医院云灾备建设探索与实践*

谢 君

（四川大学华西医院信息中心/医疗信息化技术教育部工程研究中心 成都 610041）

李俊忠

（四川省第二中医医院/四川省中医药科学院中医研究所 成都 610015）

师庆科

（四川大学华西医院信息中心/医疗信息化技术教育部工程研究中心 成都 610041）

郑小华

（四川省卫生信息学会 成都 610015）

罗以强

（四川省第二中医医院/四川省中医药科学院中医研究所 成都 610015）

〔摘要〕 以四川省第二中医医院为例，分析灾备架构建设现状及需求，提出基于云计算环境的异地灾备架构，阐述云灾备方案设计、实施结果、建设成效，指出该实践有助于降低成本和管理难度，提高灾备管理质量。

〔关键词〕 灾难恢复；云计算服务；云灾备；异地备份；连续数据保护

〔中图分类号〕R－058 〔文献标识码〕A 〔DOI〕10.3969/j.issn.1673－6036.2022.06.013

Exploration and Practice of Hospital Cloud Disaster Recovery Construction *XIE Jun, Information Center of West China Hospital, Sichuan University/Engineering Research Center of Medical Informatization Technology, Ministry of Education, Chengdu 610041, China; LI Junzhong, Sichuan Second Hospital of Traditional Chinese Medicine/Sichuan Institute of Traditional Chinese Medicine, Chengdu 610015, China; SHI Qingke, Information Center of West China Hospital, Sichuan University/Engineering Research Center of Medical Informatization Technology, Ministry of Education, Chengdu 610041, China; ZHENG Xiaohua, Health Information Association of Sichuan Province, Chengdu 610015, China; LUO Yiqiang, Sichuan Second Hospital of Traditional Chinese Medicine/Sichuan Institute of Traditional Chinese Medicine, Chengdu 610015, China*

〔**Abstract**〕 Taking Sichuan Second Hospital of Traditional Chinese Medicine as an example, the paper analyzes the construction status and requirements of disaster recovery architecture, proposes a remote disaster recovery architecture based on cloud computing environment, expounds the design, implementation and construction results of the cloud disaster recovery scheme, and points out that the practice is helpful to reduce the input cost and management difficulty, and improve the quality of disaster recovery management.

〔**Keywords**〕 disaster recovery; cloud computing service; cloud disaster recovery; remote backup; Continuous Data Protection (CDP)

〔修回日期〕 2021－10－24

〔作者简介〕 谢君，工程师，发表论文 5 篇；通信作者：师庆科，工程师。

〔基金项目〕 四川省中医药管理局“中国－阿曼苏丹国‘互联网＋’中医药服务国际合作方式方法研究”（项目编号：2021MS182）。

1 引言

基于对业务系统数据的安全保护，当前大多数医院已经建设灾备系统，不同程度实现医院重要业务数据的容灾备份，以保障业务的高可用性。随着医院业务规模扩大、网络安全形势日益严峻，医院在设施设备、机房管理、信息安全管理等方面对数据灾备建设提出了更加严格的要求[1]。而云计算、持续数据保护技术的快速发展，网络带宽的提升，云计算服务模式的成熟，为医院在云上进行灾备建设（云灾备）创造了条件。云灾备基于云计算环境，利用云服务器作为灾备机，将数据通过网络通道从本地备份到云端并提供系统迁移、应用切换、应急接管等灾备手段。其所需云计算能力、数据存储量、网络带宽等指标均可以服务方式提供，按需分配[2]。四川省第二中医医院为提高灾难恢复能力，规划、探索云灾备服务类项目，在原有以超融合平台及相应备份系统形成的灾备架构基础上，增加部署云灾备相关系统，实现对重要数据的异地保护，进一步提升业务数据高可用性。

2 现状及需求分析

2.1 概述

四川省第二中医医院已建设有医院信息系统（Hospital Information System，HIS），检验信息系统（Laboratory Information System，LIS），医学影像存储与传输系统（Picture Archiving and Communication System，PACS），电子病历（Electronic Medical Record，EMR）等业务系统。HIS 数据总量大约 350GB，每年增量约 20GB。当前已经对 HIS 进行本地容灾备份，形成一定程度的高可用架构。

2.2 超融合平台以多副本方式实现虚拟机备份

HIS 等系统部署于超融合平台，以多副本方式进行虚拟机数据冗余，实现基于硬件及虚拟机环境的高可用性[3]。当一个虚拟机系统崩溃时，其他虚拟机副本可将系统快速拉起，迅速恢复系统应用。然而当超融合平台本身出现故障甚至完全崩溃时多副本机制无法发挥作用，虚拟机中的数据库文件无法提取，必须借助超融合平台外的容灾机制进行业务恢复。

