医院云数据中心设计与实现

余莎莎 肖 辉 彭雄杰

（武汉大学中南医院信息中心 武汉 430071） （武汉市精神卫生中心 武汉 430012）

〔摘要〕 从天翼云区域划分、业务框架、云安全架构等方面阐述武汉大学中南医院云数据中心设计与实现，指出采用云数据中心可实现快速开通、弹性扩容、减少成本、运维便捷的目标，满足医院数据中心快速、弹性的建设需求。

〔关键词〕 云数据中心；医院信息化

〔中图分类号〕 R－058 〔文献标识码〕 A 〔DOI〕 10.3969/j.issn.1673－6036.2021.06.010

Design and Realization of Hospital Cloud Data Center *YU Shasha, XIAO Hui, Information Center, Zhongnan Hospital of Wuhan University, Wuhan 430071, China; PENG Xiongjie, Wuhan Mental Health Center, Wuhan 430012, China*

〔**Abstract**〕 The paper elaborates the design and implementation of the cloud data center of Zhongnan Hospital of Wuhan University from the aspects of e－cloud regional division, business framework, cloud security architecture, etc., points out that the adoption of cloud data center can achieve the goals of rapid opening, flexible expansion, cost reduction, convenient operation and maintenance, and meet the requirements of the rapid and flexible construction of hospital data center.

〔**Keywords**〕 cloud data center; hospital informatization

1 引言

传统三甲医院数据中心需采购满足要求的机房硬件、环控设备及应用软件，建设方式复杂，流程周期长；同时有限的运维人员不能满足医院信息化快速发展过程中管理和运营工作需求[1]。云计算是一种按使用量付费的模式，提供可用、便捷、按需的网络访问，计算资源采用共享池方式快速提供，只需投入很少管理工作[2]。面对交付时间紧迫，需快速部署的业务系统，减少基础设施建设周期成为当务之急[3]。医院机房不能采用传统自建数据中心模式，通过云上部署数据中心可极大减少建设时间与流程，仅需采购支持医院业务平台系统的云计算、云存储、云安全资源等服务和配套网络服务，即可快速上线应用系统。

2 设计方案

2.1 概述

中南医院对外业务系统及部分内网备份数据部署在中国电信天翼云武汉节点，采用两条不同路由云专线与医院互通。天翼云于 2019 年 4 月通过公安部信息系统等级保护 3 级评测，满足医院信息系统等级保护要求。云数据中心通过虚拟化技术将计算资源（CPU/NEIC/GPU/FPGA）、存储资源和网络资源构建成虚拟资源池[4]。医院采用 6 台独享天翼云物理服务器，虚拟化后部署近 20 台服务器，满

