

中国灾备技术 和行业白皮书 2018（修订版）

中国灾备技术和行业白皮书 2018（修订版）

上海英方软件股份有限公司

《中国灾备技术和行业白皮书 2018（修订版）》编审委员会

顾问

于 天 国际灾难恢复协会中国分会（DRI China）总裁

颜 军 北明软件有限公司 首席技术官

主编

胡军擎 上海英方软件股份有限公司 CEO

副主编

周 华 上海英方软件股份有限公司 CTO

吴开宇 上海英方软件股份有限公司 CDO

编委会（按姓氏笔画排列）

王 晨 刘东昌 刘小亮 任祥旺 李 光 严 俊 林广生

张宝君 张高翾 秦金龙 黄 亮 黄继生 焦新军 符云波

程 权 崔立达 曹智丹

校对：刘圣明 程 松 赵 春

装帧设计：陶 梅 文荣金

内容简介

经过长期的行业推广应用，以及越来越多的组织单位对灾备重视程度的提升，中国灾备市场得到了空前的发展。但另一方面，由于灾备知识普及不够，以致于很多行业人士对灾备基础知识如容灾与备份等业务界限并不十分清楚，导致沟通的成本太高，以及客户对灾备产品能够达到的预期值偏高。

在此背景下，本白皮书的定位为灾备行业基础性科普读物，力求尽量全面地向读者呈现灾备的相关概念、术语、法规条文，以及技术原理、流派、趋势和灾备行业市场、特点、解决方案等内容，并希望借此白皮书达到抛砖引玉的效果，让更多的人参与到灾备行业的宣传推广工作中来。

白皮书共分为六个章节。在第一章重点介绍灾备的起源、概念、灾难恢复衡量指标、灾备等级、国内外标准和认证，以及近几年灾备市场规模等。第二章重点阐述灾备的相关技术，包括数据复制技术、切换技术、数据加密与传输技术、常见存储常态及对应架构、灾备相关技术创新等知识。第三章则以近年兴起的云灾备为内容，从云灾备的定义、发展历程、具体业务模式和产品形态等方面介绍云灾备。第四章详细介绍灾备建设三部曲及灾备服务质量评价体系，以期给行业客户在灾备项目规划建设及服务商甄选方面提供指导帮助。第五章是白皮书的重点内容，详细介绍灾备在政府、金融、医疗、教育、制造业、电信、互联网、电力能源等领域的行业概览、需求和解决方案及未来趋势。第六章主要谈灾备行业的趋势，包括云灾备、智能化、信息安全、演练和人才储备等五个方面。

希望灾备行业的从业者及感兴趣的读者，能够从白皮书的六个章节中获得相关的知识内容。

此次白皮书的撰写、修订历时大半年，极大地丰富了2016版白皮书的章节内容。在此也要特别感谢行业多位专家，以及英方十几位高级售前工程师对重点章节内容提出的宝贵意见。与此同时，在白皮书编写的过程中，我们也借鉴了相关出版物、网络权威文章及行业报告：

- [1] 刘鹏, 罗圣美, 赵淦森. 中国云存储发展报告 [M]. 北京: 电子工业出版社, 2013.
- [2] 曹志平, 杨鹏, 张均宝, 王梓峻, 李毅. 未来就绪的信息系统架构 [M]. 上海: 复旦大学出版社, 2016.
- [3] 《公共安全 - 业务连续性管理体系要求》国家标准 (GB/T 30146-2013).
- [4] 《从传统银行到互联网，异地多活究竟有多难？》吴磊、冯浩、左左, 2017.
- [5] 《云灾备技术与应用白皮书》北京信息灾备技术产业联盟, 2017.

前言

未雨绸缪，有备无患

中国互联网应用技术的日新月异，正在加速以互联网商业为中心的生态圈建设。企业为了能够全天候不间断地为用户提供服务，必须保障其购物网站稳定可靠地运行，尤其是在每年一度的“双11”购物疯狂节期间，企业更是必须确保其电商网站对外服务的连续性。因此，业务连续性管理已受到越来越多包括电商在内的企业的高度重视。

近十年来，虽然业务连续性管理已在中国的金融、电信等大型企业得到越来越多的应用，但其应用范围仍局限在少数关键领域，其他更多的行业对其认知度还不够高，还没有认识到业务连续性管理与其生存和发展的紧密关系。

事实上，在很多重大的灾难事件中，比如“汶川地震、911恐怖袭击、卡特里娜飓风”等，由于许多企业没有建立业务连续性管理体系和制定业务连续性计划，遭受了无法挽回的重大损失。

另一方面，随着中国社会信息化指数的不断提升，云计算、大数据、人工智能等前沿科技的蓬勃发展，给人类生活和生产带来诸多便利的同时，也遭受越来越多的网络攻击、勒索病毒、钓鱼软件等日益猖獗的威胁。如何确保组织的信息安全及业务连续性，使组织从容应对各种大灾小难，是大多数企业共同面临的挑战。

而灾难恢复（灾备）在实现组织业务连续性目标中又起着至关重要的作用，因此，研究探讨灾备技术的发展，总结各种实用有效的灾备方案及其实施经验，供各行各业的相关从业人员在实践中加以参考，就是件非常有意义

的事。英方公司作为中国灾备领域的长期实践者，能够投入如此多的时间，组织许多经验丰富的专家将自己长期在各行业灾备项目实践中积累的宝贵知识和心得总结出来，并编写成灾备技术白皮书无私地分享出来，实在是难能可贵。

国际灾难恢复协会（DRI International）是一个非营利的学术机构，其致力于通过专业的培训活动来推广有关业务连续性和灾难恢复的知识，并对个人进行有关 BC/DR 领域国际权威的从业资格认证。