2.3 Oracle DG 实现数据本地实时备份

搭建 DG 服务器，以 Oracle DataGuard 方案实现与 HIS 服务器的实时同步[4]。该方式所备份数据为实时数据，当超融合平台发生故障、无法启动时可立即将服务器切换为应急 HIS 服务器并启动 HIS 服务。但应用该方式同时存在一定弊端，一旦本地出现勒索病毒攻击、备份数据库文件被破坏时，该备份数据将无法使用，无法起到应急恢复作用。

2.4 备份一体机实现业务数据定时备份

由 1 台备份一体机与 HIS 服务器定时交互，每 2 小时对数据进行 1 次增量备份，每天凌晨对数据进行 1 次全量备份。该方式可以说是前两种方式的“兜底”防护手段。因一体机具有较强反入侵功能，且 HIS、DG 服务器文件被破坏后，一体机中的备份文件因安全性高不会被连带破坏，具有院内数据在本地的堡垒作用。但该方式弊端较明显，由于是定时模式，恢复时医院将最多得到备份时间窗口为 2 小时的数据，无法恢复到当机时最新数据状态。HIS 涵盖医疗、财务、药品等重要信息，系统崩溃、数据丢失将导致全院医疗秩序混乱、业务无法运转，甚至会造成不同程度的社会影响。为保障业务系统在因病毒攻击、自然灾害等原因受到破坏、业务中断时，能快速恢复数据和业务运转、确保医疗秩序，数据在异地实时容灾备份建设显得尤为重要[5]。

3 云灾备方案设计

3.1 概述

按照数据“异地异质”的灾备要求，基于医院现有灾备建设现状，结合医院物理格局受限、无法建设专业备用机房的实际情况，考虑开展云灾备建设。通过开通院内异地实时备份点、云端备份以加强灾备能力，解决医院本地发生灾难时的数据恢复

问题。

3.2 灾备时间指标设计

3.2.1 指标定义 恢复时间目标（Recovery Time Objective，RTO），即灾难发生后从系统停机导致业务停顿开始，到系统恢复可以支持业务运营之时所需要的时间。恢复点目标（Recovery Point Objective，RPO），即发生意外灾难事件时可能丢失的数据量[6]。

3.2.2 指标设定 HIS、LIS、PACS、EMR 等系统作为医院核心业务系统，一旦灾难发生需保证数据零丢失，同时查找原因、迅速恢复，尽量缩短业务中断时间。因此无论采用哪种灾备方式，RPO 应设计为接近于零，即能恢复至灾难刚发生时的最新数据。而对于 RTO，如果从增建的本地灾备服务器中进行数据恢复，RTO 为系统切换、服务启动时间之和，要求在 30 分钟以内。如果从云灾备服务器中进行恢复，此时意味着发生了严重灾难，院内机房及本地备份均不可用，RTO 为数据合成、数据传输下载、系统启动恢复等时间之和，要求在 15 小时以内。

3.3 技术选择

要保证 RPO 接近于零的结果，需选择连续数据保护（Continuous Data Protection，CDP）技术对数据予以采集传输。CDP 是一种对数据在连续时间点进行保护的技术，其价值在于能在故障瞬间完成任何时间点的故障恢复，达到保证业务快速、连续的作用。这从根本上解决了传统备份中低恢复能力和非精细时间策略的问题，理论上消除了备份窗口时间。并且与目前基于存储复制的容灾数据复制技术不同的是，CDP 除了对灾难导致的数据物理破坏提供保护外还能对逻辑错误导致的数据破坏提供保护。

3.4 容灾备份流程设计

3.4.1 云灾备架构 在医院远程会诊室专用弱电间设置本地备份服务器，云端设置云灾备服务器，各服务器中安装部署备份系统服务端。在源数据库服务器上安装 CDP 备份代理程序，利用 CDP 技术实时传输 HIS 数据，见图 1。

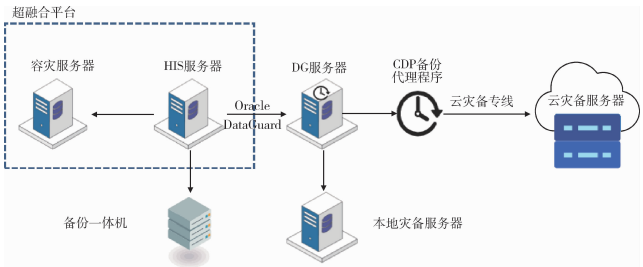

图 1 云灾备架构

3.4.2 容灾备份流程 备份代理程序从操作系统驱动层对数据库文件夹进行监控，捕捉文件所有访问操作，实时监控文件发生的一切变化，实时提取数据变化部分及变化发生时间戳后，通过内网传输至本地备份服务器，同时通过云灾备专线传输至云灾备服务器进行存储[7]。

