

数字政府政务云容灾备份系统建设思路

李锐

(中通服咨询设计研究院有限公司, 江苏 南京 210019)

【摘要】本文介绍了信息系统灾备概念和相关规范标准,对政务云发展及其在灾备系统建设中面临相关问题和实际需求进行了研究,并结合两者情况,对政务云灾备系统建设思路进行了阐述和总结,以期对政务云灾备系统建设提供参考。

【关键词】政务云;容灾备份;两地三中心;双活

一、概述

我国政府信息化建设在过去30年的发展中已走过了三个阶段,第一个阶段主要以提升政府内部行政事务办公自动化为主,重点在电子化和网络化。第二个阶段主要以资源建设和管理为主,期间结合了云计算、大数据的应用,形成了政务云的形式,并迅速推广开来,政务云的建设极大地提高了政府信息化水平,并为后续政府职能转变提供了基础。随着数字经济和数字社会的出现和发展,政府开始数字化转型,朝着建设数字政府的方向前进,迈入第三个阶段。新的前进方向在技术和制度方面都需要有相应创新支撑。政务云作为技术平台,肩负起了承担数字政府基石的重任,各级政府要求对非涉密政务系统是“应上尽上”,最终实现100%在政务云上运行。业务系统都运行在政务云平台上,一些关键业务存有大量重要的、敏感的、机密的数据,尤其是面向民生服务的,如人社、财政、税务等数据,是政府极为重要的资产,一旦发生业务系统故障,导致数据丢失或损坏,会对政府部门造成严重的经济损失,甚至会发生严重的公共事件和社会影响,如何确保数据安全与业务连续性既是重点也是难点^[1]。

政务系统中的重要数据备份是基本要求,在数据备份的基础之上,提供业务连续性的容灾方案,也逐渐成为政务云系统的常规要求,各地政府在公布的省、市政务云建设规划中纷纷对容灾备份提出明确要求。

二、政务云灾备系统建设挑战

(一)主动性不足。容灾备份包含两个概念,容灾是以遭遇灾难时能保证业务连续性为目标,以RTO(recovery time objective)恢复时间目标为指标;而备份的目标则是为了应对数据丢失问题,以RPO(recovery point objective)恢复点目标

为指标。政务云中的备份系统投资规模一般在百万级别,而容灾系统整套投资至少上千万级别。政务云实际建设过程中往往因为预算原因,灾备系统建设优先级较为靠后,或只建设备份系统或采用部分容灾技术,或采用备份/灾备一体机的方式应对检查,存在巨大安全隐患^[1]。

(二)缺乏具体规范指导。灾备体系建设主要依据国际Share 78标准和国家标准《信息系统灾难恢复规范》(GB/T 20988-2007)。在《信息系统灾难恢复规范》中通过对备用基础设施、数据备份系统、备用数据处理系统、备用网络系统、灾难恢复预案、运行维护管理能力、技术支持能力七个关键要素综合分析,将灾难恢复划分为六个等级,不同的容灾能力等级对业务系统的保护效果可以通过RTO、RPO衡量,《信息系统灾难恢复规范》中只列出了某行业的参考对应关系如表1所示^[3],政务云参考时难度较大。

表1 某行业容灾等级对应参考表^[3]

容灾恢复等级	RTO	RPO
第1级	2天以上	1天至7天
第2级	24小时以上	1天至7天
第3级	12小时以上	数小时至1天
第4级	数小时至2天	数小时至1天
第5级	数分钟至2天	0至30分钟
第6级	数分钟	0

因为容灾系统会把生产系统的变化完全复制到容灾端去,包括错误和异常导致的非业务期望结果,此种情况下就需要从备份系统中取出最近的备份进行期望恢复,因此容灾系统还不能完全替代备份系统的功能。而政务云建设者在备份和容灾是否需要分步建设、谁先谁后等问题上,因为缺少相关具体规范和建设指导,容易出现滞后或超前建设的情况,不利于

