企业私有云的研究与应用

马 旭
国家能源集团宁夏煤业有限责任公司 宁夏 银川 750000

摘 要：本文对能源企业私有云关键技术进行了研究，包括基础设施层，资源池层，云服务层，展示层，运营管理层和运维管理层。企业私有云从功能、云服务、硬件系统、迁移策略和网络安全方面进行设计。通过搭建企业私有云，实现了云主机的快速创建，操作系统补丁的稳定升级，运行稳定。改变了企业数据中心的建设模式，由传统的独立物理服务器改变为灵活可扩展的私有云，在企业中有很好的推广价值。

关键词：私有云；弹性云服务器；安全组服务

引言

传统企业数据中心硬件设备都是依据应用系统需求采购，硬件设备多，采购时间长，使信息化维护效率低下，存在数据孤岛，影响企业智能化建设。企业急需利用新的信息技术手段提高数据中心资源利用率，降低IT运维成本，解决未来安全生产业务快速变化和安全生产数据智能分析等问题。如何利用虚拟化、大数据、"互联网+"等先进技术，在满足网络安全管控需求的前提化，搭建企业私有云，提高安全生产管理效率，保证业务稳定、可靠运行，成为目前大多数企业数据中心转型改革发展路上需要攻克解决的重要问题。

1 私有云关键技术

当前云计算底层虚拟化技术主要有以VMware为代表的封闭虚拟化技术，windows的Hyper-V，XEN开源虚拟化技术和KVM开源虚拟化技术。私有云解决方案的技术路线主要有基于开源OpenStack进行的各企业发行版本，这类技术代表主要有华为云Stack，华三私有云，easyStack，Zstack。OpenStack只是系统的控制面，不包括系统的数据面组件，比如Hypervisor，硬件设备。本文选用KVM虚拟化技术和OpenStack技术路线，对应的企业产品为华为云Stack解决方案由FusionSphere OpenStack(私有云架构组件)、ManageOne(统一数据中心管理平台)。私有云以云服务的形式提供服务，提供统一运营运维管理功能。

2 企业私有云设计

2.1 企业私有云总体设计

企业私有云包括基础设施层，资源池层，云服务层，展示层，运营管理层和运维管理层。

基础设施层包括服务器、存储、网络和网络安全等设备；资源池层通过私有云软件，基于硬件设备资源，创建出计算资源池（含 GPU 资源池）、存储资源池、网络安全资源池，上层业务系统所需基础设施资源全部从资源池中获取，不直接与硬件设备交互；云服务层基于计算资源池、存储资源池、网络资源池，企业私有云为应用系统提供各式云服务，包括弹性云服务器、镜像服务、云硬盘、虚拟私有云、弹性公网IP、安全组、虚拟防火墙、弹性负载均衡、弹性云服务器备份等多种云服务，所有的云服务需要依赖于底层采购的硬件实现；展示层通过统一的云服务管理Console对资源进行统一监管和运维；运营管理层提供云服务申请、自助服务控制台、用户管理等运营管理功能[1]；运维管理层提供拓扑管理、资源管理、告警管理、集中巡检、性能管理以及统计报表等运维管理。

2.2 企业私有云功能设计

企业私有云主要功能包括Service OM私有云管理功能、ManageOne运营系统功能、ManageOne运维系统功能、FusionCare巡检功能、FusionSpere CPS私有云配置功能，通过对这些功能的配合使用，可以完成对整个私有云业务快速上线，具体架构如图1所示。

