云计算环境下开放大学数据中心私有云建设研究*

——以国家开放大学为例

李沐明　袁亚兴

（国家开放大学　信息化部，北京　100039）

［摘　要］随着云计算技术的不断发展，利用云计算技术可以建设高效安全的云管理平台。文章基于数据中心在管理、维护、扩展等方面存在的问题进行研究，提出基于统一基础架构的数据中心私有云建设方案，并总结该私有云管理平台的实现意义，为开放大学办学体系信息化建设提供建议。

［关键词］云计算；开放大学；数据中心；私有云；信息化

［中图分类号］G434　　［文献标识码］A　　［文章编号］1008-7656（2019）03-0015-04

引言

随着信息网络时代的不断发展，传统的 IT 架构的数据中心面临着越来越多的压力，信息系统的增加带来了服务器需求大幅增长，需要更多的人力、物力投入到数据中心的建设和管理中，为了解决这些问题，行业一直在不断探索新的技术和管理方案[1]。

云计算（Cloud Computing）概念最早是 2006 年由 Google、Amazon 等公司提出，它是分布式计算、虚拟化、网络存储等多种技术混合演进、发展融合的产物[2]。“云”是一些可以自我维护和管理的虚拟计算资源，通常是一些大型服务器集群，包括计算服务器、存储服务器和宽带资源等。各种类型的云计算应用主要有公有云、私有云、混合云。目前，国内厂商提供公有云的主要有阿里云、腾讯云、华为云、百度云等。在数据中心私有云建设方面，目前已有哈尔滨工程大学、解放军理工大学、中南大学、湖南大学、湖南师范大学等高校在数据中心部署私有云管理平台。

随着高校信息化建设的不断加快，基本建立了服务于教学、招生、科研、管理的公共基础架构，完成了众多的应用信息系统包括 OA 系统、招生系统、科研系统、门户网站、学院网站、收费系统等。这些系统通常由不同的业务部门进行建设，分布在数据中心内不同物理服务器上，由不同的运维管理人员进行相关管理操作。文章以国家开放大学（以下简称国开）为例，对数据中心面临的问题进行分析，通过对数据中心私有云平台的网络架构进行研究，提出一种安全可靠的主机网络架构，并实现一种适合开放大学数据中心的私有云建设方案，从而提高学校业务信息系统

*［基金项目］国家开放大学 2018 年度青年课题“云计算环境下国家开放大学数据中心私有云规划建设研究”（编号：G18F0037Q）
［收稿日期］2019-03-06

的可靠性，当服务器宕机时保证业务信息系统不中断，保证业务信息系统稳定运行。

一、国家开放大学数据中心现状

国开是教育部直属的，以现代信息技术为支撑，学历教育与非学历教育并举，实施远程开放教育的新型高等学校[3]。国开数据中心于 2011 年建成，共有 200 余台物理服务器，50 余台网络交换机，60 余个信息系统（网站）。大部分的用户量小的信息系统包括业务测试系统均单独部署在物理服务器上，使得国开数据中心在管理、维护等方面存在一些问题。

（一）部分服务器利用率不高

一台服务器安装一个操作系统，大多运行 1 个应用程序，cpu 和内存等资源利用率不高。

（二）信息系统管理成本高

各信息系统不是在同一个时间段里进行部署，服务器等设备的采购型号也不统一，不同品牌的服务器之间需要不同的运维人员负责系统的维护，信息系统管理成本高。

（三）部分信息系统可靠性差

由于各服务器都处于单机状态，可能存在单点故障，如果有服务器处于宕机状态，那么该服务器上运行的信息系统也会随之中断。服务器的管理员在进行操作系统升级维护时也可能需要对该服务器进行重启等工作，这也使得信息系统存在中断运行的可能。

二、数据中心私有云建设方案

数据中心私有云平台搭建的关键技术是虚拟化，目前常用的虚拟化技术主要有 KVM、Xen、VMWare、hyper-v 等，针对国开数据中心建设中存在的问题，通过对主流的虚拟化技术进行比较，本文采用文献研究、工程验证的研究方法，先对云计算关键技术之一的虚拟化技术相关文献进行研究，通过对主流的虚拟化技术对比分析，结合国开信息化建设的实际情况，选取适合国开数据中心私有云建设的的虚拟化技术，提出一个适合国开数据中心的私有云规划建设方案，然后结合国家开放大学虚拟化平台建设项目进行实践，将该私有云规划建设方案进行实施。

（一）私有云平台网络架构

在网络方面，IP 网络主要包含两类链路：一类是业务链路，用于传输虚拟服务器对外提供服务的业务流量，宿主机通过业务交换机上联至上游网络；另一类是宿主机之间通讯链路，用于传输 VMKernel 管理流量和 HA 集群中 FT 数据同步流量，宿主机之间互联，无需提供对外连接。IP 网络中业务部分链路里宿主机通过双链路上联至业务交换设备，为业务系统对外提供对外传输数据链路条件，链路通过捆绑后实现负载均衡以及预防单点故障.IP 网络中业务外链路里每台宿主机至少预留两个 NIC 接口并各自通过专用线路进行互联，其专用于为 VMKernel 传输管理流量以及为 FT 提供日志同步数据链路。

