及资源立体化监控

华夏银行云原生DevOps平台





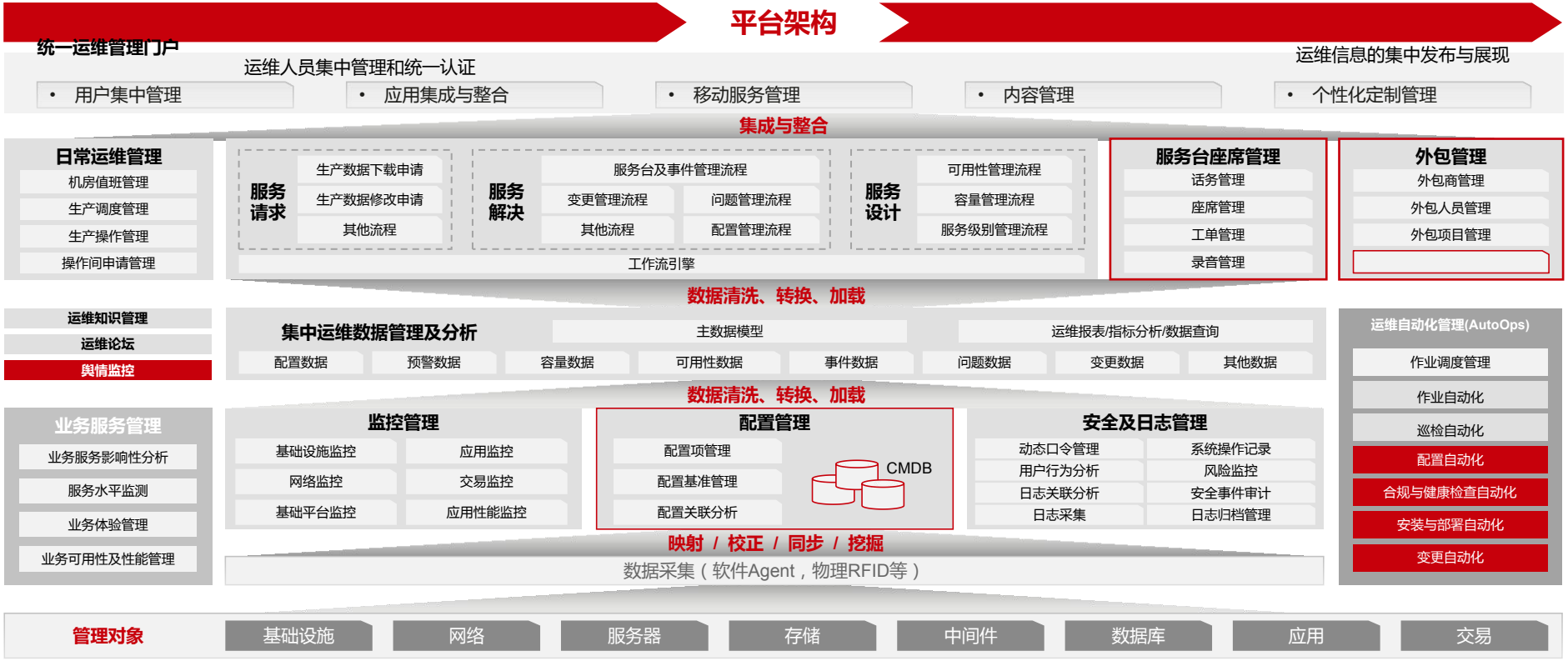
① 提供端到端的工具链，增强平台能力覆盖

② 组件基于行业流行组件，拥抱开源，提高技术复用性

云原生平台规划-云原生平台功能架构

1. 构建统一的服务网格容器平台
2. 基于现有云管平台（云魔方），整合云原生运营能力（资源发放）。
3. 统一云原生运维监控（MO）
4. 与现有DevOps平台对接，搭建云原生CI/CD流水线，。

