

大型枢纽国际机场云运营模式探索与实践

李 锋 胡玉东 刘 晗

首都机场集团有限公司北京大兴国际机场 北京 100000

摘 要：北京大兴国际机场以“Airport3.0智慧型机场”的运行管理理念为核心，辅以“互联网+机场”的理念，整体信息化建设已初具规模。随着大兴机场近百余个信息系统全部上云，基础架构平台分散、异构、多样，服务管理复杂难度高的问题逐渐凸显。如何高效、快速的提升系统运营水平和运维管理能力，以支撑业务及信息化的发展，成为了运维首要解决的问题。

关键词：云计算；多云管理；运维运营

一、云运维面临的挑战

北京大兴国际机场在IT规划设计之初就考虑全面深度使用云计算，如今已实现全部信息系统上云用云，是行业内第一家完成全部系统上云的机场。北京大兴国际机场云平台作为一体化基础支撑平台，不仅为北京大兴国际机场提供稳定、高效、安全的计算、存储、网络资源，同时也为驻场单位和专业公司的信息系统提供所需云资源。

随着业务的发展、管理要求提升、信息系统的增多，新的基础架构平台的建设、IT资源规模的增加以及运维工具平台的引入更新，北京大兴国际机场日常IT服务和管理的压力也越来越大。因此在信息化建设的过程中，如何平衡资源交付与运维管理，同时解决运营不清晰的顽疾成为要重点攻克的内容。

二、大兴机场的基础设施现状

在过去几年的信息系统建设过程中，大兴国际机场已构建百余套信息系统。承载上述信息系统的正是目前在用的各类基础设施，目前已投产的包括虚拟化平台、私有云IaaS平台、PaaS平台、桌面云，并同时使用公有云服务及容器云原生服务，涵盖了各种类型的基础设施形态。现阶段，所有信息系统已全部上云，云资源规模也已达数千实例。配套的运维支撑工具及安全服务建设也初具规模和体系，包括OA、CMDB、备份、堡垒机及漏洞扫描等系统。

在信息系统建设完善的过程中，诸多运维及运营管理的问题日益凸显，主要表现在如下几个方面：

作者简介：李锋（1978-），性别：男，民族：汉，籍贯：江苏，学位：硕士，职位：业务经理，职称：工程师，研究方向：云计算。

（一）难以高效快速响应交付系统建设运行所需资源（响应慢、难管控）

北京大兴国际机场有多个管理部门，每个管理部负责多个模块业务的信息化建设，建设所需资源由数据中心统一调配发放且没有标准流程系统进行支撑。数据中心系统管理员日常的工作职责内容不仅仅包括发放资源，经常不得不忙于其他当时优先级较高事务，最终无法及时处理资源请求，导致排期发放时间较长，从数小时至数天不等。

（二）服务和运维的工作量大压力大（成本高）

虚拟化、云平台的控制台操作权限主要面向系统管理员，变更需要安全合规走流程，但虚拟化、云平台本身不提供流程管理，又无法开放控制台给业务侧人员，导致系统管理员在日常工作中投入大量人工操作。同时系统管理员发放资源后，还需要对资源进行多方位管理，包括访问授权管理、资源归属管理、应用系统关联管理、监控管理、漏洞扫描管理、备份管理等，这些信息同步配置也需要大量的人工工作量，在配置和管理的过程中，均要投入较多的专业人员，沟通成本极高。

（三）难以精细化管理（难运营）

由于云资源分布在各个云平台控制台中且数量巨大，没有集中统一的跟踪分析管理工具，靠人工跟踪分析很难及时发现识别，极易造成资源浪费。同时，资源信息及归属人归属项目信息依赖人工记录维护，很难维护保证信息的准确性、一致性，导致有时需要回收优化时难以找到对应的负责人。

三、解决方案及功能设计

对于上述问题，主要的原因在于缺乏一个整合集成的IT多云服务管理运营门户平台。因此通过建设多云运营管理平台，能够有效地解决资源交付自动化、资源服

务自助化、流程统一化、运营精细化等问题。

（一）总体技术方案及设计

建设多云服务管理运营门户，需要从多云纳管能力、多云自服务能力、多租户权限能力、运维工具集成与服务化能力、计量计费运营能力资源全生命周期管理能力多方面进行建设。

●**流程侧：**统一纳管异构IT基础设施，资源交付自服务

多云服务管理运营门户的第一要务就是打通信息孤岛。目前，大兴国际机场大部分IT基础设施还处于离散的状态，各类资源的管理能力是彼此孤立的。面向已经投产应用的资源，我们缺少有效的统一管理手段，资源池的容量扩展缺少合理的依据；与资源管理离散相伴的，是管理和服务交付流程的分散。

