DOI：10. 16516/j. gedi. issn2095-8676. 2018. S1. 044

能源企业租用公有云服务的实践探讨

王华明，殷金华
（中国能源建设股份有限公司，北京 100022）

摘要：[**目的**]当前，公有云服务的发展日益迅速，不少企业也开始尝试公有云服务，对公有云服务上的部署方式及必要的安全防护措施进行总结，形成了一套较为科学、实用的方法，便于各企业的信息系统迁移、部署到公有云上。[**方法**]分析了近四年来中国能源建设集团股份有限公司租用公有云服务的实践经验。[**结果**]总结和阐述了公有云服务上的部署方式及安全防护措施，形成了一套较为科学、实用的能源企业租用公有云服务方法。[**结论**]公有云的应用系统部署，信息系统登录的防护，以及在公有云上实现迁移和满足性能的应用等方面需要进一步的研究和探索。

关键词：公有云；信息安全；信息技术
中图分类号：TK01；TP309　　**文献标志码**：A　　**文章编号**：2095-8676(2018)S1-0242-04

Discuss on Lease Practice of Energy Enterprise Public Cloud Services

WANG Huaming，YIN Jinhua
（China Energy Construction Co. ，Ltd. ，Beijing 100022，China）

Abstract：[**Introduction**]At present the public cloud service develops rapidly，many companies also begin experimenting with the public cloud service，try to migrate and deploy their information systems on public clouds. [**Method**]The practical experiences in nearly four years were studied for China Energy Construction Co. ，Ltd. [**Result**]The paper elaborates and summarizes the deployment methods and safety protection measures of public cloud service，and develps a set of scientific and practical methods. [**Conclusion**]This work provides some guidance for further study on how to do well in login of information system，especially when application system deployed on public cloud.

Key words：public cloud；information safety；information technology

0　引言

在国家政策支持和市场需求的推动下，国内公有云服务[1-3]的发展如火如荼，可谓百花齐放。除阿里云、腾讯云外涌现出不少以技术为核心的创新型企业，发展势头迅猛，不少企业也开始尝试公有云服务。笔者所在企业——中国能源建设集团股份有限公司(后简称中国能建)应用公有云服务已近三年，已对公有云的产品及部署应用需考虑的问题有了初步的认识或经验，现成本文进行分享、交流。本文仅侧重中国能建尝试公有云服务 IaaS 方面的应用、经验等。

收稿日期：2018-06-06　　**修回日期**：2018-10-16

中国能建租用公有云服务部署的大多为管理信息系统，已初步形成了一定规模的服务器群，便于后期数据集成与共享。为访问方便及安全考虑，建立了本地机房与公有云云端的网络互联。

1　部署应用情况

中国能建在公有云上创建了专属的、与租用云服务其他区域相对隔离的 VPC(虚拟局域网)，企业机房与公有云的互联方式成熟方案为云专线或 IPSEC VPN 两种方案，中国能建采用后者进行建设。通过企业机房与此 VPC 的 IPSEC VPN 互联，使得企业局域网络与 VPC 的二层互联。

公有云的 ECS 服务器具有安全组功能(类似路由器、防火墙等设备的 ACL 访问控制功能，但配置的颗粒度能更细)，中国能建部署的 ECS 服务器

进行了精细化配置，从公网入/出、内网入/出 4 个方向按照最小化授权原则限定了只可访问的 IP 及服务端口。其他各产品功能如表 1 所示。

表 1　产品功能表

Tab. 1　Function table of the product

产品	功能
应用防火墙	系统域名的 DNS 解析采用 CNAME 方式，并指向系统 WEB 服务器及映射公网 IP，使得所有的应用访问都必须通过应用防火墙的防护。
链路负载均衡	用此产品自定义所有服务器的出口带宽，可应用此产品进行端口映射功能，同时将应用防火墙的回源 IP 设置为此产品的白名单，实现能访问系统的 IP 都是通过应用防火墙的 IP，进而防范非法访问。
ECS 服务器	弹性服务器。根据需求分别选择了云 linux 系统、Windows2008 系统，CPU、内存、硬盘能灵活配置。
MySQL 实例	数据库实例。属于 PaaS 应用，可选冗余高可用产品。CPU、内存及存储空间能灵活配置。
态势感知	实现网页篡改、肉鸡行为、暴力登录及后门、DDoS 攻击、WEB 应用攻击等的检测及提醒。
主机防护	在 ECS 服务器上安装插件，实现服务器的系统漏洞、WEB-CMS 漏洞、其他漏洞的检测提醒，实现异常登录、网站后门、主机异常等入侵检测和提醒等。
云监控	实现各主机硬件资源及网络流量的实时监控，并能异常时进行告警；实现站点 HTTP 的监测和异常告警。

2　应用分析

2.1　成本分析

成本计算应涵盖选用的服务器、数据库、安全防护产品、网络链路租赁等全部产品，还需考虑机房部署时采购的 IT 资产折旧及运行时的耗材维修、设施部署及运维人力成本、操作系统正版化、机房基础设施建设费用、电力运行成本等等诸多方面。成本分析的精确定量对比不是本文的重点，以一台服务器举例对比大致成本如下：