作为国际灾难恢复协会中国分会（DRI China）的负责人，我多年来有幸参与和见证了中国各行各业的灾备建设与发展，并从业务连续性管理角度为许多企业的灾备建设提供了自己的建议，帮助企业理解业务连续性管理办法对灾备建设的重要指导意义。尤其是很高兴能与像英方这样的专注于灾备产品开发和服务并掌握核心灾备技术的专业公司合作，共同在各行业推广业务连续性管理和灾备技术的知识和应用，帮助各企业做好应对各种突发事件的准备，确保企业具备抵抗任何灾害袭击的能力，正所谓“未雨绸缪，有备无患”。

这本汇集各方专家见解的灾备技术白皮书涵盖的内容很全面，涉及的技术很专业。据我所知，中国目前像这样全面系统地论述灾备技术专业资料并不多见，免费公开的就更少。英方公司从 2016 年起就一直坚持不懈地花费大量时间组织多方专家编写中国灾备技术白皮书，并无私地供广大灾备从业者分享，确实体现了英方公司作为灾备行业领先者的应有担当。

国际灾难恢复协会中国分会总裁 于天

让世界早有准备！

当今世界，以互联网产业化、工业智能化和工业一体化为代表的第四次工业革命已经悄然到来。在这个进程中，全新的技术革命带来数据信息瞬息万变的交汇、管理和利用，并普惠社会的方方面面。

中国是这场技术革命的参与者和引领者之一，中国政府从“互联网+”到“中国制造2025”，与时俱进地为全行业指明了未来发展的方向。中国高铁、移动支付、量子通信、北斗导航等一张张响彻世界的中国名片，是产业信息化带来的生产效益和经济效益快速提升的必然结果。在这些宏大的产业信息化领域，越来越多的人和单位已经意识到，信息安全保障体系的作用非常关键。为此，中国政府已经将信息安全的工作提升到国家战略高度，并制定相关的法律法规贯彻下去。

灾备，被誉为对企业信息安全的最后一道防线，是新时代产业信息化运营的保障体系之一。它的终极目标是确保组织单位的数据不丢，业务不停，在规定的时间内持续、稳定地对外提供服务。我觉得，这也是英方的价值所在。今天，英方已经能够为客户快速找回丢失的数据，能够让用户的业务永续，并在操作的过程中，摒弃了以往传统容灾备份诸多的不确定性，让整个灾备的运维体系更加便捷、智能、安全和经济。

这一切离不开信息技术日新月异对行业带来的利好。英方作为一家长期专注于容灾及业务高可用领域的高新科技企业，时刻关注着灾备领域国内外的最新动态，并在长期的灾备建设实践中总结了很多宝贵的实战经验。

这本白皮书是我们全国各地一线工程师厚积薄发的工作成果，特别是在行业实践方面，本书非常详细地阐述了八个主要行业的灾备情况，希望能够给大家带来启迪，同时也希望大家多提宝贵意见，共同服务行业的健康发展。

未雨绸缪，防患未然，让世界早有准备！这是英方人的使命。我们深知抵达这一使命的艰辛与不易，但这并不能撼动我们将灾备事业进行到底的决

心。板凳要坐十年冷，在软件这个高科技行业，在过去，中国企业长期处于模仿学习的阶段，但是随着中国全球发展战略的提速，核心软件技术国产化，我们正处于迈向弯道超车的绝佳黄金时期。

一个民族有一群仰望星空的人，这个民族才有希望。今天，构建高效的IT资产保护体系，服务全球客户，英方人的愿景正在一步步的实现。

上海英方软件股份有限公司 CEO 胡军擎

目 录

第一章 灾备行业基础知识概述

1. 1 灾备的起源	1
1. 2 灾备的重要性	2
1. 3 灾备行业术语	2
1. 3. 1 数据备份	2
1. 3. 2 业务连续性	5
1. 3. 3 灾难恢复衡量指标	8
1. 4 灾备的三个等级	9
1. 4. 1 数据级灾备	10
1. 4. 2 应用级灾备	10
1. 4. 3 业务级灾备	10
1. 5 灾备行业国内外标准及认证	12
1. 5. 1 国际标准	12
1. 5. 2 国家标准	15
1. 5. 3 中华人民共和国网络安全法	17
1. 5. 4 DR 及 BCM 相关认证	17
1. 6 灾备市场规模	18
1. 6. 1 中国市场	18
1. 6. 2 全球市场	20

第二章 灾备关键技术分类

2.1 数据复制技术	21
2.1.1 基于主机操作系统的数据复制	21
2.1.2 基于应用和中间层的数据复制技术	22
2.1.3 基于数据库的数据复制技术	23
2.1.4 基于存储系统的网关的数据复制	24
2.1.5 基于存储介质的数据复制	25
2.1.6 同步与异步复制方式	28
2.1.7 快照技术	29
2.1.8 数据一致性	30
2.2 切换技术	31
2.2.1 网络切换技术	32
2.2.2 应用切换技术	33
2.3 重复数据删除技术	35
2.4 数据加密与传输技术	35
2.4.1 源端加密	36
2.4.2 传输加密	36
2.5 三种常见存储形态及对应架构	37
2.5.1 块存储与直接附加存储	38
2.5.2 文件存储与网络附加存储 (NAS)	40
2.5.3 对象存储与分布式存储架构	41
2.6 相关技术创新	41
2.6.1 灾备与 SDS	41
2.6.2 灾备与容器	43
2.6.3 灾备与超融合	44
2.6.4 灾备与云计算	45
2.6.5 边缘计算和云灾备	46

