专家问诊

问题	专家回复
我们银行原来重要的数据和应用都是存在本地数据库，数据库都是很老的了，而且数据量也很大，迁移到云端会有很多风险，有什么办法可以保障迁移安全呢？	数据和应用的上云迁移，是一个系统化工程，需要从方方面面来综合考虑，IBM经过这么多年的运维管理实践，有一套成熟的评估模型和策略体系来看迁移是否可以做。如果可以做，中间的哪些环节需要重点考虑，都会有哪些风险。从以往的案例中，在设计，部署和迁移演练等环节非常重要，从安全角度来看我们可以从网络安全，工具安全，数据传输安全，平台安全等几个方面来考虑。
目前已有运维管理平台，配置库，监控平台，作业平台等管理平台，考虑到与现有平台对接，建设多云管理平台时需要注意什么？	多云管理平台是一个统一的完整的可以跨多平台，多云和多集群环境的可视化管理平台，在未来的混合多云，敏稳双态架构下进行简单化操作管理。可以从这些方面来考虑它的建设性。
云厂商提供的都是流水，但是云资源的具体成本支出并不了解，每个月的IT预算都超了，是否可以进行成本优化，或者资源评估，到底那些钱花的值，有方法可以直观了解吗？	混合多云环境下的资产治理模型不仅支持查看多 个公有云成本，还支持查看私有云成本。鉴于公有云服务种 类繁多，因此在治理系统中了解所使用的各种云的成本很重 要。系统必须满足各项企业需求，如数据安全性、基于角色的访问控制以及将成本分摊至各部门。利用IBM多云成本与资产管理的解决方案，提供了跨多个提供商使用云服务的规范化视 图，有助于提供企业所依赖 的安全性、可扩展性和用户管理功能。它支持基于预算和财 务控制，为采购的云服务提供强大的治理模型另外，该服务 还支持按计费制和用量制分摊云服务成本。
云管平台、流程管理、应用管理等不同管理平台是否可以合一进行管理呢？优劣势都有哪些呢？	云管平台从狭义上讲是一种云资源管理平台，经过这些年的发展，无论是从技术创新还是业务需要，已经发展成综合性的管理平台，也就是广义上说的完整的可视化管理平台，它集成了ITSM流程服务管理，事件监控告警管理，敏捷开发运维管理等能力，在OSS与BSS均有加强和延展。IBM的混合多云管理平台提出了134概念：1个平台，3个层面（业务，编排与自动化，运营与运维），4个组件（自助订阅，DevOps，运营控制台，治理控制台），很好诠释了中间的优劣势。

专家问诊

问题	专家回复
核心应用一般会部署在集中式架构上，创新应用会部署在分布式架构上，两种架构如何更好的集成呢？	企业在发展过程中，会有相当长的一段时间处于传统架构与云架构并存的混合IT架构环境。传统架构关注的是可靠，稳定，是稳态环境，多部署核心应用，是集中性的管理运维模式；云架构关注的是便捷、快速、迭代，追求数字化创新，打造微生态，是分布式的管理运维模式；两种架构需要从人员与技能，流程与工具，平台与设施 三个方面进行综合考虑，才能做好递进式的集成，很难说有一个固定的条条框框来套
云管监控系统与AIOps是否可以结合呢？	AIOps 认知型IT运维，在引入认知技术之前需要对基础设施，平台，工具等进行综合考量，在具备了流程事件管理，集中日志管理，监控告警等能力的前提下才能最大发挥AI在Ops上的赋能。云管监控系统是AIOps的一个基础前提，两者可以做结合。
请问如果是多云多集群环境如何进行监控部署？	IBM的AIOps解决方案可以实现在多云环境下从业务视角提供从运维管理到CIO的动态视图，实时了解以使用者为中心的服务、应用和基础架构运行状态。
市面上有众多云管平台的品牌和厂商，该如何进行选型，可以从哪些方面来判断哪个厂商的产品适用于自己企业呢？	1、传统企业上云之后，架构将发生很大的变化，既有传统IT架构，又有更加灵活敏捷的云架构，架构更加复杂，管理的复杂度也随之增加； 2、在混合IT架构的管理上，我们需要考虑不同的工作负载如何部署到不同的IT环境，哪些工作负载能够上云，哪些还需要使用传统IT架构支持； 不同的传统IT架构和云架构的管理模式也不一样，需要有更专业的，既有传统管理服务又有云管理服务的合作伙伴帮助传统企业实现服务模式的转型； 3、同时，传统企业的上云以及云上管理，亦不同于互联网企业的云原生架构的使用，他们不是从零开始，也不能一蹴而就全部采用云原生架构。

专家问诊

问题	专家回复
很多云服务商都有自己的云管平台，企业是否需要统一纳管全栈云平台？	很多企业都计划上云，大多数企业已经上云，部分企业同时还上了几朵云，然而每个云服务商都有自己的一套云管理平台，通过自有平台进行纳管资源的管理，在多云的环境中缺乏一致性管理，缺少可视性和可控性，建设统一的多云全栈云管理平台是一大趋势。
多云统一管理平台能否替代传统云平台实现管理、运维？	混合多云管理平台是一个具有多云统一资源视角，一致性操作管理，跨集群跨云跨数据中心的综合云管理平台，涵盖敏稳双态模型下的运维和运维管理。大多数情况，通过多云管理平台可以操作处理多数的运维，甚至运营，少数的需要结合传统平台协作处理。
在多云环境下，如何保证业务系统进行安全连接？如何确保数据传输过程的安全性及如何进行监控？	IBM将安全作为多云管理服务体系中，一组至关重要的治理工作。IBM会评估客户组织自身制定的安全策略、所在行业的行业安全标准与法律规定、以及ISO27001、ISO20000等国际标准化组织颁布的安全策略与实施的最佳实践指导，将各个安全策略细化到标准化的安全管理流程、安全策略控制项目、及相应的安全配置项目、及安全基线设置。在异构的混合云架构下，根据标准化的安全管理流程、安全控制策略、安全配置项设置，在不同的公有云、私有云、以及On-Premise环境的，对安全进行加固设置。通过定期执行安全检查，对安全基线与实际安全检查结果的对比，可以及时主动的掌握并发现混合云架构环境中存在的安全漏洞或隐患，并随之采取行动进行安全的加强，以达到标准化、系统化、主动预防、实时追溯的混和云架构的安全管理体系。