服务器配置为：2 核 CPU、16 G 内存、600 G 硬盘(100 G SAS 系统盘 + 500 G SAS 数据盘)、Windows 2008 server，企业在云端的服务器大部分按此配置，运行至今能满足信息系统硬件需求。此配置阿里云官网报价为一年费用为 5 598 元，华为云官网报价为 6 926 元。传统机房建设时，服务器产品 CPU 目前最少 4 核，此硬件配置采购价不低于 1.6 万元，并考虑操作系统后采购成本价不低于 2 万元。电力运行费方面，服务器按 400 W 电源配置、电费 1.5 元/度计算，服务器电费每年至少 5 200元。

从服务器采购及电力运行成本角度看，公有云应用成本具有优势。

2.2　设施运维分析

云上的各种产品即选即用，配置及调配灵活，省去机房部署的上架、上电及调配线路等，包括安装部署操作系统、调整服务器硬件资源等方面都能体现运维的便捷性，此外云服务都提供窗口化界面，日常运维都能随时随地完成。公有云 IaaS 服务，各云服务商公布都能保证“多个 9”的可用性，还有各云服务商都推出自有的与底层融合的操作系统，这些都保证了基础服务的稳定可靠，运行稳定性强于机房部署应用。运行的可视性方面，机房运行时，纵然使用各种运维管理系统监测但还需辅助人工巡检，云运用时都可利用云监控等产品实时监控各种资源及服务的运行情况。

2.3　信息安全防护分析

机房信息安全的基础防护常用“三把斧”(防火墙、入侵检测、杀毒软件)部署，安全防护还有应用防火墙、IPS、漏洞扫描、终端防护、数据备份、上网行为管理等，部署位置一般为终端上安装、网关或主干链路部署、旁路侦听等。但常出现“糖葫芦”的部署引起路由交换效率低、服务器主机防护的颗粒度不细、再增设安全产品会需要网络结构的改造等不便之处。

中国能建选择公有云安全产品的思路还是延续机房的相关产品功能，部署有应用防火墙、主机防护及漏洞扫描产品、云磁盘备份或快照产品，并着重配置服务器安全组。通过配置，机房安全需考虑的应用层面(如页面防篡改、WEB 攻击、代码攻击)、网络层面(边界防护、ACL)、主机层面(如病毒防护、数据防护)等维度都能满足，但部署的效率大大提升、实现的颗粒度也更细，且能充分“享受”云安全平台的高效防护(因机房安全设备的升级效率无法与云平台媲美)。

此外，中国能建还在研究测试云产品上的证书管理服务(HTTPS)、数据库安全审计、服务器运维堡垒机等安全产品。

3　实践经验

中国能建应用公有云后，总体感受是省钱、省力、省心。本文仅从技术角度总结的经验如下：

3.1 概要说明

经尝试公有云，单从信息系统角度讲是将应用系统搬迁至“云机房”，并配备所需的网络、计算、存储及安全防护资源等。云应用仍遵循企业整体信息化规划的技术架构，与规划中基础设施层以上的信息化建设和应用无关，仅基础设施的提供方式发生了改变，并且变得更灵活、弹性。

公有云服务提供了丰富的各类产品，各类产品的选用上需根据应用部署的需要有针对性的配置和安全防护，如是否公网 IP 访问，如是否进行 WEB 防火墙发布等等。企业进行云应用，在相当一段时间会保留本地机房的 IT 设施，也能本地建设“私有云”来形成“混合云”的 IT 设施架构，甚至租用多个云服务来形成“多重云”。云服务上的计算资源、存储资源都是面向对象产品、即买即用，仅仅还需建立机房(或私有云)与云端的互联，并且互联方式也为传统的 IPSEC VPN 或云专线方式(租用运营商点到点的如 SDH 专线)。

3.2 云应用的规划方面

3.2.1 服务地域

云服务的地域是进行云服务选择的第一步，地域选择导致两个不能“兼得”的问题：(1)云服务需用云专线方式与机房互联时，选择的地域是否与机房同城直接影响专线链路计费(运营商专线仅同城和异地两个计费方式，且价格差异较大)；(2)选择的地域能否实现与本地机房异地备份。云服务商在企业本地未建设云服务地域时，以上问题就不涉及。中国能建的做法是选择本地云服务区域，但可利用云服务的异地备份产品实现“系统异地保障”的有关要求。

3.2.2 IP 规划

从企业信息化技术架构看，云应用及机房建设两种方式在基础设施层以上都无差别。中国能建在应用云服务后，体会在云端部署一定规模的信息系统时需要创建 VPC 网络(创建后才能规划自有的 IP 地址段)，并且 IP 地址段需配置与机房局域网络二层互联的网段。这同机房建设方式是一样需要规划、考虑的问题。