第三章 云灾备

3.1 云灾备	47
3.1.1 云灾备的定义与发展历史	47
3.1.2 云灾备的特点	49
3.1.3 云灾备实施注意事项	51
3.1.3 虚拟化及混合云化	53
3.2 云灾备的具体业务模式	54
3.2.1 SaaS 层灾备	54
3.2.2 PaaS 层灾备	54
3.2.3 IaaS 层灾备	55
3.2.4 DRaaS（灾难恢复即服务）	55
3.3 云灾备的主要产品形态	56
3.3.1 云迁移	56
3.3.2 云备份与恢复	57
3.3.3 云高可用	59

第四章 灾备业务实施及服务质量评价

4.1 灾备建设三部曲	61
4.1.1 业务连续性规划	61
4.1.2 灾备规划	62
4.2 灾备规划的方法	63
4.2.1 风险分析与业务影响分析	63
4.2.3 灾备计划制定	64
4.2.4 灾备方案实施	64
4.2.5 灾备演练	65
4.2.6 专家服务（ADTIS）	66
4.3 灾备服务质量评价	68

4.3.1 功能性要求	68
4.3.2 可靠性要求	68
4.3.3 性能效率要求	69
4.3.4 信息安全要求	69
4.3.5 易用性要求	69

第五章 重点行业灾备建设特点及方案分析

5.1 政府及组织灾备建设特点及方案分析	72
5.1.1 行业概览	72
5.1.2 需求与解决方案	72
5.1.3 行业趋势	79
5.2 金融行业灾备建设特点及方案分析	80
5.2.1 行业概览	80
5.2.2 需求与解决方案	82
5.2.3 行业趋势	91
5.3 医疗行业灾备建设特点及方案分析	92
5.3.1 行业概览	92
5.3.2 需求与解决方案	93
5.3.3 行业趋势	98
5.4 教育行业灾备建设特点及方案分析	99
5.4.1 行业概览	99
5.4.2 需求与解决方案	100
5.4.3 行业趋势	105
5.5 制造行业灾备建设特点及方案分析	106
5.5.1 行业概览	106
5.5.2 需求与解决方案	108
5.5.3 行业趋势	110
5.6 电信行业灾备建设特点及方案分析	111

5. 6. 1 行业概述	111
5. 6. 2 需求与解决方案	112
5. 6. 3 行业趋势	118
5. 7 互联网行业灾备建设特点及方案分析	119
5. 7. 1 行业概览	119
5. 7. 2 需求与解决方案	120
5. 7. 3 行业趋势	125
5. 8 电力能源行业灾备建设特点及方案分析	126
5. 8. 1 行业概览	126
5. 8. 2 需求与解决方案	127
5. 8. 3 行业趋势	131

第六章 灾备技术及行业未来发展趋势

6. 1 云灾备将成为主要形势之一	132
6. 2 智能化成为灾备的下一个趋势	132
6. 3 灾备是网络信息安全的重要保障	133
6. 4 演练在灾备系统变得日益重要	135
6. 5 灾备人才队伍建设正在加快	135

第一章 灾备行业基础知识概述

灾备，即灾难备援，在IT系统中是指利用科学的技术手段和方法，提前建立系统化的数据应急方式，以应对灾难的发生。随着灾备业务的不断更新，灾备的外延也越来越广，不仅包括数据备份和系统备份，业务连续规划、灾难恢复规划、灾难恢复预案、业务恢复预案，还包括通信保障、危机公关、紧急事件响应、第三方合作机构和供应链危机管理等等。

1.1 灾备的起源

20世纪70年代，灾备概念兴起于美国。从顾名思义，灾备是灾难备份的缩略语，而从更严格意义上说，信息系统的灾备应当是指信息系统的灾难备份与恢复，这它包含两层含义：灾难前的备份与灾难后的恢复。正如存储专家Jon Toigo所言，DR/BC规划对那些打算应对那些100%引起财务危机的5%宕机的人来说是个挑战。你不能用灾难事件的概率和频率来麻痹自己。准备好应对那5%，你也能轻松应对剩下的95%。

1979年，SunGard在美国费城建立了全世界第一个灾备中心，当时人们关注的主要是企业IT系统的数据备份和系统备份等。后来，IT备份发展到了灾难恢复规划（DRP），并在IT备份中加入了灾难恢复预案、资源需求、灾备中心管理，形成了对生产运行中心的保障概念。再后来，人们进行灾难恢复规划时从仅考虑保护IT系统的角度逐渐扩展到考虑IT所支持业务的角度，根据保护业务的要求来衡量灾备的目标：哪些业务最重要？哪些业务可容忍的恢复时间最短？

除此之外，灾备规划中加入了业务影响分析、策略制定、业务恢复预案、人员架构、通信保障、第三方合作机构等，并最终融入到业务连续性规划（BCP）之中。美国911事件后，灾备进一步从全面风险管理的角度出发，除了面向业务，还有了紧急事件响应、危机公关和供应链危机管理等等。

1.2 灾备的重要性

在灾备概念兴起之后，越来越多的机构开始对灾备的重要程度进行了量化的分析。美国德克萨斯州大学的较早的一次调查显示：“只有 6% 的公司可以在数据丢失后生存下来、43% 的公司会彻底关门、51% 的公司会在两年之内消失。”另一份针对这一课题的研究报告也显示：在灾难之后，如果无法在 14 天内恢复信息作业，有 75% 的公司业务会完全停顿，20% 的企业在两年之内被迫宣告破产。美国明尼苏达大学的研究也表明，在遭遇灾难的同时又没有灾难恢复计划的企业中，将有超过 60% 在两到三年后退出市场。而随着企业对数据处理依赖程度的递增，该比例还有逐渐上升的趋势。

IDC 在全球范围内，针对多个行业的中小型企业（员工数小于 1000 名）的调研显示，近 80% 的公司预计每小时的停机成本至少在 2 万美元以上，而超过 20% 的企业估算其每小时的停机成本至少为 10 万美元。