〔修回日期〕 2021－05－19

〔作者简介〕 余莎莎，硕士，中级工程师，发表论文 4 篇；通讯作者：肖辉，主任。

足医院信息系统运行所需要的计算资源要求。医院本地部署核心交换机、汇聚交换机等网络设备，医院互联网出口部署上网行为管理、下一代防火墙和负载均衡设备。

2.2 天翼云区域划分（图1）

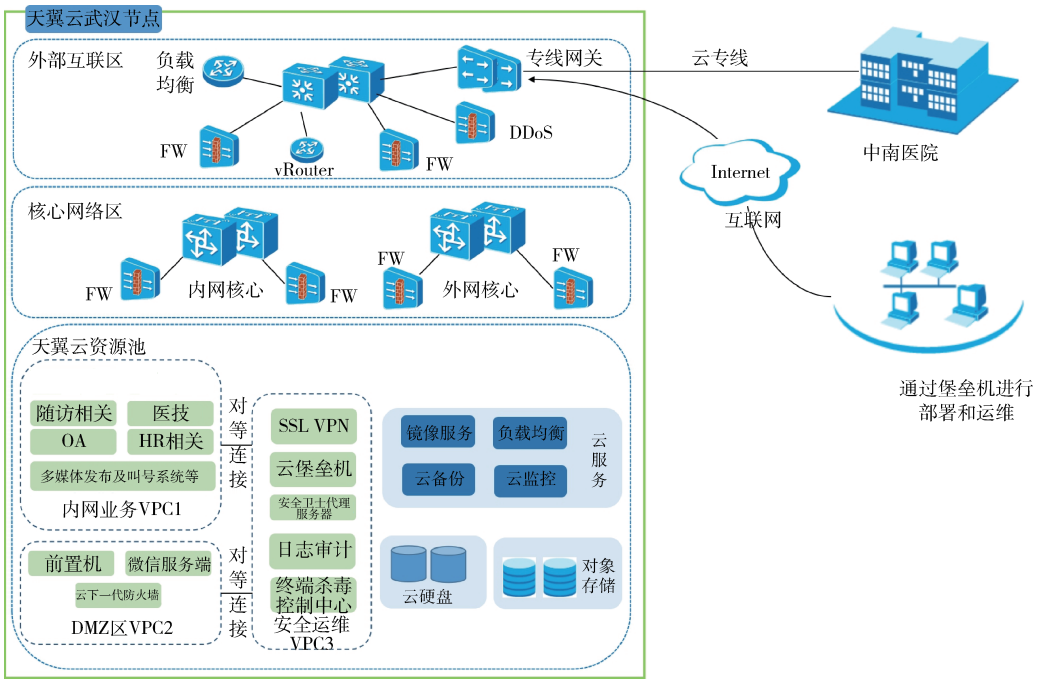

图1 天翼云逻辑分区

2.2.1 外部互联区域 包括互联网出口区、互联接入区及云专线（Direct Connect，DC）互联区，在互联网接入区部署专线网关，虚拟专用网（Virtual Private Network，VPN）防火墙，可实现中南医院通过电信专线接入。外部互联区域同时部署分布式拒绝服务（Distributed Denial of Service，DDOS），入侵检测系统（Intrusion Detection System，IDS）等设备，提供来自互联网的云层面流量清洗攻击防护、基于4层云安全防护以及应用层面的安全防护处理，为对外发布业务系统提供安全访问。所有外联流入流量都需要经过细粒度安全策略控制。

2.2.2 核心网络区域 包括内网和外网平面，内网平面承载整个云平台管理及运营，不对租户开放；外网承载租户及公网用户业务，服务器根据不同功能划分在不同分区，区域内部也分为内、外网两个平面，区域防火墙提供本区域与内、外网核心区互联及安全控制等功能。

2.2.3 云资源池区域 资源池包含云主机、物理机、云硬盘、对象存储等资源服务，提供镜像服务、负载均衡、云备份、云监控等功能性服务。管理员可以通过云主机部署业务系统，各业务系统可划分不同虚拟私有云（Virtual Private Cloud，VPC），通过虚拟私有云为公有云租户提供逻辑隔离区域[5]，在VPC上租户可申请弹性带宽和IP、创建子网、设置安全组及动态主机配置协议（Dynamic Host Configuration Protocol，DHCP）等，为租户提供更安全、经济、功能更完善的虚拟网络环境。租户互联网数据中心（Internet Data Center，IDC）和云上VPC互通可选择高速通道专线和VPN网关两种方式。为保证连接速率和效率，由两条不同路由的1G高速专线连接医院本地网络与天翼云。云主机资源池是由多台物理机组成的高可用集群，任何一台物理机出现故障都不影响业务系统正常运行。

2.3 医院业务框架

2.3.1 概述 云数据中心方案中，医院不再保留业务系统运行环境，前端业务系统与后端服务器数据交互与存储均交由云服务提供商所提供的高速专

用线路承载[6]。医院与云平台之间通过两条不同路由链路实现互为主备，保障链路高可靠性和效率。中南医院业务系统在天翼云上的部署分为 3 大区域，即内网区、非军事区（Demilitarized Zone，DMZ）和安全运维区，见图 2。

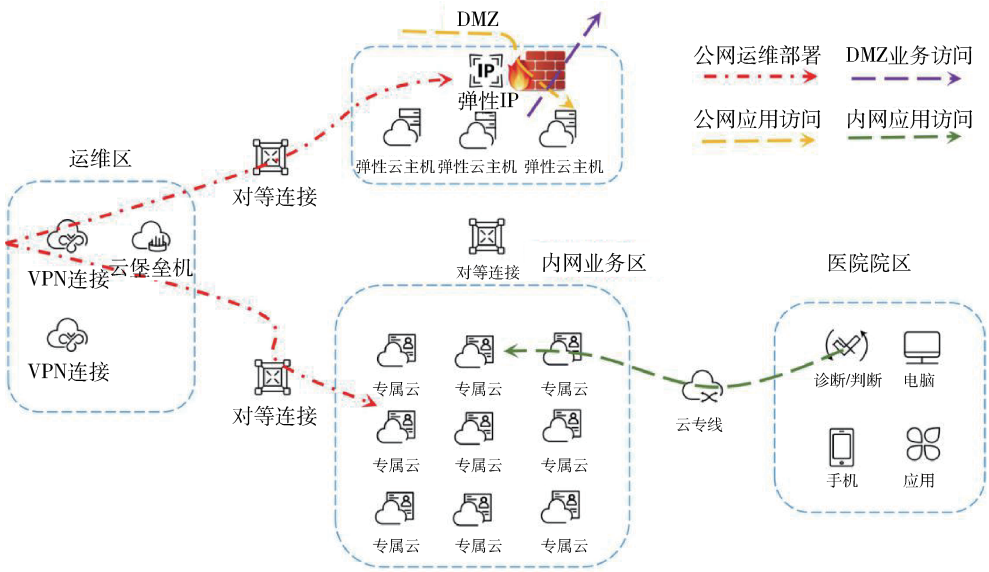

图 2 中南医院云数据中心分区

2.3.2 内网区 采用天翼云专属云资源池，部署医院医技及 OA 等应用系统备份数据，通过医院专线接入到云端，每个业务单独部署在业务子网内，每个子网由防火墙安全组进行入出方向访问控制。

2.3.3 DMZ 区 采用天翼云专属云资源池，部署与互联网具有交互需求的业务应用前置机，包括 HIS 第 3 方检验报告收发前置机、微信服务业务等，采取云下一代防护墙 + 安全组策略 + ACL 访问控制策略进行入出方向控制，DMZ 区服务器无法主动访问内网区。