3.5 数据应急恢复流程设计

以假定本地机房所有备份文件不可用而必须从云端恢复，将数据及时恢复至指定时间点为前提来设计数据应急恢复流程。云灾备数据恢复流程如下：首先，备份系统对云灾备服务器中的备份进行数据合成，即解析备份数据并根据日志文件将其恢复至指定时间点。其次，将得到的恢复文件通过专线传输至本地灾备服务器并导入数据库。为减小带宽压力、缩短传输时间，对数据在传输前进行压缩，传输后进行解压。最后，进行系统启动恢复，即将恢复后的数据库文件在业务系统中导入并启动系统，以保障业务系统继续可用，见图 2。

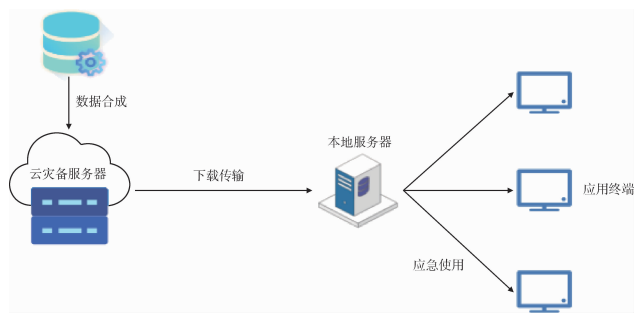

图 2 恢复应急流程

3.6 灾备软件功能设计

3.6.1 架构及技术 对灾备软件要求采用浏览器/服务器（Browser/Server，B/S）架构，以 Web 访问方式进行业务管理。采用 CDP 技术，以字节级复制方式对生产端数据进行连续数据保护，实时同步到灾备服务器。对专线占用极低、不影响现有的业务系统运行。

3.6.2 功能实现 支持文件数据的增量、全量备份，支持自定义存储周期[8]、备份时间，可在后台自动运行无需人工干预，同时能有效防御勒索病毒的破坏。支持多种常用文件格式并通过压缩方式传输数据，以减少带宽占用量。

3.7 云服务购置

3.7.1 云计算服务模式 当前云计算服务模式正在快速发展，可将信息化项目所需基础设施、平台、软件等以服务形式提供给需方，需方可采购整体服务，此类案例已较为普遍。云计算服务模式包括以下 3 类：一是软件即服务（Software as a Service，SaaS），其将应用作为服务提供给客户；二是平台即服务（Platform as a Service，PaaS），其将开发、运行平台作为服务提供给用户；三是基础设施即服务（Infrastructure as a Service，IaaS），其将网络、虚拟机或者其他资源作为服务提供给用户。

3.7.2 云服务购置方式 在该院云灾备服务项目中，网络资源、机房、服务器硬件等按照 IaaS 方式提供；备份软件及部署运行按照 SaaS 方式提供；虚拟机、服务器操作系统等按照 PaaS 方式提供。云服务器操作系统采用虚拟化 Linux 系统以提高安全性、稳定性[9]，保障备份任务 7 × 24 小时不间断运行[10]。专线设计为带宽 50Mbps、上下行对称的传输通道。云服务器部署及备份软件安装配置、运行维护以及相应专线、带宽等由云服务商作为整体服务提供，医院以租用形式购买。

4 实施结果

4.1 灾备时间指标测算评估

4.1.1 灾备时间指标随带宽变化测试结果 在当前系统数据量的条件下，经测试各 RPO 约等于 0。在当前带宽为 50Mbps 的条件下，经测试数据合成时间为 3.5 小时、数据传输下载时间为 18.3 小时、系统启动恢复时间为 0.5 小时，此时 RTO 约 22.3 小时，见表 1。

表 1 灾备时间指标随带宽变化测试结果

带宽（M）	数据合成时间 A（小时）	数据传输下载时间 B（小时）	系统启动恢复时间 C（小时）	RTOA + B + C（小时）	RPO
50	3.5	18.3	0.5	22.3	0
100	3.5	9.2	0.5	13.2	0
200	3.5	4.6	0.5	8.6	0
500	3.5	1.8	0.5	5.8	0

4.1.2 其他情况 如果只需以本地数据文件在遭受破坏最后一刻的实时备份来恢复数据，由于云灾备服务器中已实时存储全量最新数据，该数据与生产库完全一致，无需数据合成过程，即数据合成时间为 0，RTO 将进一步缩短。例如，根据表 1 结果，50Mbps 带宽下，RTO 将由原来的 22.3 小时变为 18.8 小时。100Mbps 带宽下，RTO 将由原来的 13.2 小时变为 9.7 小时。