（二）私有云平台建设方案

基于 VMware 架构的数据中心私有云平台建设方案包括前期规划、实施部署（基础部分）、实施部署（功能部分）、测试验收四个环节。前期规划主要分为两个部分：设备物理规划与系统参数规划。设备物理规划主要包含物理资源统计、存储空间规划、网络接口规划、Fault Tolerance 规划等。系统参数规划包含宿主机参数规划、vCenter 参数规划、虚拟分布式交换机规划、网络分段规划以及 NSX 安全策略规划。

统计物理资源主要目的是合理规划整个虚拟化平台的可用及有效容量，防止出现资源过度分配的情况，提早进行扩容。为保证虚拟化平台获得最佳的存储性能，共享存储空间至少应分为三部分：VHD 存储集，用于存储虚拟机磁盘文件，如条件允许应考虑将读写频繁的虚拟机磁盘文件安置于存储高速区域（SSD、10K/15K SAS），为高速读写提供足够的 IO 性能；Image 存储集，用于存储光盘镜像、操作系统镜像等文件，主要操作为读取，操作频率极低，条件允许应尽量安置于存储低速区域（10K SAS/NL-SAS）；HA 仲裁，VMware HA 集群存活仲裁盘，容量一般不大于 10GB，可用于当 HA 集群网络 Keep-Alive 机制故障但宿主机未宕机的情况下的存活检测。

宿主机在安装 vSphere 前应有统一的参数规划要求，包括主机名、IP 地址、DNS、本地存储等。vCenter Server 可选两种部署方案，分别为软件单体安装与 OVA 打包安装，区别在于单体安装需要用户自行安装操作系统与数据库，OVA 打包安装则通过由 VMware 预先制作的 OVA 应用包直接部署。VMware vSphere 环境中包含两类虚拟交换机：

vSphere 标准交换机与 vSphere 分布式交换机。在本次建设方案中将为业务数据路径配置 vSphere 分布式交换机、为管理数据路径配置 vSphere 标准交换机。通过为业务配置 vSphere 分布式交换机，在最大限度保证虚拟化平台对外数据出口的灵活性和易用性外，还可以为后期部署 VMware NSX 功能提供必要的基本条件。针对管理部分网络需求则采用 vSphere 标准交换机提供虚拟网络互联支持。

网络分段规划主要针对不同数据路径规划充足的地址空间，根据目前规划，本次项目建议主要划分两类网络：一类是虚拟化平台内部管理网络，该网络无对外出口，仅供 vCenter 与各宿主机 vSphere 软件传输管理、迁移以及同步流量；另一类是虚拟化平台业务对外网络，该网络根据业务归属或安全等级进行分段，并为不同分段分配 VLAN id、下一跳地址等信息。管理网络 IP 地址配置（宿主机 IP 地址）：应于宿主机 vSphere 安装时进行；业务网络 IP 地址配置（虚拟机 IP 地址）：应首先将网络分段规划与网络接口规划结合，而后配置 vSphere 分布式交换机，最终在部署配置 VM 时进行指定。

（三）私有云平台实施部署

基础部分实施部署工作主要进行虚拟化平台底层部分安装调试及基本功能配置。根据 VMware 最佳部署实践介绍，下列各项工作建议以既定顺序执行。实施工作内容中标准化操作流程将不在此处描述，所有实施方法、操作流程均以 VMware 部署文档为准，主要包括设备上架与线缆连接、存储空间分配、宿主机系统安装、Vcenter Server 安装、数据中心及 HA 集群配置、虚拟交换机配置、网络设备配置、NSX 安装及配置、VM 模板配置等。实施部署功能部分针对虚拟化平台中高级功能、特色功能方面进行安装调试工作。实施部署功能部分针对虚拟化平台中高级功能、特色功能方面进行安装调试工作。Update Manager 安装、Data Protection 安装、VM 安装配置、vCenter Converter 软件安装、Fault Tolerance 配置等。

VMware NSX 作为 VMware 为服务器虚拟化平台中提供的网络虚拟化功能模块，与无 NSX 的主要差异在于:NSX 可为虚拟化环境中每台 VM 提供分布式的防火墙保护；NSX 可针对某一组或某一特性的一些 VM 提供统一的防火墙策略；NSX 无需外部设备即可实现 VM 间数据流的 3 层转发与过滤；NSX 无需外部安全设备即可实现不同安全级别的划分（零信任环境）；NSX 可通过 Edge 边界提供 NAT、边界安全等传统路由器设备提供的功能。VMware NSX 部署的必要条件之一是虚拟化环境中 Virtual-to-Virtual 网络必须是 vSphere 分布式交换机。只有通过分布式交换机，才可以实现 NSX 的各项策略、功能推送至每台 VM。如果数据中心对于信息系统安全要求比较高可考虑采购 NSX 模块。