2.3.4 安全运维区 采用天翼云主机，满足各软件厂家远程部署业务需求，通过 VPN 和堡垒机分为运维和业务子网，主要采用安全组策略进行访问控制。运维区流量通过安全组源地址和端口限制，利用对等连接实现与 DMZ 和内网区通信。

2.4 云安全架构

云数据中心安全措施包含两个方面，一是在数据中心物理和虚拟网络不同区域部署防护措施，天翼云提供 Anti - DDos 流量清洗、云下一代防火墙、服务器安全卫士等，形成物理和虚拟网络全覆盖的基础防御体系。二是在云安全中心部署安全态势感知[7]，实现对云上系统网络、应用、管理等方面的安全防护。为满足各应用厂家前期部署和运维需求，云数据中心部署运维 VPN（双机）和堡垒机（双机）。为满足 OA 移动办公需求，部署业务 VPN（双机），从物理上将运维和应用需求 VPN 接入隔离。此外为方便将云主机防护检测报告通过邮件告知用户，部署服务器安全卫士代理服务器，通过安全组控制内网和 DMZ 各云主机上的安全卫士实现单向通信。所有云主机部署服务器安全卫士、日志审计和杀毒软件进行安全防护，所涉及堡垒机、下一代防火墙、VPN 等安全产品均采取双机部署，保证系统高可用性。

3 建设成效

3.1 医院数据中心建设更快

中南医院对外业务区基础设施环境搭建时间不足 10 天，采用云上部署方式可以极大减少采购硬件、运输组装时间，仅需向云资源运营商提出需求，云资源交付时间短，为软件部署调试预留更多

时间。云上资源、数据空间充足，如有需要可以通过镜像快速复制一套同样的数据中心，满足快速搭建要求。

3.2 机房建设投入更少

信息中心人员不仅对应用系统、硬件设备、机房不断电系统（Uninterruptable Power System，UPS）及精密空调等环控设备进行管理和维护，必要时还需要到 IDC 机房现场实施维护。云资源按需订购付费，运维主要由云资源运营商负责，信息中心人员只需维护相关应用。

3.3 数据管理效率更高

数据安全风险是医院信息安全防范重点，医院需要从各个层面加强数据安全管理，从数据采集、存储、传输、处理、交换到销毁各环节展开全生命周期保护。由于医疗数据具有海量小文件的特性，导致医院产生大量沉默数据。采用云上部署数据中心可提升数据敏捷度，增强全量数据管理能力。

3.4 机房扩容更便捷

本地化机房空间不足时只能重新采购硬件设备，流程、时间长，无法快速满足医院需求。医院使用云资源具有弹性扩容特点，满足系统建设初期资源快速增长、迅速开通的需要。

4 结语

虚拟化技术发展突飞猛进，其成熟可靠性得到广泛验证，已成为企业级数据中心建设的主流方案技术，而云计算技术发展又不断推动基于虚拟化平台的云数据中心建设浪潮[8-9]。采用云上部署医院数据中心，可实现快速开通、弹性扩容、减少成本、运维便捷的目标，满足医院数据中心快速建设需求。在医院日常数据中心建设中，云上部署可以将一次性 IT 投入成本变为每年均匀运营费，减少医院现金流压力，同时还可减轻信息中心人员运维压力，使其将更多精力集中在信息化建设中。未来云上部署医院数据中心将成为信息化发展的重要方向[10]。本文介绍的中南医院云数据中心建设经验对相关医院有一定参考价值。

参考文献

1 马军，闫若玉，王斌，等. 基于混合云架构的医院数据中心的建设［J］. 中国医疗设备，2019，34（1）：95－97.

2 孙瑛，朱刘松. 浅析云计算在医院信息化建设中的应用［J］. 中国中医药图书情报杂志，2014（2）：660－661.

3 刘阳，文霞. 基于混合云技术的医院 IT 架构研究［J］. 中国数字医学，2018，13（7）：93－95，103.

4 何嘉，彭商濂. 云数据中心虚拟机管理研究综述［J］. 电子科技大学学报，2016，45（1）：107－112.

5 陈晓健. 谈云机房网络建设［J］. 中国科技信息，2018（17）：52－53.

6 杨秀峰，曹晓均，周毅，等. 全院信息系统基于公有云托管服务的探索与实践［J］. 中国数字医学，2016，11（4）：90－92，89.

7 耿延军，王俊，周红亮. 云数据中心网络纵深防御研究［J］. 信息安全与通信保密，2019（7）：22－29.

8 王磊，吴晓芬，郑云肆，等. 医院云数据中心设计和应用［J］. 医学信息学杂志，2018，39（1）：26－29，50.

9 赵禹. 利用虚拟化技术瘦身医院 IT 系统［J］. 中国管理信息化，2017，20（5）：142－144.

10 彭建明，王蓓. 新疆维吾尔自治区人民医院分院信息系统整体上“云”实践［J］. 中国数字医学，2018，13（5）：49－51.