2016 年灾备行业的一份可用性报告显示：企业每年因应用停机所造成的损失达到 1600 万美元，可用性差距进一步扩大。报告指出，尽管去年发生了诸多备受瞩目的停机事件，但依然没有引起足够的重视。全球 84% 的资深 IT 决策者（ITDMs）承认，他们正在经历“可用性差距”的困境，这一数字较之 2014 年增长了 2%。

1.3 灾备行业术语

在灾备行业，有很多专用术语，随着组织对数据资产的重视，这些行业术语也逐渐走进人们的视线，并成为灾备某个领域的代名词。

1.3.1 数据备份

数据备份是容灾的基础，是指为防止系统出现操作失误或系统故障导致数据丢失，而将全部或部分数据集合从应用主机的硬盘或阵列复制到其它存储介质的过程。

按照备份数据量，可以分为：全量备份、增量备份、差量备份。

全量备份——用存储介质对整个数据及系统进行完全备份。这种备份方式的好处是很直观，容易被人理解，易恢复；缺点是在备份数据中有大量重复数据，由于需要备份的数据量相当大，因此备份所需时间较长。

增量备份——每次备份的数据只是相当于上一次备份后增加和修改后的数据。这种备份的优点很明显：重复数据少，即节省磁带空间，又缩短了备份时间；缺点在于当发生灾难时，数据恢复比较麻烦。

差量备份——是拷贝所有新产生或更新的数据，这些数据都是最近一次全量备份后产生或更新的。

增量备份与差量备份的区别是，增量备份判断数据更新标准是依据上一次备份检查点，而差量备份一定是依据全量备份检查点。如没有全量备份，就没有差量备份。差量备份的主要目的是限制完全恢复时使用的介质数量。

	全量备份	增量备份	差异备份
备份方法	备份所有文件	备份自从上一次备份后的全部改动和新文件	备份自从上一次完全备份后的全部改动和新文件
备份速度	最慢	最快	较快
恢复速度	最快	最慢	较快
空间要求	最多	最少	较多

表 1.3-1 三种备份方式比较

按照备份时间频率，可以分为定时备份和实时备份。

定时备份——是指有时间间隔的数据备份方式，比如一天一次，一周一次，或者一个月一次，定时备份不能保证数据的零丢失。

实时备份——是指无时间间隔的数据备份方式，通过实时数据复制，保证主备两端的数据读写一致，确保数据的零丢失。

CDP（continual data protection）是一种连续数据保护技术，被称为高级

的实时备份，它兼具数据备份与数据恢复的功能，通过 CDP 实时备份技术，可以实现到秒级的细粒度抓捕效果，英方股份 i2CDP 能够提供细粒度数据持续保护，可恢复至任意历史时间点。

此外，根据数据备份时服务器是否停机又可分为冷备和热备；按照数据存储介质之间的距离又可以分为本地备份和异地备份。

在国内，基于高可用系统中的两台服务器的热备（或高可用）使用较多，因此双机热备的术语常被人提起。双机热备按工作中的切换方式分为：主 - 备方式（Active-Standby 方式）和双主机方式（Active-Active 方式），主 - 备方式指的是一台服务器处于某种业务的激活状态（即 Active 状态），另一台服务器处于该业务的备用状态（即 Standby 状态）。而双主机方式即指两种不同业务分别在两台服务器上互为主备状态（即 Active-Standby 和 Standby-Active 状态）。注：Active-Standby 的状态指的是某种应用或业务的状态，并非指的是服务器状态。

严格意义上讲，双机热备不属于备份，更像是容灾。容灾，从广义上讲，任何提高系统可用性的措施都可称之为容灾。

本地容灾，一般指主机集群，当某台主机出现故障，不能正常工作时，其他的主机可以替代该主机，继续进行正常的工作。

异地容灾，是指在与生产机房有一定距离的异地建立与生产机房类似的信息平台（备份中心），并采用特定的技术将生产中心的数据传输到该备份中心，从而在生产中心发生较大的灾难如火灾或地质灾害时，仍能对生产数据进行保护的容灾系统。

一个容灾系统的实现可以采用不同的技术，而容灾系统的划分，由其最终要达到的效果来决定。从其对系统的保护程度来分，可以将容灾系统分为数据级容灾和应用级容灾。

容灾半径是衡量容灾方案所能承受的灾难影响范围的一个指标（如图 1.3-1 所示）。不同灾难的影响范围是不同的，而距离也会影响到容灾技术

的选择。比如在地震灾难频发的地区，对关键信息保护必须做好容灾备份，尤其是异地容灾备份是十分必要的。做异地容灾备份，必须保证三百公里之外，同时还必须做到“三不”，即不在同一地震带，不在同一电网，不在同一江河流域。

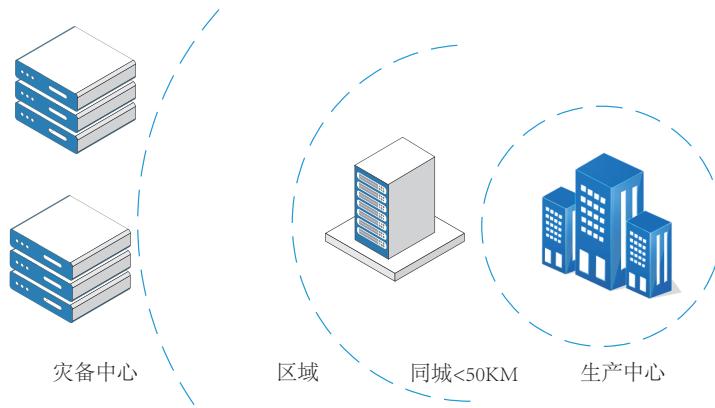


图 1.3-1 容灾半径

备份与容灾的区别：备份是为了应对灾难来临时造成的数据丢失问题，容灾是为了在遭遇灾害时能保证信息系统能正常运行，帮助企业实现业务连续性的目标。备份系统与容灾系统在容灾备份一体化产品出现之前是相互独立的两个系统，容灾备份产品的最终目标是帮助企业应对人为误操作、软件错误、病毒入侵等“软”性灾害以及硬件故障、自然灾害等“硬”性灾害。