政务云系统的健康演进。

三、政务云灾备系统建设思路

(一) 参考规范 and 标准

随着数字政府建设的深入，政务应用服务的持续可靠运行要求越来越高，《GW0013-2017 国家电子政务外网标准：政务云安全要求》中提出关于等保三级信息系统的的核心数据安全及备份恢复要求，包括：应建立异地灾难备份中心，配备灾难恢复所需的通信线路、网络设备和数据处理设备，提供业务应用的实时无缝切换^[4]。随后出现的团体标准《电子政务云灾备体系建设规范》中按业务核心功能中断影响将应用系统的重要程度分为了五类，对应灾难恢复五个等级，同时也对应到GB/T 20988附录A中的第2~6级^[5]。

表 2 政务云容灾等级对应表

业务级别	灾难恢复等级	关键指标要求	GB/T 20988 对应级别
关键业务	第五级	$RTO \leq 15 \text{ 分钟}$ $RPO=0 \text{ 分钟}$	第 6 级
重要业务	第四级	$RTO \leq 1 \text{ 小时}$ $RPO \approx 0 \text{ 分钟}$	第 5 级
较重要	第三级	$RTO \leq 4 \text{ 小时}$ $RPO \leq 1 \text{ 小时}$	第 4 级
一般	第二级	$RTO \leq 24 \text{ 小时}$ $RPO \leq 24 \text{ 小时}$	第 3 级
次要	第一级	$RTO \leq 7 \text{ 天}$ $RPO \leq 36 \text{ 小时}$	第 2 级

上述两项标准的提出，为政务云的灾备系统建设提供了较为细致的参考，综合考虑灾难发生后的恢复时间、落实与维护灾备策略所需的投入等因素（容灾恢复时间的需求越短，成本和难度就越大），对政务云灾备需求分析如表 3。

表 3 政务云灾备建设分类需求

业务分级	应用特征描述	容灾需求	备份需求
关键业务	指支撑中央政务机构的一项或多项政务职能，或省级以上各层政务机构日常运作，或面向省级及以上公众范围提供服务。若数据损坏或服务中断将存在长期性的财政、民生影响。	应用双活	本地备份 + 异地备份
重要 / 较重要	指对单位运营必要的 IT 应用，该类应用对维持业务运作的控制是所必需的，若数据损坏或服务中断将影响到多个部门，造成直接的重大财务或社会影响。	主备容灾	本地备份 + 异地备份
一般 / 次要	指应用中断会导致一些不便，造成较小的财务或社会影响，但数据不允许丢失。	无	本地备份

(二) 备份建设思路

备份是为了防止数据丢失，采取某种策略和计划，在指定时间内将需要备份的数据写入备份介质。常见的备份类型如下表 4 所示：

表 4 常见备份类型清单^[6]

备份类型	描述	优点	缺点
全量备份	将需要备份的数据源完全备份到目的地中。	最常见的类型。恢复方便。	备份耗时较长，且恢复备份，因此占用存储空间相对较多。
增量备份	只备份自上一次备份（完全备份或增量备份）后新增或变化的数据。	备份数据量小，备份速度快。	所需恢复时间比完全备份或差异备份所需时间相对要长。
差异备份	执行差异备份时，仅备份自上次完全备份后新增或变化的数据。	备份数据量小，备份速度比完全备份快。	恢复数据所耗费的时间比完全备份相对要长。如果数据变化量大，其所耗费的时间比增量备份时间相对要长。

1. 本地备份方案

在政务云本地中心中设计预留云备份空间，实现对业务系统和数据的统一备份保护。合理采用数据压缩或数据重删等技术，对云平台下的主机整体进行数据保护，同时降低带宽使用率，提高介质空间的使用率。使用云备份软件构建云备份服务，实现对云主机和数据库的备份。

对云主机备份，主要通过镜像快照技术，实现对云主机状态的备份，并保证回滚功能。此部分主要使用全量备份和增量备份组合。

数据库备份，主要包括 MySQL、PostgreSQL 等轻载数据库，其数据备份和其所属云主机备份一致，

通过镜像、快照技术实现。

2. 异地备份方案

指按照一比一比例,将本地备份数据全部进行异地备份,考虑需要依靠异地备份恢复风险发生概率相对较低,主要防范机房、数据中心级别严重灾害。

为确保在有限的带宽、有限的时间窗口内,能够完成数据复制任务,为提高数据容灾效率,采用技术手段主要包括数据压缩、全局源端重复数据删除、断点续传、云主机自动异地恢复。

