

# 2019云规划（思路篇）

# 目录

- 一、使用公有云趋势及必要性
- 二、公有云的局限
- 三、私有云建设演进
- 四、IT治理与云管理能力
- 五、建议分阶段建设目标

# 一、使用公有云趋势及必要性

- 2017-2018年，公有云市场急剧演进
- 公有云不再是互联网公司的专用（视频、游戏、电商、社交等APP）
- 公有云不再是中小企业节省成本的起步选择（网站、OA、邮箱）
- 目前所有的Enterprise即大型企业都在使用公有云
  - 灵活的成本管控，OPEX方式支出资产，比自建IDC买服务器便宜很多
  - 相对灵活的策略，按年付款可享受良好折扣，按月付款可随时terminate资源
  - 随时获得异地数据存储和调用（多机房多可用区域），切换应用系统部署的地域成本极低，不用在大量拉专线异地建机房
  - 企业在重新评估核心应用和重要应用的范围，不再保护之内的应用都逐渐下放公有云

# 一、使用公有云趋势及必要性

- 新一代企业应用，包括To-B/To-C类型，诞生和起步就在互联网公有云，普遍应用原生的PaaS层开发技术，包括但不限于如下：
  - 微服务开发架构，比SOA更彻底的拆分，软件结构为数个服务中心（Docker或IaaS虚拟机）
  - 消息总线产品（MQ类）
  - 缓存产品（Redis等）
  - 分布式与负载均衡，可以支持数十个应用服务器分布运行（SLB）
  - 外网流量缓存和卸载（CDN、SLB）
  - 海量数据保存（OSS对象式存储）
  - 轻量级/分布式数据库（MySQL RDS或DRDS）
  - 容灾（数据备份到异地，归档OSS，Multi-Tier Store）
  - 自动调度类功能

# 一、使用公有云趋势及必要性

- 现有To-BT类应用，非关键业务正向着公有云迁移
  - 上云依然是IaaS类虚拟机应用，属于垂直式的烟囱式应用
  - 扩展只能Scale-up，向上升级主机规格
  - 一般到双机或着四节点就达到最大化，主备为主
  - 数据库一般为单机或集群高可用版本，不能分
- 以ERP（SAP HANA）开发测试为代表的公有云使用需求变得典型和常见
  - ERP属于核心应用的，但开发测试环境一般无敏感信息
  - 开发环境通常要求短周期，3-6个月，最大1年，符合云的弹性能力要求，选择公有云灵活方便

# 一、使用公有云趋势及必要性

- 在公有云上供应物理机（裸金属或者其他称呼）的服务方式变得流行：
  - 性能高，机器配置较新，通常为Xeon V5
  - 用户独占所有资源，无虚拟化，可充分跑出所有压力
  - 不存在公有云的技术干扰，如虚拟化的限制、虚拟网络配置的限制，用户可自行配置希望的技术架构和实现，包括买物理机自行配置虚拟化
  - 满足GPU等特殊场景
  - 与云资源平滑对接，与用户自己的公有云VPC虚拟网络互通无问题

# 一、使用公有云趋势及必要性

- 几点小结和一些Point：
  - 1、公有云对大企业极其普遍，不再拒之门外
  - 2、应用开发如能彻底转向原生的互联网分布式架构，更适合跑在公有云上
  - 3、现有传统应用继续只能以虚拟机方式迁移上云，架构无法重构，但迁移相对简单
  - 4、下放非关键应用到公有云降低成本
  - 5、物理机提供方式逐渐普及，满足定制化需求

## 二、公有云使用局限

- 公有云产品能力各不相同，特色不同，差异较大
- 功能项满足程度不一样
  - 可任意定制的能力（操作界面限制，规则填写配置的限制）
  - 跨可用区配置能力（网络、调度、融合网络）
  - 高可用能力（副本，有效性99.999999的9数量）
  - 代码兼容性（SQL等）
- UI操作风格不一样
- 稳定可靠程度不一样