1.3.2 业务连续性

业务连续性（Business Continuity）是指在中断事件发生后，组织在预先确定的可接受的水平上连续交付产品或提供服务的能力。它明确一个机构的关键职能以及可能对这些职能构成的威胁，并据此采取相应的技术手段，制定计划和流程，确保这些关键职能在任何环境下都能持续发挥作用。业务连续性（BC）针对的事件场景应包括三类：一般故障（Outage）、紧急事件（Emergency）和灾难事件（Disaster）。实现业务连续性所需的IT措施包含三个方面：业务状态数据的备份和复制、业务处理能力的冗余和切换、外部接口冗余和切换。

业务连续性管理（Business Continuity Management，简称 BCM）是一套一体化的管理流程，通过该流程可识别组织面临的潜在威胁以及这些威胁一旦发生可能对业务运行带来的影响，并为组织提供了一个指导框架来建立有效应对威胁的自我恢复能力，从而保护关键相关方的利益、声誉、品牌和创造价值的活动。

业务连续性管理是一个长期的、不断完善的循环过程，需遵循国际标准的 PDCA 循环模型，即策划（Plan）—实施（Do）—检查（Check）—改进（Act）。

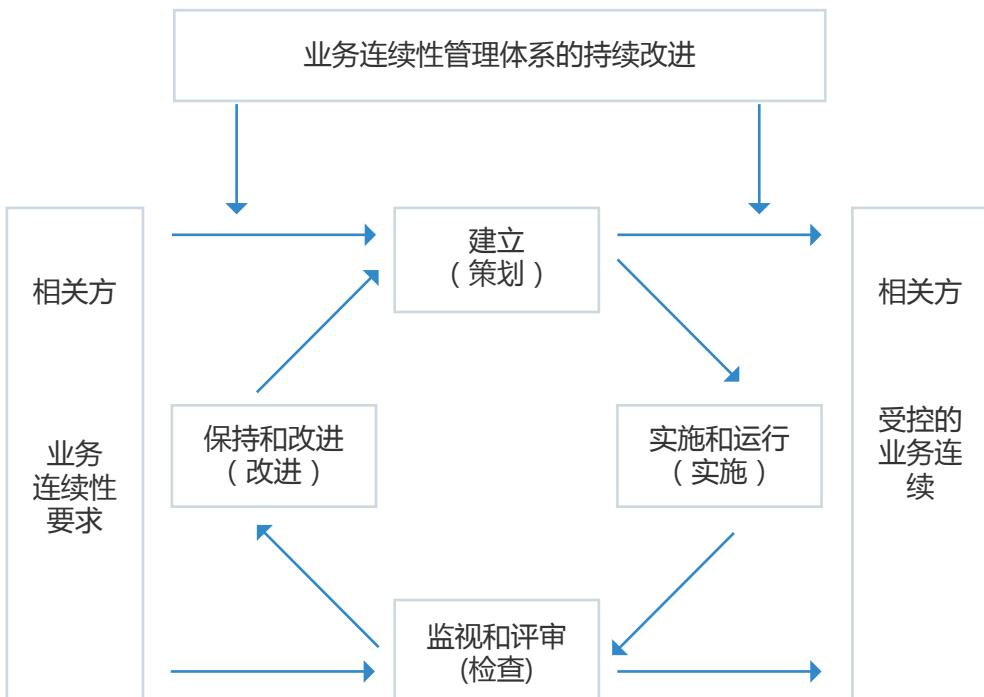


图 1.3-2 应用于业务连续性管理的 PDCA 模型

业务连续性管理为企业的灾备建设提供了基本原则和方法，业务连续性管理确定的业务恢复目标就是设计灾备方案的依据。首先，按照业务连续性管理方法对潜在的灾难事件加以识别并进行分析，从而确定可能造成企业运行中断的威胁，以及业务中断给企业带来的影响和损失；然后再根据业务中断的影响及其恢复时所需的资源来制定灾难恢复策略，从而使灾难事件给企业带来的损失最小化。它含盖了风险管理、应急管理、IT 灾难恢复、设备管理、

资源管理、安全管理、人员管理等多项内容。

实现业务连续性的技术手段通常包括以下两种：

1. 高可用性（High Availability，简称 HA）

指的是通过技术手段，尽量缩短因日常维护操作（计划）和突发的系统崩溃（非计划）所导致的停机时间，以提高系统和应用的可用性。业界的通行做法是采用群集系统（Cluster），将各个主机系统、网络系统、存储设备（部分高可用系统包含存储设备的高可用）等通过各种手段有机地组成一个群体，共同对外提供服务。

通过创建群集系统（采用实现高可用性的软件）将冗余的高可用性的硬件组件和软件组件组合起来，以达到消除单点故障、减少设备意外发生时的宕机时间。一般说，高可用技术通过对网卡、CPU、内存、系统软件设置不同的可用性监测点，在这些节点发生故障时实现冗余切换，持续提供服务。

然而，传统的高可用技术（如双机热备）并不能有效应对数据或者软件逻辑故障所造成的意外宕机情况，如人为误操作、网络病毒攻击等，近几年兴起的 CDP（Continuous Data Protect 持续数据保护）技术，在面对业务各类风险事件时的高级别的应急技术则可以看做是高可用的有效补充与扩展（当然，CDP 技术也融合了备份、快照等多种技术于一体）。