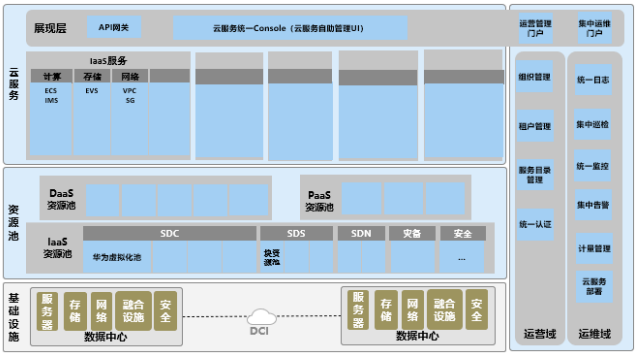

图1 企业私有云基础功能架构图

2.2.1 Service OM平台功能

计算资源，主要包括主机组、规格、虚拟机管理，可以对私有云的物理服务器以主机组进行管理，通过创

建不同规格与主机组进行绑定，让业务发放的虚拟机落到制定的主机组资源中，使不同业务均衡的分散到不同主机组中，提升资源利用，节约成本。

镜像资源，可以通过将镜像资源上传，并注册，注册后，制作成公共镜像，可以通过运营平台发放与主机。

存储资源，可以通过创建磁盘类型，绑定后端存储，来划分不同的后端存储类型，使发放的云主机的磁盘可以落到不同的后端存储上，可以节省资源，提升性能。

网络资源，创建网络资源，首先需要把物理网络打通，通过创建外部网络，可以建立外部连接与VDC之间通信，主要用于外部用户访问VDC的云主机，也可以建立内部连接，用于VDC内部云主机的通信。

2.2.2 ManageOne运营系统功能

运营平台功能设计，主要包括VDC管理、ECS云主机管理、EVS云磁盘管理，VHA云硬盘高可用，虚拟私有云VPC隔离、审批流程管理，管理员可以通过对私有云VDC管理功能配置，完成对国家能源集团宁夏煤业有限责任公司组织架构，进行资源分配，并可以通过创建审批流程，对提交的ECS云主机、云磁盘进行部门审批，ManageOne运营系统可提供自动化，资源的统一管理，业务的自动化和服务化。管理员都可以定义审批流程。最大支持5级流程审批，具体设计如图2所示。

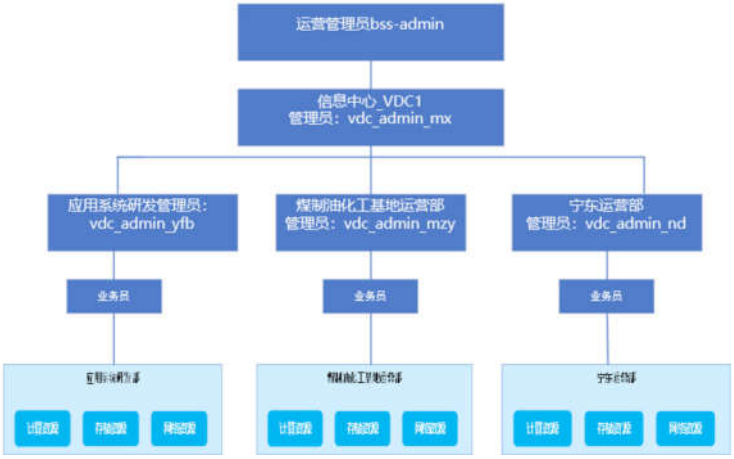

图2 VDC组织架构图

2.2.3 ManageOne运维系统功能

运维系统提供运维管理门户，支持对多数据中心的统一运维管理，包括资源管理、告警管理、拓扑管理、性能管理以及统计报表，立体监控功能，智能故障定位，运维可视化、CMDB等功能。通过运维系统能够对硬件问题进行快速定位和处理故障，对计算、存储、网络以及大数据资源池的统一监控和分析。