4.2 灾备时间指标与云服务配置关系分析

4.2.1 缩短 RTO 可以提升云服务配置 数据合成是备份系统在云服务器中的数据解析处理过程，数据合成时间与计算能力、内存等云服务器性能有较大关系。在数据量一定的情况下，性能越高合成时间越短。数据传输下载时间取决于带宽，带宽越大下载时间越短。因此缩短 RTO 可以提升云服务配置。

4.2.2 配置与成本之间需要做好平衡 配置越高成本越高。云灾备是医院数据保护的最后一道防线，医院能容忍在多少时间内恢复数据并长期付出多少成本守住这一道防线，是一个值得思考的问题。数据的完整性、应用的连续性、恢复的及时性与成本之间需要做好平衡[11]。经对成本、预期 RTO 目标等因素综合考虑，医院将原设计的 50Mbps 扩容为 100Mbps。

5 建设成效

5.1 加强业务高可用性和灾难恢复能力

通过该项目实施，HIS 生产库数据实现异地实时备份，RPO 约等于 0，RTO 为 13.2 小时，达到预期目标，业务系统容灾能力得到进一步提升，业务恢复时间进一步缩短。

5.2 云灾备建设以服务形式交付，起到降本增效作用

医院不必一次性花费大量资金投入到基础设施、系统及软件采购上，只需支付每年的服务费用，节省大量成本。同时减少信息团队备份系统相关硬件巡视、管理等基础工作的负担[12]，将更多精力聚焦在备份管理工作上，从而减少软硬件运维人力投入。将项目建设以服务方式进行交付，使得信息化建设进一步回归服务本质。医院只需要购买服务，按需响应、按需扩容，确保服务效果即可[13]。医院在享受专业化服务的同时进一步提升灾备效益。

5.3 不足与下一步计划

本次建设由于为探索性建设，只对 HIS、LIS 数据进行云灾备。随着预期目标的达成、项目应用及管理的成熟，将进一步加大投入，扩大备份范围，将 PACS、EMR、体检等业务系统纳入云灾备对象，以加强医院业务系统的高可用性。

6 结语

云灾备建设实施 1 年多来系统总体表现平稳高效，专线网路稳定可靠，服务满意度较高，实现基于云计算环境的核心系统数据异地灾备，加强对医院核心数据资产保护，达到最初的设计目标[14]。以购买服务方式进行云灾备建设，按需分配、弹性扩容，在降本增效的同时有效提升医院灾难恢复能力，最大程度降低数据丢失风险，将数据保护的最后一道防线从机房筑到云端，是医院灾备建设的重要方式和新趋势。

参考文献

1 韩成果，金树柏，任嘉曦. 基于天翼云的中小企业数据保护及容灾备份研究［J］. 计算机时代，2019（12）：47－50，53.

2 刘周. 从传统灾备技术到云灾备技术架构初探［J］. 金融科技时代，2020，28（8）：33－37.

3 宋阳，范根，郝泽余，等. 医院双院区超融合资源池设计与建设［J］. 中国数字医学，2021，16（5）：70－74.

4 曹婷，王坤，陈芳. 基于医院信息系统容灾措施的研究与实践［J］. 中国数字医学，2014，9（8）：100－103，106.

5 中国国家标准化管理委员会. 信息安全技术信息系统灾难恢复规范［EB/OL］.［2021－04－02］. https://www.doc88.com/p－98173094245346.html.

6 张云，何懋，周帆帆. 基于混合云的医院容灾系统设计与实现［J］. 电子技术与软件工程，2020（23）：189－190.

7 黄志刚，郭玉东，杨宗博. 文件级 CDP 的设计和实现［J］. 计算机应用，2008，28（S2）：277－279.

8 周松柏，冯昌琪. 构建 PACS 系统云存储［J］. 中国数字医学，2011，6（4）：111－112.

9 黄思文. 虚拟化大型医院数据中心容灾建设［J］. 医学信息学杂志，2017，38（3）：40－42.

10 孟晓阳，朱卫国，苏博，等. 大型医院信息系统业务连续性方案研究［J］. 医学信息学杂志，2017，38（10）：26－30.

11 马锡坤，吴艳君，王鹏. 基于云计算的数据中心容灾系统的建设［J］. 中国医疗设备，2014，29（1）：93－95.

12 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.

13 金忠林，吴福强，俞小萍. 医院信息系统数据云灾备服务模式的探索与实践［J］. 中国数字医学，2018，13（10）：101－102，111.

14 聂海鑫，冯迟. 云存储在医院中的应用方向［J］. 医疗卫生装备，2013（34）：102－103.