云运维平台


平台架构
统一运维管理门户
运维人员集中管理和统一认证
• 用户集中管理
• 应用集成与整合
• 移动服务管理
• 内容管理
• 个性化定制管理
运维信息的集中发布与展现
集成与整合
日常运维管理
机房值班管理
生产调度管理
生产操作管理
操作间申请管理
服务请求
生产数据下载申请
生产数据修改申请
其他流程
服务解决
服务台及事件管理流程
变更管理流程
问题管理流程
其他流程
配置管理流程
服务设计
可用性管理流程
容量管理流程
服务级别管理流程
工作流引擎
服务台座席管理
话务管理
座席管理
工单管理
录音管理
外包管理
外包商管理
外包人员管理
外包项目管理
数据清洗、转换、加载
运维知识管理
运维论坛
舆情监控
集中运维数据管理及分析
主数据模型
运维报表/指标分析/数据查询
配置数据
预警数据
容量数据
可用性数据
事件数据
问题数据
变更数据
其他数据
运维自动化管理(AutoOps)
作业调度管理
作业自动化
巡检自动化
配置自动化
合规与健康检查自动化
安装与部署自动化
变更自动化
数据清洗、转换、加载
业务服务管理
业务服务影响性分析
服务水平监测
业务体验管理
业务可用性及性能管理
监控管理
基础设施监控
应用监控
网络监控
交易监控
基础平台监控
应用性能监控
配置管理
配置项管理
配置基准管理
配置关联分析
CMDB
安全及日志管理
动态口令管理
系统操作记录
用户行为分析
风险监控
日志关联分析
安全事件审计
日志采集
日志归档管理
映射 / 校正 / 同步 / 挖掘
数据采集（软件Agent，物理RFID等）
管理对象
基础设施
网络
服务器
存储
中间件
数据库
应用
交易

坐着运维

02

云架构规划蓝图-实现业务敏捷的统一平台

GOPS 2021 shenzhen

一套云管，双核架构

规划要点

1. 云管理平台：才艺展示的地方，包括资源管理、编排、流程、自动化、审计、计费等等
2. 云计算平台：稳定运行，虚拟化、容器、分布式、软件定义、sdn等等，提供核心能力，不能出问题
3. 云运维平台：监控、故障诊断、日志分析、自动化运维、应急处置、以及移动化展示

为什么提出云运维平台的概念

一、资源统计和展现

为什么提出云运维平台的概念

GOPS 2021
shenzhen

二、架构复杂、运维困难

没经历过这种场面的运维人员，他的职业生涯是不完整的。

十年之前，我不认识你

十年之后，我认不出我

招聘要求

1. 至少精通一种开发语言(JAVA、COBOL、C++、C、Python等），具有5年及以上系统开发经验；
2. 2、精通所负责系统的架构设计，能够根据产品状况提出项目的总体/专项解决思路框架；
3. 具备丰富的系统设计经验，精通高可靠、高负载、高并发的技术架构；能够对系统架构和性能设计提出建设性意见，并落地实施。
4. 精通AIX/LINUX操作系统、Oracle/Mysql数据库、Vmware虚拟化存储、Cloud云计算、网络虚拟化（Virtual）、容器、SDN/NFV等基础软硬件平台、网络、运维等相关主流技术
5. 精通分布式服务主流技术框架，拥有大型分布式系统的高并发、高负载、高可用性设计能力。
6. 具备丰富的大规模系统/机房/网络/数据中心规划、部署、运维能力，精通运维领域相关技术原理，能够独立组织、完成大规模升级、演练工作。

实际工作

word、excel、ppt、Visio、Xmind、Project...
立项报告、会议纪要、统计数据、监管报送、变更方案、制度流程、应急演练.....