（四）私有云建设平台测试验收

测试验收阶段分为三步，即依次进行性能测试、功能测试以及平台业务的可用性测试。测试简要描述如下。

1.性能测试。检测外部业务访问性能，如 Web 或 App 响应速度，具体测试客体由用户提供。

2.功能测试。检测虚拟化环境各项功能，包括基本功能与高级功能，VM 创建、修改、删除；手动 vMotion，宿主高负载下自动 vMotion；集群整体低负载下 DRS 调配；Update Manager 推送更新；其他 vCenter Server 可提供基础功能。

3.可用性测试。检测虚拟化环境中 HA、FT 以及 Data Protection 功能，HA 功能检测，VM-Kernel 中断 HA 检测、FC 存储网络中断 HA 检测、同时中断 HA 检测；FT 功能检测，宿主机强制断电检测（基于系统底层命令执行重新启动）；DP 备份恢复检测。

三、数据中心私有云管理平台实现

考虑到 VMWare 是相对比较成熟的商业软件，市场占有率较大，而且搭建的私有云平台易于管理，比较稳定，因此本文采用 VMWare 虚拟化软件实现硬件、存储资源的集成和整合，搭建基于 VMWare 的私有云管理平台，基于 VMware 架构的私有云平台搭建完成后，将业务信息系统部署到该私有云平台，同时将已有的基于 KVM 架构的管理平台上的业务系统迁移到该私有云平台，对数据中心的业务信息系统实行统一管理。

利用数据中心内 5 台 Lenovo X3950x6 服务器搭建基于 VMWare 架构的私有云管理平台，利用两套存储设备做虚拟机复制，用于虚拟化共享存储，利用两台 DELL EMC 光纤交换机做链路主备，用于存储链路冗余。共有物理 cpu 1104GHz，物理

内存 2560G，物理存储空间 90TB。经过虚拟化后，可扩展 1920 个 vcpu，可划分 cpu 4416GHz，可支持 200 台虚拟服务器在线运行。

国开私有云平台目前已部署虚拟机 89 个，内存使用率 32.5%，存储使用率 37.3%，还可容纳 150 台左右虚拟机。随着信息化建设的不断深入，新开发的信息系统可优先部署在该私有云平台上。

基于云计算的数据中心私有云规划建设，是对学校数据中心的一次基础技术升级，主要意义如下。

（一）提高服务器等资源利用效率

通过数据中心已有的服务器和存储等硬件资源，利用虚拟化技术将硬件资源和网络资源等进行整合，搭建数据中心私有云管理平台，能够将高标准化的服务器达到最优化，充分提高硬件资源利用率，将服务器成本降低 20%～50%，并且将服务器及存储利用率上升至 40～80%。

（二）应用系统部署更加灵活

通过统一的私有云管理平台能够实现硬件资源的快速部署，并且增强数据的可操作性，可以满足绝大部分分析任务，快速响应分析需求，提高系统管理的效率和质量，并能以最小的管理代价和工作量实现数据资源的合理化分配。在业务系统不断调整的时期，学校可以根据需要利用云数据中心进行资源的合理分配，满足 IT 实时的部署需求。

（三）信息系统更加安全可靠

通过统一的私有云管理平台，对所有的信息系统进行统一规划，进行安全加固和优化，做好数据备份，能够保证学校信息系统的安全性，从而为学校信息化建设提供基础保障，为学校教职工搭建一个高速、稳定、安全、可靠的应用环境[4]。并且通过 IT 资源的分配能够实现大量用户并发访问需求，快速创建服务器并部署应用系统，通过容灾备份等措施虚拟服务器上数据的快速恢复。

四、结语

随着《网络安全法》和《教育信息化 2.0 行动计划》等一系列法律、政策的出台，在信息化建设的过程中需要高度重视信息系统的安全，因此在私有云平台的建设过程中要加强安全加固，加强对数据中心私有云平台的监控和管理，避免内部数据信息的泄露和丢失，保障信息系统在运行中安全可靠，这是当下及未来数据中心私有云建设的一项重要工作。

[参考文献]

[1] 许玉焕.基于 VMware 的高校云计算数据中心设计与实现 [J] .网络安全技术与用，2016 (8) .

[2] 苏命峰.云计算环境下高校数据中心的虚拟化研究与实现 [D] .长沙：湖南大学，2014.

[3] 杨志坚.国家开放大学建设:改革与创新 [J] .中国远程教育，2013 (7) .

[4] 李菊.基于私有云安全平台的网络安全部署研究与实施 [J] .信息网络安全，2013 (8) .

[作者简介] 李沐明（1993–），男，河南信阳人，国家开放大学信息化部科员，实习研究员，硕士，研究方向：教育信息化、网络安全；袁亚兴 (1977–)，男，江西丰城人，国家开放大学信息化部副部长，助理研究员，硕士，研究方向：教育信息化、数据挖掘。

[责任编辑　周个妹]