以 i2CDP 为例，i2CDP 为关键数据提供持续的、不间断的保护，可根据需求将数据快速恢复到之前的任意时间点。i2CDP 在将变化的数据实时复制到灾备中心的同时，也将数据的变化以日志方式记录下来，实现对数据变化的可回溯，依据数据变化日志，快速定位需要恢复的时间点，将数据一键式恢复到异常点之前。这些都是对传统高可用技术面对意外时的短板的修复和有效补充。

2. 灾难恢复（Disaster Recovery）

灾难恢复（DR）（国内通常简称为灾备或容灾）属于业务连续性的技术层面。在信息服务中断后，调动资源，在异地重建信息技术服务平台（包

括基础架构、通信、系统、应用及数据），灾难恢复也包括本地的恢复与重建。

目前，流行的灾备系统往往包括本地的 HA 集群和异地的 DR 数据中心。从故障角度，HA 主要处理单组件的故障导致负载在集群内的服务器之间的切换，DR 则是应对大规模的故障导致负载在数据中心之间做切换。从网络角度，LAN 尺度的任务是 HA 的范畴，WAN 尺度的任务是 DR 的范围。从云的角度，HA 是一个云环境内保障业务连续性的机制，DR 是多个云环境间保障业务连续性的机制。从目标角度，HA 主要是保证业务高可用，DR 是保证数据可靠的基础上的业务可用。

1.3.3 灾难恢复衡量指标

在灾难恢复方面，组织会考虑两个方面的目标恢复能力：RTO 与 RPO。

RTO（Recovery Time Objective）恢复时间目标

在运行中断情况下，基于可接受的停机时间和可接受的性能水平所制定的重建和恢复功能或资源的时间目标。根据标准定义，RTO 是从中断时刻到恢复至可接受水平所需的时间，这不仅包含了容灾恢复的时间，还包含了宣布灾难之前的应急处置和判断决策等时间。而且 RTO 针对的是造成中断的事件，并不一定是灾难事件。RTO 值越小就意味着所要求的恢复能力越强。

RPO（Recovery Point Objective）恢复点目标

为使活动能够恢复进行，而必须将该活动所用的信息恢复到某时间点。“恢复点”是指中断前最后一次备份数据的时间点，这意味着当需要恢复时所需修复或追补的数据量。如果 RPO 等于零，就意味着要求数据零丢失。否则为了恢复业务处理，就需要对丢失数据进行修复或追补。



图 1.3-3 RPO 与 RT0

RTO 针对的是服务丢失，RPO 针对的是数据丢失，两者是衡量容灾系统有两个主要指标，但它们没有必然的关联性。RTO 和 RPO 的确定必须在进行风险分析和业务影响分析后根据不同的业务需求确定，对于不同企业的同一种业务，RTO 和 RPO 的需求也会有所不同。当然，对于组织而言，最好的情况是 RPO=0，RTO=0，但显然这种情况是个理想状态。

此外，随着对业务恢复指标的进一步细分，还可引入降级运行目标 DOO、网络恢复目标 NRO、任意时间点回退 APIT 等指标。

DOO（Degraded Operations Objective）降级运行目标

是指灾难事件发生期间数据中心不可用时，关键业务系统在灾备中心运行的服务级别允许降低到一个可接受程度。这意味着灾难事件发生时，为了加快恢复速度，可以允许关键业务恢复到一个较低的服务级别，这个事先确定的允许降低的服务级别就是 DOO。DOO 反映了业务连续性的常用策略。

NRO（Network Recovery Objective）网络恢复目标

是指在灾难发生后切换到灾备中心所需的时间。在这一预定时间内不仅要求将网络连接从数据中心切换到灾备中心，还要使用户的网络访问能够成功地转移到灾备中心。

APIT（Any Poit In Time）任意时间点回退

在数据发生逻辑错误时，我们需要对破坏的数据进行恢复，这时 CDP 持续数据保护技术的衡量标准可以用任意时间点回退进行评判。

1.4 灾备的三个等级

根据恢复的目标与需要的成本投入，灾备大体可以分为三个等级，如图 1.4-1 可以用三个嵌套的同心圆表示，从数据级灾备、应用级灾备到业务级灾备，业务恢复等级逐步提高，而需要的投资费用也相应增长。

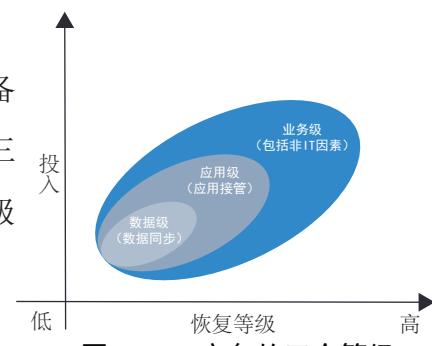


图 1.4-1 灾备的三个等级

1. 4. 1 数据级灾备

数据级灾备强调数据的备份和恢复，包括数据的复制、备份、恢复等在内的数据级灾备是所有灾备工作的基础。在灾备恢复的过程中，数据恢复是最底层的，比如数据必须完整一致后数据库才能启动，之后才是启动应用程序，应用服务器接管完成后，才能进行网络的切换。这个流程需要严格执行才能确保灾备的顺利切换。很多应用在切换的过程中之所以会失败，数据“没起来”是其中一个重要的因素之一。

数据级灾备的关注点在于数据，即灾难发生后可以确保用户原有的数据不会丢失或者遭到破坏。较低级的数据级灾备可通过将需要备份的数据用人工方式保存到异地来实现，比如将备份的磁带定时运送到异地保存。较高级的数据灾备方案则依靠基于网络的数据复制工具，实现生产中心和灾备中心之间的异步 / 同步的数据传输，比如采用基于磁盘阵列的数据复制功能（基于数据库的复制方式可分为实时复制、定时复制和存储转发复制）。