3.2.3 部署产品规划

部署产品根据信息系统的基础软硬件需求购置 ECS 服务器、数据库实例及配置信息系统访问的发布方式等。中国能建尝试公有云后，对信息系统的云部署的相关产品规划已形成“套餐”式配置。总结“套餐”的组成为：应用防火墙(如需域名解析时)+主机安全防护产品+弹性服务器(或数据库实例，着重进行安全组配置)+云监控。

3.2.4 部署流程

云应用并非勾选几个服务器及安全防护产品就已完毕，其中的产品还前后衔接、环环相扣，实际应用中，需要对各个云服务商产品了解的基础上固化云部署的流程，并后期要定期开展对照核查工作，着重通过系统服务器的数据流向核实安全组的配置。

3.3 基础应用产品方面

3.3.1 弹性服务器磁盘设置及部署

云产品都提供了镜像(或快照)方式对弹性服务器进行数据备份，应用此数据备份(镜像)挂载在新购服务器上后能实现系统服务器的快速无差别恢复(类似有的备份系统的 CDP 功能)。中国能建应用此特点开展信息系统的应急接管，但多个云服务商自动定期完成此功能时一个共同的局限是只对系统盘。

鉴于此，可根据系统的数据量情况，在配置服务器时只选用系统盘来部署信息系统的应用程序和数据等，从而配置镜像(或快照)服务后实现信息系统的业务连续性。

3.3.2 服务器及数据库硬件资源选配

云资源中，服务器及数据库硬件资源(CPU、内存、硬盘)在增加配置能随时增加，但减少或降低配置时需在计费周期完毕后才能变化。建议在部署时根据系统开发商提出的需求降低档次购置资源，待运行后再行增加。

另一方面，云服务购买时有包年月和按需两种方式，建议都可先选择按需付费的方式购买，待试运行结束后再进行计费方式的切换。

3.4 安全防护产品方面

3.4.1 依托云应用防火墙防护

企业应用公有云服务后，云监控显示各类攻击事件都较机房时大大幅度的增高(站群每日 WEB 攻击都以十万做单位)。云应用后，对于域名发布(公网 IP 的也需设置域名)的需要部署应用防火墙产品来进行防护，并且配置时还需利用域名来隐藏后台的实际的服务地址及服务端口，同时，还需要将应用防火墙的回源 IP 设置在防火墙的下联产品中，

这样就能实现依托公有云应用防火墙来实现高可靠的信息系统应用层防护。

3.4.2　最小权限配置服务器安全组

云端服务器的安全组(ACL 控制)功能是云主机防护最有效、最灵活的地方，是网络层防护的核心，需要按照最小授权原则配置服务器的公网/内网 IP 的访问入/出方向的 IP 与端口。

云应用时，各服务器(含数据库实例)主机要更改各信息系统发布的服务端口(不能为默认的 HTTP 80 端口)和服务器运维(Windows 服务器不能为远程桌面默认的 3389 端口、Linux 的不能为 SSH 默认的 22 端口)端口，此为安全防护的基础。另外，还需对安全组配置后使得整个 VPC 网络下的服务器间默认不能互通(避免非法访问或攻击一旦侵入一台服务器后能扫描整个 VPC 下的服务器)；还需要全面梳理信息系统服务器间的数据流向，只放行必要的 IP 及服务端口；最后，建议以单台 ECS 服务器(或数据库实例)为一个安全组分类进行配置 ACL，不要将一个信息系统涉及的所有服务器(或数据库实例)合并一个安全组来配置，这样有助于安全防护的精度。

4　结论

中国能建应用公有云 IaaS 方面的有关产品有了一定的认识，对于公有云的 PaaS、SaaS 服务更了解甚少，还有对于 IaaS 的其他应用，如数据库安全服务，面向对象存储还处于了解概念阶段。云服务最大的优势是弹性计算，目前按需增配 CPU、内存、磁盘等也绝对不是弹性的真谛。此外，应用系统部署在公有云上，如何做好信息系统登录的防护需要统筹考虑。还有，各企业应用的 Oracle RAC 如何在公有云上实现迁移和满足性能的应用等等方面都需要去浩瀚的云深处不断探索！

参考文献：

[1]　董其强，刘海．企业混合云架构下的信息安全建设[J]．信息与电脑(理论版)，2018(5)：213-215.

[2]　覃宇阁．混合云环境下移动互联网安全体系探析[J]．通讯世界，2017(4)：3-4.

[3]　中华人民共和国国家质量监督检验检疫总局，中国国家标准化管理委员会．信息安全技术 信息系统通用安全技术要求：GB/T 20271—2006[S]．北京：中国标准出版社，2006.

作者简介：

WANG H M

王华明(通信作者)

1979-，男，湖北当阳人，高级工程师，通信专业学士，主要从事信息技术研究、信息化管理工作(e-mail) hmwang@ceec.net.cn。

殷金华

1967-，男，湖北广水人，教授级高级工程师，工程测量专业学士，主要从事信息技术研究、信息化管理工作。

(责任编辑　张春文)