站在支持业务快速创新的角度，资源申请的发起方应该是业务需求方。多云服务管理运营门户的服务化能力能够最大限度地降低资源申请复杂度，并依据流程设定实现自动化的服务分发。需求方按需、自助式地申请IT资源，减少了不必要的沟通，快速开发业务应用，资源使用完毕后及时释放并回收。这样的资源使用闭环将切实提升资源的利用效率，规范化资源使用流程，从底层技术层面确保IT资源交付的便捷、高效与合规。

基于多云服务管理运营门户，还可以进一步规范IT服务系统的用户权限体系。针对云平台的角色设定，梳理IT资源管理与使用的职能角色体系，与内部的。围绕用户的实际需求，不同的租户使用不同的工作空间，并且对应用访问权限进行高权（通过堡垒机进行运维审计）和低权的设置，提升系统整体的安全合规水平。

●**服务侧：**混合IT资源的精准管理、合理规划与智能运营

作为促进业务与基础设施融合的关键平台，多云服务管理运营门户的另一个重要作用是提升IT服务体系整体的智能化水平。通过平台建设，我们不仅可以实现对云资源等资源的监控与管理，还能实时、精确地掌握内部用户对资源的使用情况，并且输出报表进行分析，为IT系统运营提供可靠的佐证。

通过多云服务管理运营门户的运营能力建设，极大的解决IT运营和业务运营割裂的问题，并对IT支撑业务的能力持续优化和改进。通过多云服务管理运营门户，我们不仅可以梳理IT资产的容量管理，还可以用预算管理、报表分析等能力和真实的系统运维数据为IT和业务决策提供有效的指引。

我们还可以借此搭建自己的资源优化体系，不仅IT

资源的分配有据可依，也能实际提升IT运营的绩效水平。多云服务管理运营门户能够在资源全生命周期管理的基础上提供服务运营和监管的真实数据，为IT系统运营提供容量分析、监控分析和优化建议。在资源利用率达到阈值时发出预警公告，及时回收僵尸资源，减少资源浪费情况的发生，优化整体IT容量管理。

●**技术侧：**架构持续迭代，形成多云就绪的IT管理架构

从现阶段信息化发展的趋势看，多云将会成为未来企业IT的主要形态，而企业IT架构也需要能够适应多云应用模式。那么在面向多云基础设施的控制面，我们需要一个架构领先、能够持续演进和快速迭代的多云服务管理运营门户。多云服务管理运营门户将在多云基础设施的控制面发挥关键作用。

多云服务管理运营门户需要具备足够的可扩展性，以满足未来五年IT架构体系进化的需求。这意味着多云服务管理运营门户的规划与建设需要充分地考量灵活性和可扩展性，借助模块化的架构，通过增加管理模块的方式，不断地迭代和演进，很好地消化和适应IT基础设施规模和形态的扩充，同时在流程方面保持延续性和可移植能力。

多云服务管理运营门户并不是一个僵化的管理平台，而是一个能够自适应和自升级的平台。在IT服务化的早期，我们会先从计算和存储的服务化起步，而伴随着云化和服务化进程的深入，各类不同的PaaS服务，安全服务，都可以接入多云服务管理运营门户中，并向用户持续输出自助式云服务。也就是说，我们通过多云服务管理运营门户构建出一整套面向多云应用环境的规范，和一套可扩展的API接口规范，通过调用不同的功能模块满足更多服务交付的需求。这将赋予“多云服务管理运营门户”长久的生命力，为数字化转型的长远目标提供稳固而持续的技术支撑。

（二）云管理功能

多云统一管理能力：建设多云管理能力层，对接纳管虚拟化平台、私有云平台、公有云平台以及容器云各类基础架构平台，自动同步云资源。由于基础架构的建设也是一个不断更新换代的过程，这层需要具备灵活快速的扩展能力，建设实现采用插件的方式，遵循“开放封闭原则”，需要扩展支持纳管新的云平台时，只需要实现对应的封装对应云平台API的插件。

多租户权限能力：建设多租户能力，通过工作空间进行资源管理的隔离，使不同租户的用户只能够查看和管理其租户下的资源，并可对租户的资源数量进行配额

限制,基于租户进行计量计费,产生类似公有云的账单。多云运营管理平台的多租户能力,使管理员能够定义角色和权限层次结构;还能通过运营管理策略,实现资源动态灵活的授权,对资源的用量进行管理限制,进而建立出一套符合自己实际情况的安全合规管理体系,实现在混合IT环境中的安全管理再平衡。