1. 4. 2 应用级灾备

应用级灾备强调应用的具体功能接管，它提供比数据级灾备更高级别的业务恢复能力，同时也是业务级灾备的基础，只有具体应用得到恢复，后续的业务才能有效进行。

应用级灾备是在数据级灾备的基础上把应用处理能力再复制一份，也就是在异地灾备中心再构建一套支撑系统。该支撑系统包括数据备份系统、备用数据处理系统、备用网络系统等部分。应用级灾备需要具备提供应用接管的能力，即在生产中心发生故障的情况下，能够在灾备中心接管应用，从而尽量减少系统停机时间，提高业务连续性。

1. 4. 3 业务级灾备

业务级灾备是最高级别的灾备建设，如果说数据级灾备、应用级灾备都是在 IT 系统的范畴之内，业务级灾备则是在以上两个等级的灾备基础上，还需考虑到 IT 系统之外的业务因素，包括备用办公场所、办公人员等，而

且业务级灾备通常对支持业务的 IT 系统会有更高的要求（RTO 在分钟级）。

对于正常业务而言，仅有 IT 系统的保障还是不够的。当一场大的灾难发生时，用户原有的办公场所都会受到破坏，用户除了需要原有的数据、原有的应用系统，更需要工作人员在一个备用的工作场所能够正常地开展业务。实际上，业务级灾备还关注业务接入网络的备份，不仅考虑支撑系统的服务能力，还考虑服务使用者的接入能力、甚至备份的工作人员。

表 1.4-1 给出了以上三种灾备等级的 RTO 与 TCO 对比：

级别	定义	RTO	TCO 总拥有成本
数据级	<p>指通过建立异地容灾中心，做数据的远程备份，在灾难发生之后确保原有的数据不会丢失或者遭到破坏。但在数据级灾备这个级别，发生灾难时应用是会中断的。</p> <p>在数据级灾备方式下，所建立的异地灾备中心可以简单地把它理解成一个远程的数据备份中心。数据级灾备的恢复时间比较长，但是相比其他灾备级别来讲它的费用比较低，而且构建实施也相对简单。</p> <p>数据源是一切关键性业务系统的生命源泉，因此数据级容灾必不可少。</p>	<p>RTO 最长（若干天），因为灾难发生时，需要重新部署机器，利用备份数据恢复业务。</p>	最低

应 用 级	<p>在数据级灾备的基础之上，在备份站点同样构建一套相同的应用系统，通过同步或异步复制技术，这样可以保证关键应用在允许的时间范围内恢复运行，尽可能减少灾难带来的损失，让用户基本感受不到灾难的发生，这样就使系统所提供的服务是完整的、可靠的和安全的。</p>	RT0 中等 (若干小时)	中等。 异地可以搭建一样的系统，或者简单些的系统。
业 务 级	<p>业务级灾备，除了具有应用级灾备所需的 IT 相关技术，还要求具备全部的基础设施。其大部分内容是非 IT 系统（如电话、办公地点等），当大灾难发生后，原有的办公场所都会受到破坏，除了数据和应用的恢复，更需要一个“备份”的工作场所有能够正常的开展业务。</p>	RT0 最小 (若干分钟或者秒)	最高

表 1. 4-1 灾备等级对比

1.5 灾备行业国内外标准及认证

1.5.1 国际标准

(1) SHARE78

目前通用的灾难恢复标准采用的是 1992 年在 AnaheimM028 会议上制定的 SHARE78 标准，在该标准中阐述了灾难恢复的 7 个层级：

Tier0 层：没有异地数据 (No off-site Data)

即没有任何异地备份或应急计划。数据仅在本地进行备份恢复，没有数据送往异地。事实上这一层并不具备真正灾难恢复的能力。

Tier1 层： PTAM 卡车运送访问方式 (Pickup Truck Access Method)

灾难恢复方案必须设计一个应急方案，能够备份所需要的信息并将它存储在异地。PTAM 指将本地备份的数据用交通工具送到远方。这种方案相对来说成本较低，但难于管理。

Tier2 层： PTAM 卡车运送访问方式 + 热备份中心 (PTAM + Hot Center)

相当于 Tier1 再加上热备份中心能力的进一步的灾难恢复。热备份中心拥有足够的硬件和网络设备去支持关键应用。相比于 Tier1，明显降低了灾难恢复时间。

Tier3 层：电子链接 (Electronic Vaulting)

在 Tier2 的基础上用电子链路取代了卡车进行数据的传送的进一步的灾难恢复。由于热备份中心要保持持续运行，增加了成本，但提高了灾难恢复速度。

Tier4 层：活动状态的备份中心 (Active Secondary Center)

指两个中心同时处于活动状态并同时互相备份，在这种情况下，工作负载可能在两个中心之间分享。在灾难发生时，关键应用的恢复也可降低到小时级或分钟级。

Tier5 层：两个活动的数据中心，确保数据一致性的两阶段传输承诺 (Two-Site Two-Phase Commit)

它提供了更好的数据完整性和一致性。Tier5 需要两中心与中心的 bias 被同时更新。在灾难发生时，仅是传送中的数据被丢失，恢复时间被降低到分钟级。

Tier6 层：0 数据丢失 (Zero Data Loss)，自动系统故障切换

Tier6 可以实现 0 数据丢失率，被认为是灾难恢复的最高级别，在本地和远程的所有数据被更新的同时，利用了双重在线存储和完全的网络切换能力，当发生灾难时，能够提供跨站点动态负载平衡和自动系统故障切换功能。