## 二、公有云使用局限

- 上云容易下云难，切换到其他公有云不易
  - 各厂家设置技术门限，数据导入容易，导入时候，存在多种限制
    - 数据访问方式的限制
    - 读取限制速度
    - 费用计量限制
    - 数据格式限制
  - PaaS类互联网分布应用下云难度较大
  - IaaS类老应用，以虚拟机方式迁移难度较低

## 二、公有云使用局限

- 公有云厂家深度定制的产品下云无解决方案
  - 数据库等保存持久数据的定制产品（非标准MySQL/Oracle）下云难度最大，下云后业界没有同等解决方案
  - 下云意味着重构应用，换应用底层接口，更换其他开源组件实现，或商用组件实现
  - 下云过程无技术支持，应用开发周期长，风险高
  - 选择特定产品，一般意味着一旦上云就无法下云，除非以后另行建设私有云，使用全自主架构，再去做整体迁移和切换
  - 以DRDS分布式数据库为代表产品

## 二、公有云使用局限

- 费用急剧膨胀，规模蔓延，降低不下来
  - 公有云使用容易产生一定的随意性
  - 付款方式也不是企业以往的预算-规划-招标-执行-财务控制-风险金（一定比例）
  - 前期规划的投入金额可能以预想的几倍的速度飞速消费
  - 计费方式过于灵活，一种服务可能有5种计费方式，不尝试下，往往不能确定最优惠的，例如
    - 按百万次访问次数，按流量，按单次访问大小，按时间，按小时实时计费，以及以上几种混合
    - 选择预付费包年包月的方式较稳定，无财务测算的风险，但往往单价价格又贵

## 二、公有云使用局限

- 数据被窥探的风险
  - 硬盘文件全透明，所有虚拟机都带有云厂家的Agent，做扫描硬盘，杀毒，防木马，硬盘被看光
  - 网络流量全透明不加密，企业内网流量随意mirror做netflow分析
  - 磁盘落地全透明不加密
  - PaaS层数据更容易被采集，例如用公有云RDS数据库，所有数据结构化，极其适合被批量便利扫描
  - 安全系统总控后台不属于用户管辖，例如数据库审计产品，只记录用户访问，对公有云平台的运维管理员操作是透明的

## 二、公有云使用局限

- 几点小结和一些思路：
  - 1、确定应用和软件技术架构后，再去找对应的产品
  - 2、尽量选标准化的PaaS层架构做软件开发，未来切换云技术风险低
  - 3、确定几大公有云的核心产品技术特点，做好上云、下云的长期规划
  - 4、做好核心产品的备选方案，遇到技术问题无法攻克有退路
  - 5、按使用量计费的要谨慎，多方评估后，给出使用量最好和最坏情况后，再确定预算。
  - 6、提前了解部署模式等可能设计技术方案和所选产品改造的问题，降低实施风险
  - 7、核心应用数据隐私面前选择私有

## 三、私有云建设演进

- 商用系统占有稳固
- 开源系统给了企业第二选择，但未对商用产品形成替代，许多公司采用多种技术路线并存的方式，存量依然使用商用产品
- VMware始终排在行业No.1
- Xen/Xen Server基本退出市场竞争
- Hyper-V/Windows Server 2016未看到较大规模的增速

## 三、私有云建设演进

- Openstack开源版本迭代迅速，功能上主要发展广度，新模块急剧增加，但部分核心模块的功能完善度依然不足
- Openstack社区供应来源从几大Openstack发行版公司变化为硬件厂家（华为等）和超大型用户自身贡献（中国移动等）
- 业内主营业务为纯Openstack生态的公司面临较大压力和挑战
- 大量公有云厂家落地推出私有云版本
  - 阿里Zstack、飞天
  - 金山Kingstack、银河
  - Ucloud - Ustack等