2.3 云服务设计

（1）IaaS-弹性云服务器（ECS）

ECS是由内存、CPU、云硬盘、镜像组成的一种可随时获取、弹性可扩展的计算服务器。

（2）IaaS-虚拟私有云（VPC）

VPC是私密的、隔离的虚拟网络环境。用户可以自由配置VPC内的IP地址段、子网、安全组等子服务。

（3）IaaS-安全组服务（SEG）

SEG是安全过滤规则，可以对进出虚拟机端口的网络报文进行限制。

（4）IaaS-云硬盘（EVS）

EVS为弹性云服务器提供块存储空间，EVS可进行格式化、创建文件系统等，可持久化存储数据。

2.4 硬件系统设计

硬件设备如下：计算资源池华为2488V5服务器3台，云平台管理服务器华为2288H V5服务器3台，GPU资源池华为G5500服务器 2台，存储资源池磁盘阵列华为双活磁盘阵列华为OceanStor Dorado5000 V3 2台。

2.5 迁移策略设计

迁移策略的制定需要结合现网应用系统分布、部署情况、复杂程度、访问以及被访问通信矩阵、中断影响程度等结合分析；

通用的迁移策略原则如下：

（1）先易后难，即先搬迁简单应用，配置容易修改的应用；

（2）先测试后生产，即先迁移相关的测试系统或者开发系统，最后在迁移关键的生产应用；将相对重要程度低的主机才迁移上云，积累迁移经验，迁移带来的风险也可控；

（3）应用耦合度低的应用优先迁移，此类应用和其他主机、系统关联程度低，迁移带来的影响范围较小；

（4）单套应用系统整体迁移，即将一套应用系统包含的各个主机安排在同一个迁移批次；

（5）强关联性的应用系统安排统一批次迁移；部分应用系统可能存在强相关性，比如考勤系统和薪酬系统，存在部分数据的共享与应用的频繁访问，则安排强关联应用系统统一批次迁移。

2.6 企业私有云网络安全设计

对管理、业务、存储网络平面相互隔离，业务区域之间还可以通过VPC进行隔离。在虚拟数据中心中，不同的部门或不同的业务，可以使用独立的“VPC”（虚拟私有网络）来隔离。通过VPC划分，在数据中心内部不同安全级别的业务区域属于独立的VLAN。VPC可以在私有云获取私有的资源，管理员可以完全控制虚拟网络环境，而不受其他部门的干扰。

3 运行效果

通过搭建企业私有云，实现了云主机的快速创建，操作系统补丁的稳定升级，运行稳定。改变了企业数据中心的建设模式，由传统的独立物理服务器改变为灵活可扩展的私有云，在企业中有很好的推广价值。企业私有云应用后，对企业智能化生产和信息化建设又是一次跨越式的变革。一是降低了IT的硬件和运维成本，减少了大量的硬件资源投入。二是提供给企业更多的灵活性，可以根据自己的业务情况有计划的进行计算和存储资源投资。三是增强了扩展性，可以增加单台云主机的CPU、内存数，也可以增加云主机的台数。四是资源可以快速部署和开通服务，在传统的IT建设模式中，购买物理服务器时间通常都为几周甚至长的可以达到几个月，很有可能错过业务发展的关键期。在云计算模式下，云主机是即开即用的，云主机的开通时间基本在5分钟左右，再加上软件安装时间，整个的业务部署可以在1、2个小时内完成。五是降低了硬件故障带来的业务系统停用等风险，简化了操作系统恢复难度，具体应用效果如图3所示。

图3 企业私有云资源池概览截图

4 结论

开展能源企业私有云研究和应用，获得以下结论：

(1)提供统一的资源管理、跨资源池的资源部署、运维管理、服务管理和自助服务等能力。避免了信息化资源的重复建设，提升了现有资源的利用率，提升了组织运作效率。

(2)建立了本地双活存储保护机制，当一套存储设备发生故障时，数据零丢失，业务不中断[2]。

(3)实现了企业业务数据的集中管控，简化运维流程，在厂矿较多的公司具有推广价值。

参考文献：

[1]宋伟, 杨超. 轨道交通自动售检票线网管理中心方案设计[J]. 自动化博览, 2021, 38(5):4.

[2]沈光亮. 以云平台为底座的城轨云架构研究[J]. 都市快轨交通, 2020, 33(5):6.