躺着运维

03

系统简介

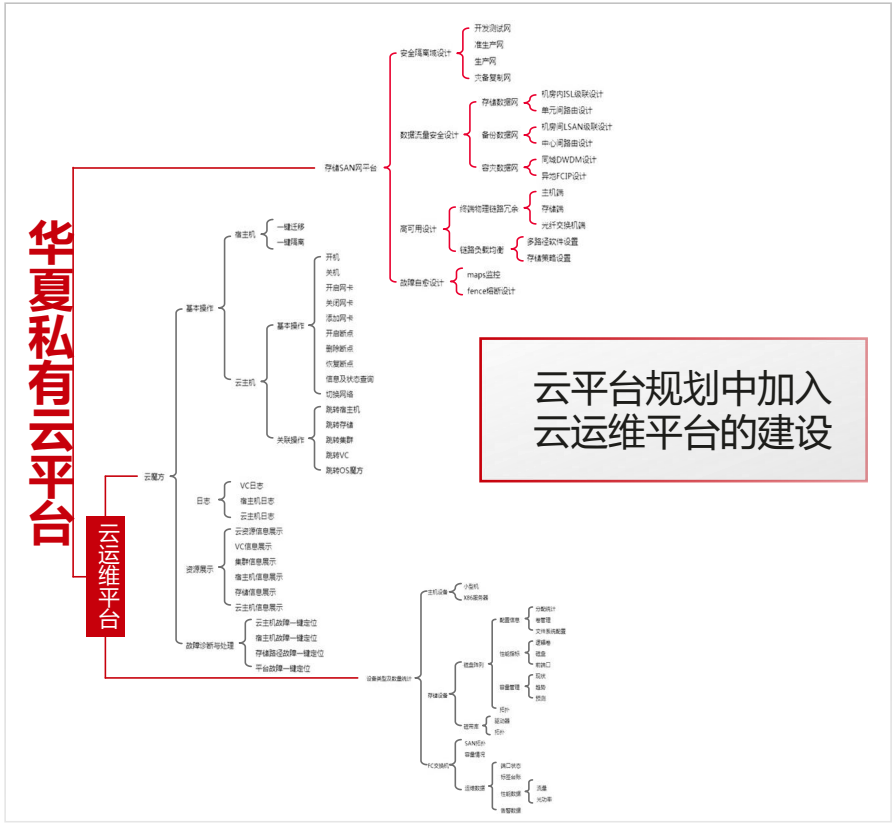
云魔方运维服务平台

设计初衷：被动变主动

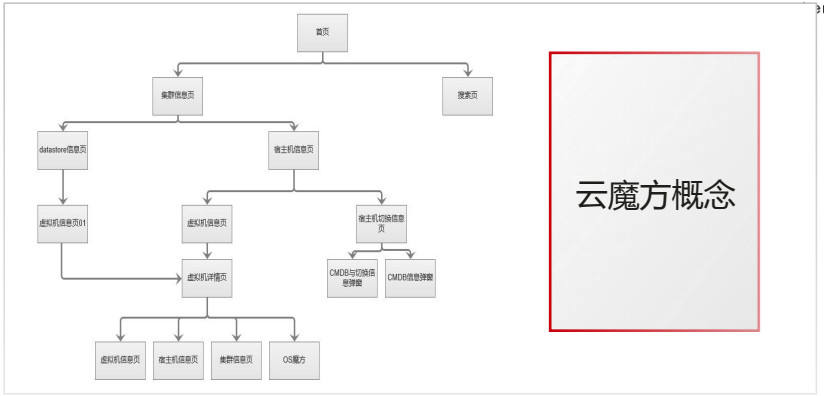
目标定位

信息查询、故障定位、日志采集、
数据分析、应急处置...

华夏云运维平台建设



云平台规划中加入
云运维平台的建设



云魔方概念

移动端流程

功能描述

i掌运入口、首页虚拟数据中心和搜索

- 统一入口
- 常用信息首页展示
- 任意匹配关键字搜索

功能描述

云主机基础操作、性能和快速通道

- 基础操作：对主机、存储网络的各种快速应急操作；
- 快速通道：快速跳转到云魔方或其他魔方相关页面。

功能描述

性能图表展示

- 性能：cpu、内存、存储、网络等常用性能指标；

功能描述

宿主机宕机分析流程

- 故障点逐级定位
- 恢复状态随即可查

功能描述

主动检查

- 各个维度深度巡检

功能描述

正常流程

- 按照资源部署架构逐级下探
- 静态数据每日和cmdb同步更新

应用架构和技术栈

微服务架构

1. 项目采用Spring Boot + Spring Cloud + VUE 微服务架构设计。可以使后台能更好的追求高并发、高可用、高性能，Spring Boot 的开发风格可以做到一键启动和部署。帮助开发人员构建有弹性的、可靠的、 协调的应用程序。开发者很容易入手并快速应用于生产中。