## 三、私有云建设演进

- 以Openstack建设私有云主要考量点：
  - 是否稳固，踩过了那些坑，修改了那些Openstack社区版本的bug
    - KVM稳定度/性能/虚拟机溢出等安全问题
    - Ceph分布式存储性能/稳定性/安全性/备份/复制/容灾能力
    - 组网灵活度，跨数据中心/可用区/负载均衡
    - 网络吞吐性能，10GE以上的技术如25G接受度
    - 架构冗余能力

## 三、私有云建设演进

- 以Openstack建设私有云主要考量点：
  - 功能是否完善，大量新功能依赖后期开发
    - OSS对象存储等技术和应用系统的对接
    - RDS等不同场景的服务构建、性能、功能、容量、管理
    - 安全类产品在私有云中的嵌入，包括流量的防护和清洗，堡垒机产品的自动融合等

# 三、私有云建设演进

- 以Openstack建设私有云主要考量点：
  - 管理的完善度
    - 服务目录的定义和展示
    - 计费模式的要求
    - 账单呈现的要求
    - 审批流程
    - OA等系统对接
    - 自助管理要求
    - 多云管理的要求

## 三、私有云建设演进

- 推进并影响私有云建设的因素
  - Docker和CI/CD普及难度大，开发体系全面替代性升级困难
  - 自动化运维尚未成熟，大部分系统以监控展现为主，自动触发调度在技术上和业务上还有普遍性推广的难度

## 四、IT治理与云管理能力

- 运维技术层面价值
  - 生命周期管理定义，资源申请和分配的监管、追踪和回收
  - 服务目录标准化，云服务配置规格标准
  - 计费 and 成本核算，投入的云资源匹配到项目和部门
  - 管理流程、审批的自动化审批
  - 技术操作开通自动化，管理复杂度降低，技能要求降低
  - 公有云和私有云同流程统一纳管

## 四、IT治理与云管理能力

- IT治理更高价值：
  - 从成本中心转型向利润中心
  - 一致的门户，对业务部门和使用者的形象展示
  - 运维大屏幕展示，核心数据和决策价值

## 四、IT治理与云管理能力

- CMP建设思路和路线
  - 深度和广度两条线
  - 深度：单个产品功能项的API打通，对云原生功能在CMP上的复现程度
  - 广度：接入产品的数量
- 两种对接思路
  - 重资源操作，侧重产品接入数量，各产品配置和运行性能监控从API完全取值展现
  - 重流程管理，侧重产品门户、定义、申请、计费，详细复杂技术管理部分下方到云自带的控制面板上配置

## 五、建议分阶段建设目标

- Phase 1 新一代云战略制定
- Phase 2 公有云调整 (Transformation)
- Phase 3 CMP平台建设
- Phase 4 私有云下一代演进和迁移

# 五、建议分阶段建设目标

- Phase 1 新一代云战略制定
  - 业务系统落地需要哪一种云服务，目标云功能
  - 公有云国内、国外合作策略
  - 自我可控、合规和安全的强制要求及私有云目标
  - 统一开发云门户及管理平台（CMP）的目标
  - 其他运维管理工具、系统、及人工支持的目标

## 五、建议分阶段建设目标

- Phase 2 公有云调整 (Transformation)
  - 公有云产品功能、路线、服务规格的选型和扩容
  - 云间专线
  - 数据备份/容灾
  - 上下云迁移与整合

## 五、建议分阶段建设目标

- Phase 3 CMP平台建设
  - 运营管理目标的落地
  - 统一门户建设
  - 流程建设
  - 计费和账单的启动
  - 各云API打通
  - 数据拉取和报表展现

## 五、建议分阶段建设目标

- Phase 4 私有云下一代演进和迁移
  - Next Generation 下一代私有云建设，关键功能和厂家选型
  - 现有私有云迁移调整
  - CMP对接
  - 长期功能演进维护
  - 日常运营维护管理