专家问诊

问题	专家回复
开发测试，生产环境，多地多中心环境下多套容器云环境，构建统一的云管平台是必然，但如果进行跨集群，跨数据中心的统一的容器，虚拟机，物理机的部署任务编排，有没有什么技术架构推荐？	目前提供跨多集群多中心的容器编排能力的平台比较多，其中最流行最广泛使用的是开源的企业级容器编排平台kubernetes，目前已经成为一种业内标准。各大厂商基于开源的kubernetes都有陆续推出自家平台，比如：微软的AKS，google的GKS，阿里的K8S，红帽的OpenShift等，除了提供编排能力，还提供调度、自愈、弹性伸缩、集群管理等能力，其中红帽的OpenShift尤为卓越，一方面因为是它提供了kubernetes代码的最高贡献量，一方面因为是除了以上基本能力外还将周边生态组件进行了集成打包，提供一个高安全高可靠高性能的解决方案。
应用分布在多个云平台中，混合多云架构需要确保基础数据也可以在云管平台中流畅地移动，无论是在本地还是公有云，如何使数据可迁移？	受限于一些监管上的安全要求，部分行业的数据不允许出中心，不允许出境，只能留存于本地，而部分行业可以允许非核心的数据留存于公有云之上。对于严监管要求下的这些行业，不用考虑数据迁移。需要考虑数据迁移的行业，一般来说，我们建议将数据进行分类分级分档，对于冷的或冰冻类的历史归档数据，可以采用周期性的全量导出、导入形式来进行迁移，对于热的或实时流动的数据，可以采用消费/订阅模式 或 数据API服务 亦或可以采用底层数据同步方式 或其他同等的方式进行迁移。
业务系统设计软硬件数量多，种类也比较广，需要不同领域的技术专家进行运维，如何调配专家资源或者协同外部专家一起会诊，解决复杂问题？	在未来的云，特别是多云环境的管理要求下，对工具之外的管理模式、人员能力、敏捷流程等都提出更高要求；传统企业的IT人员大多只熟悉传统的IT架构，对云架构，特别是基于容器的微服务架构，还是有技术能力上的差距，这就需要专业的云管理服务伙伴和这些企业一起共建云上的运维能力，通过有效的代管、共管，逐步到完全自主管理的转移。

问题

专家问诊

传统架构的发展不均衡以及历史遗留的问题，大多时候云平台的统一管理都是为了统一而统一的统一。真正实现统一管理，需要怎么的梳理设计呢？

专家回复

企业在自身发展的过程中会累积大量的资产、数据、业务以及维系业务运行的各类技术架构和基础设施架构，为了最大限度的发挥已投产的最大效益，往往采用不断叠加方式做所谓的统一管理。为了真正实现的统一管理，可以从以下几个方面综合考虑（包括但不紧限于）。

从技术架构层面，支持异构虚拟化管理，混合多云管理，同时涵盖自动化框架、安全框架、运维管理、运营管理，也包括各类技术框架，比如数据库、大数据、人工智能、区块链等；

从应用架构层面，支持业务应用的快速交付，快速推向市场，能方便利用后端的技术框架快速迭代快速部署，形成各自业务应用线，应用方便做现代化转型；

从资源层面，支持不同架构下不同云下的资源统一纳管，调度，编排等能力，提供一致性视角，加强BSS和OSS方面能力；

从服务层面，支持自服务管理，服务目录，服务编排等能力，提升服务水平等级；

从安全层面，支持物理安全，硬件安全（计算、存储、网络），平台安全，数据安全，应用安全等，逐步向运营安全中心发展；

从数据层面，支持数据管理，数据治理，数据运维，数据运营等服务；

问题

专家回复

专家问诊

我们公司用到了大量的容器，但现在发现容器环境有很多安全隐患，包括镜像、主机、 注册表和编排平台，容器安全怎么去改善？

企业在容器化技术选用，广泛使用的过程中都会触及这样一个安全的话题，恰恰这个往往是技术自研的企业在起始阶段容易忽略，后期需要加强的一个方面。如何有效的规避安全隐患，一般来讲，可以从上中下3层次来综合考虑。最上层，可以从镜像仓库、镜像构建/部署、编排入手，保证应用容器是安全可靠，无漏洞隐患，可以通过镜像安全模块扫描；中间层，需要从容器内容、容器平台、容器集群入手，保证容器引擎，集群环境是安全可靠，无漏洞隐患，可以通过容器平台安全模块扫描；最下层，需要从基础设施，技术架构方面入手，保证计算、存储、网络等基础资源是安全可靠，无漏洞隐患，可以通过底层平台安全模块扫描。红帽的OpenShift在安全层面可以提供多达10层的安全保护和防护，遵循国际安全标准，在镜像仓库（注册表）、租户、容器内容、集群、网络隔离、存储、管理编排等方面保证安全可靠，无漏洞隐患。