前后端分离

1. 彻底解放前端，前端不再需要向后台提供模板或是后台在前端HTML中嵌入后台代。
2. 提高工作效率，分工更加明确。前端只关注前端的事，后台只关心后台的活，两者开发可以同时进行，在后台还没有时间提供接口的时候，前端可以先将数据写死或者调用本地的JSON文件即可，开发更加灵活。
3. 降低维护成本，代码重构及可维护性增强。
4. 实现高内聚低耦合，减少后端（应用）服务器的并发/负载压力。
5. 即使后端服务暂时超时或者宕机了，前端页面也会正常访问，但无法提供数据。
6. 可以使后台能更好的追求高并发、高可用、高性能，使前端能更好的追求页面表现、速度流畅、兼容性、用户体验等。

应用架构和技术栈

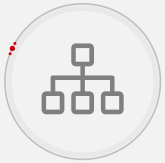
GOPS 2021
shenzhen

微服务架构

应用架构和技术栈

GOPS 2021 shenzhen

技术栈



项目框架
SpringBoot

项目框架
SpringCloud

ORM框架
MyBatis

数据库连接池
Hikari

数据缓存
Redis

注册中心
Eureka

消息中间件
kafka

语言
JAVA

接口文档
Swagger2

数据库
oracle

反向代理负载均衡
Nginx

安全控制

1 i掌运魔方二次验证

- 前端通过cookie获取token及username。
- Java后端将token作为参数调用i掌运指定接口获取用户信息。
- Java解析接口返回数据，通过数据中的username与前端cookie中获取的username对比，相同则放行，不同则拦截。

2 操作权限

主要分为三类，用户通过不同权限可以访问不同的功能：

查询类权限

操作类权限

巡检操作权限

安全控制

3 数据加密

- 采用AES算法对数据鉴别处理，保证重要信息不被非法插入、篡改、删除、更换次序，实现传输数据的完整性和正确性。
- 后端向前端传输数据会通过html转码，以防止跨站脚本攻击。

4 增加白名单

- 通过创建一份合法的资源列表（白名单），并且规定用户只能选择其中的文件名、协议和路径等，通过这种方式，可以控制用户不能直接访问资源。

安全控制

5 配置文件加密

- 将配置文件中的数据库、redis等密码，通过jasypt进行加密，避免配置文件中出现明文密码。

6 防SQL注入

- 使用参数化语句，进行sql语句查询。
- 不使用拼接SQL语句进行数据库查询。
- 增加Xss过滤器防sql注入。

数据存取

优化数据存取，让我们获取数据更加快速、稳定和安全。

- 日志通过kafka实时接收，通过正则表达式匹配到目标数据，进行批量入库处理，将报警信息快速展示在页面中，Kafka可以处理实时数据管道，也能够处理高速和大容量的数据。能够支持每秒数千条消息的消息吞吐量，消息复制是持久性的原因之一，因此消息稳定且永远不会丢失。
- 通过多线程定时从cmdb采集全量数据，多线程能使我们的程序更快相应，大大缩短采集数据的时间。
- 通过Spring定时任务，完成对虚拟化数据的定期更新、清理和数据库备份等操作。
- 一些常用的数据和一些数据量大且不经常变更的数据，我们将其放入redis中，可以减小数据库压力，也可以增加程序的访问速度。
- 通过优化sql和建立索引，使我们在获取数据时速度更快，能更好提高用户体验。
- 通过对特定的数据进行加密处理，可使我们的数据安全得到保障。

魔方家族

wán 完

GOPS 2021
shenzhen

Thanks

高效运维社区

开放运维联盟

荣誉出品