计量计费运营能力:建设对虚拟化、私有云平台资源的计量计费能力,公有云账单的统计分析,跟踪优化能力。让使用资源的业务用户侧能够查看类似公有云的月度年度私有云费用账单以及公有云账单费用,配置费用配额,从而使用户对资源的成本费用有概念,合理使用资源,减少资源浪费。建设资源生命周期回收管理,减少资源浪费。

(三) 云服务功能

统一服务能力:建设在线服务门户,基于虚拟化、私有云、公有云、容器云的整合集成,在线提供各类云资源服务目录,自动化部署,使得管理部产品经理项目经理能够自助登陆用户服务门户,浏览服务目录,选择虚拟机操作系统、磁盘、安全组、弹性IP等产品,在线申请,后台管理员审批后,由云管平台自动根据资源需求及分配策略调用云平台API完成资源的部署。该能力建设的一个关键的点,需要建立灵活的服务目录配置工具,能够以低代码方式,扩展服务目录,配置产品,满足日常各类服务需要,在不需要编码的条件下支持新的虚拟机操作系统类型、IaaS+中间件数据库的服务目录产品,同时能够针对不同的角色人群提供不同的申请向导。另一个是需要实现资源池部署分配策略的配置,定义逻辑资源池,使得系统在审批后,能够自动根据分配策略,将资源部署到限定的云账号、地域、VPC、子网/VLAN宿主机中。

(四) 安全服务功能

通过对运维安全工具的集成,能够在资源部署变更后,自动同步配置资源的信息到堡垒机、备份、漏洞扫描等运维工具,并且能够将安全工具的配置操作包装为自主服务目录给到管理部。通过运维工具集成简化流程,减少人工同步配置操作工作,并保证信息的一致性、完备性、准确性,避免人工漏掉、同步错误。同时通过运维操作的服务化,实现运维服务的自服务,缩短运维服务的响应时间,减少人工操作。

四、平台创新性及收益

(一) 平台创新性

1. 机场行业全面上云,打造业技融合最佳方案

随着多云服务管理运营门户的投产,大兴国际机场

业务已经全面上云,多云服务管理运营门户已经成为大兴国际机场计算、存储、网络和安全资源的一体化基础支撑平台,也是目前机场行业内最佳的业技融合方案。

通过多云服务管理运营门户,信息部门向大兴机场各部门和驻场单位的稳态业务,以私有云和社区云为基础提供快速、安全的自助服务,向大兴机场各部门的敏态业务,以云原生资源为基础提供高效、敏捷的服务模型。正是这种方便快捷的资源交互与管理模式,使得业务和技术行成了高效的联动,极大的提升了工作的生产力。

2. 实现了云、网、安一体化模式,提供了最佳用户体验的云服务

多云服务管理运营门户除了为云服务提供可视化的操作流程外,还实现了云网协同、云安联动、网安联动。基于云网协同模式,信息部门统一对云、网进行管理和策略下发,提升了运维效率;基于云安联动模式,通过微分段技术,实现了对同一网段内的虚拟机的安全防护;基于网安联动模式,通过信息安全平台检测安全事件,下发至SDN控制器,进而实现数据中心安全事件策略的阻断,助力机场信息化安全建设。

借助多云服务管理运营门户实现的云、网、安一体化模式,为技术人员提供了优质的用户体验,同时保障了云环境的灵活性、扩展性以及安全性,为业务创新和数字化转型提供了有力的支撑。

结语

大兴机场是国内第一家全部业务系统整体上云的超大型枢纽机场,为行业成功上云、云网安一体化建设和云运营提供了宝贵经验。

通过多云服务管理运营门户高度可靠的服务能力,确保了各信息系统稳定运行,保障机场运行的安全性和顺畅性。借助平台灵活性和响应能力,提高大兴机场的业务效率和服务质量,助力信息系统快速部署和升级同时实现高效运营和精细管理。最重要的是提升服务质量,为旅客提供了更好的出行体验,提升了机场服务的质量和效果,推动行业整体信息产业升级。

参考文献

- [1] 涂亚飞. 云计算环境下计算机网络安全防范研究[J]. 金融科技时代, 2023(09)
- [2] 韩委轩. 云计算环境下计算机网络安全技术的优化研究[J]. 网络空间安全, 2023(04)
- [3] 周小新. 云计算环境下的计算机网络安全技术探究[J]. 信息与电脑(理论版), 2023(14)