(三) 容灾建设方案

容灾是指灾害发生时,还能保证IT系统正常运行,关注业务连续性,容灾包括数据级、应用级、业务级,本文指业务容灾,需要建立双中心,以对业务系统提供相同的处理,双中心一般是建立在同城范围内(距离<50公里),并通过高速链路(裸光纤或波分设备)进行数据实时同步,相互独立但互为备份并可切换运行,在意外的情况下通过业务连续性管理系统切换服务,将业务无感切换到另一机房,保证业务的连续性。包括主备、热备、双活三种方案:

热备,当主部件或者设备发生故障时,通过设置的热备能够自动顶替,对业务毫无影响的故障切换^[7]。

冷备,相比热备而言,冷备不像热备那么及时自动地解决问题,需要人为干预,这中间的过程可能会造成业务的不可用甚至数据丢失^[7]。

双活,当其中一个数据中心发生软、硬件故障或者灾难时,另外一个数据中心能够在无需人工干预的情况下,自动、快速、安全地将应用、网络流量切换过来,保证业务前端应用无感知,业务零停顿,应用零影响,保证业务的连续性^[7]。双活相比于热备而言,可提高灾备中心资源利用率。

(四) 演进型政务云灾备系统建设思路

演进型灾备系统建设以综合场景、技术健全、全周期管理为原则。设计考虑云备份与恢复、同城灾备、异地灾备等多重场景,综合应用存储、数据库、网络层、应用层等全技术栈,采用同城双中心加异地灾备中心的“两地三中心”的灾备模式^[8],同城双活中心通过裸光纤或波分设备连接,异地中心通过专网连接。

根据项目实际情况,一般建议采用分步实施的方式,先建立同城的灾备中心,再建立异地的灾备中心。异地灾备中心应当与政务云本地中心保持较远的距离(建议200公里以上)^[8],以便在火灾、洪水、地震等重大灾难出现时仍然能有效保证数据的安全性和业务的连续性^[9]。

四、结束语

政务云的安全和可用性要求会随着政府数字化转型的发展不断提高,容灾备份系统作为基础环节,规划建设适合自身发展的灾备系统,对提高系统的风险抵御能力十分紧迫。由于灾备系统建设涉及基础设施、硬件设备、网络、数据库、云计算及软件等多方面技术和产品,专业性和融合度较高,是一个持续性、发展性的长期工程,常常是一个分步实施的过程,因此其分步的经济性和适用性十分关键,本文通过梳理灾备概念、相关技术,结合政务云业务在灾备方面的需求和对应方案,给出了政务云灾备系统具体建设思路,对当前各级政务云建设有较好的参考意义。值得一提的是,灾备相关技术的发展也是日新月异,例如容灾云平台^[10]、多活数据中心、云灾备技术^[11],合理地使用都可能给政务云带来更高的资源利用率、更丰富的业务可用性体验。

参考文献:

- [1] 郭婵娟.扬州市政府云计算中心容灾备份建设实践[J].中国信息化,2019(8):67-69.
- [2] 王晓冬,王皓磊.中国政务信息系统灾备体系建设研究[J].电子政务,2014(12):108-114.
- [3] GB/T 20988-2007 信息系统灾难恢复规范[S].北京:中国标准出版社,2007.
- [4] 许超彬.政务云平台容灾备份系统建设思路研究[J].电子测试,2019(13):122-123.
- [5] T/ZBLM 0001-2023 电子政务云灾备体系建设规范[S].北京:北京信息灾备技术产业联盟,2023.
- [6] 吕彤,闫仲毅,梁晓.国产化环境下检察业务应用系统备份问题研究[C]第二届新时代优秀检察成果·智慧检务建设论文集(二),2021.
- [7] 陈荣山,姚婕,吴昊.从单机到双活数据中心建设的思考[J].科技创新与应用,2023(5):169-172.
- [8] 王智,尹长林,许文强.政务云“两地三中心”容灾备份体系研究与设计[J].网络安全和信息化,2021(4):28-33.
- [9] 胡宗贤,毕丹宏,唐宇.电子政务云存储与灾备设计方案研究[J].电信快报,2017(12):21-24.
- [10] 韦宇星.广西政务云“两地三中心”多服务灾备设计与实现[J].无线互联科技,2022(23):75-77.
- [11] 邹汉铮,巴刚,杨加富.关于数字时代云容灾备份中心设计及应用方法研究[J].通讯世界,2022(7):35-37.