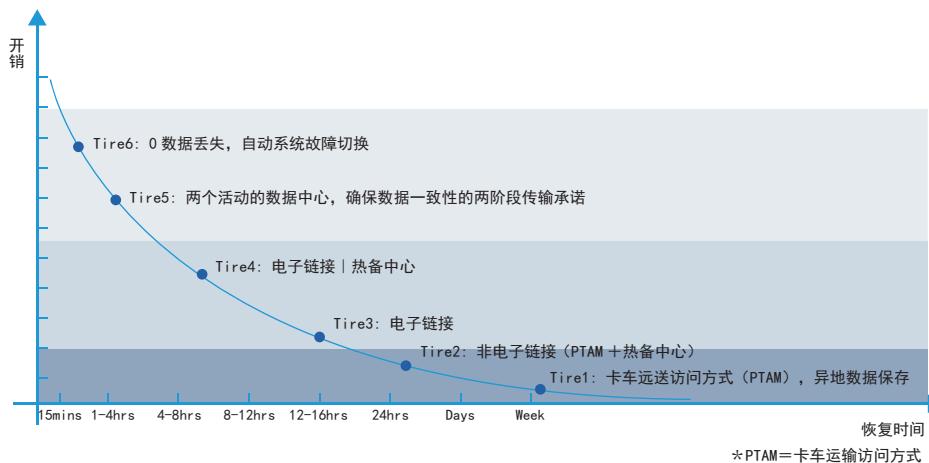


图 1.5-1 容灾各层级的恢复时间与成本关系

(2) ISO 22301

ISO 22301 的中文名称是业务连续性管理体系，它能够帮助企业制定一套一体化的管理流程计划，使企业对潜在的灾难加以辨别分析，帮助其确定可能发生的冲击对企业运作造成的威胁，并提供一个有效的管理机制来阻止或抵消这些威胁，减少灾难事件给企业带来损失。ISO 22301 拥有非常高的国际认可度。它指定了计划、实施、监督、审查和改进企业的业务连续性管理体系的具体要求，从而最大限度地减少突发事件造成的影响。

ISO 22301 适用于所有行业中的大、中、小型公有及私有组织，并且特别适用于处于高风险和高度监管环境下的行业，例如 IT 通信业、金融业、制造业等。各行各业的企业面对国际及中国地区不断频发地自然灾害及人为事故，其业务运作的不确定性和风险都被大幅度增加，而加强企业业务连续性管理则成为了打造最佳企业应急预案的必备选择。

(3) BS 25999

英国 BSI (British StandardInstitution) 出台了世界上第一个关于业务连续性管理 (BCM) 的英国标准—BS 25999，是为了在最棘手和意外的情况下保证企业的业务持续运行，从而保护企业的员工、维护企业的声誉并提供持续运营的能力。该标准为在组织内了解、开发和实施业务持续性提供了基础，

它包含一套基于 BCM 最佳做法的全面控制措施，涵盖整个 BCM 生命周期。

BS 25999 分两部分制定：第 1 部分《BCM 实践指南》于 2006 年底公布；第 2 部分《BCM 规范》于 2007 年底公布。

BS 25999 适合于各种规模及各行各业的任何组织，尤其适合在高风险环境中运营的组织，例如电信、金融、运输和其他公共行业。

1.5.2 国家标准

(1) GT/T20988-2007

《信息安全技术信息系统灾难恢复规范》国家标准（GB/T20988-2007）是我国灾难备份与恢复行业的第一个国家标准。该标准由国务院信息化工作办公室领导编制的，并于 2007 年 11 月 1 日开始正式实施。该标准规定了信息系统灾难恢复应遵循的基本要求，适用于信息系统灾难恢复的规划、审批、实施和管理，并参照国际标准 SHARE78 的 7 个层级定义，确定了符合中国国情的 6 个灾备能力等级要求。

根据国家标准 (GB/T20988-2007) 对灾备各级别的具体定义（附录 A），表 1.5-1 给出了灾备各级别要求对比。

由表 1.5-1 可以看出，国标 (GB/T20988-2007) 的 6 个灾备级别与国际标准 SHARE78 的 tier1 至 tier6 基本是对应的，前三级（tier1 至 tier3）基本一致，后三级（tier4 至 tier6）略有差异。

(2) GB/T30146-2013

2013 年，《公共安全业务连续性管理体系要求》国家标准 (GB/T 30146-2013) 正式发布。该标准同等采用了国际标准 ISO22301:2012。国家标准 (GB/T 30146-2013) 按照 PDCA 循环模型，对业务连续性管理工作提出了详尽的要求，并对业务连续性管理行业内的一些相关术语及指标做了明确的规定，是企业业务连续性管理体系建设水平的衡量标准。目前越来越多的企业都在争取获得国家标准 (GB/T 30146-2013) 的认证。

国际标准 SHARE78		《信息系统灾难恢复规范》 GB/T 20988 - 2007	
Tier-0	无异地备份数据	第1级	基本级。备份介质场外存，安全保管、定期验证
Tier-1	有数据备份，无备用系统 用卡车运送备份数据	第2级	备份场地支持。网络和业务处理系统可在预定时间内调配到备份中心
Tier-2	有数据备份，有备用系统 用卡车运送备份数据。	第3级	电子传输和部分设备支持。灾备中心配备部分业务处理和网络设备，具备部分通讯链路。
Tier-4	灾难恢复具有两个中心彼此备份数据，允许备份行动在任何一个方向发生。两个中心之间，彼此的关键数据的拷贝不停地相互传送着。在灾难发生时，需要的关键数据通过网络可迅速恢复，通过网络的切换，关键应用的恢复也可降低到小时级或分钟级。	第4级	电子传输和完整设备支持。数据定时批量传送，网络 / 系统始终就绪。温备中心模式。
Tier-5	保证交易的完整性，为关键应用使用了双重在线存储，在灾难发生时，仅传送中的数据被丢失，恢复时间被降低到分钟级。	第5级	实时数据传输及完整设备支持。采用远程复制技术，实现数据实时复制，网络具备自动或集中切换能力，业务处理系统就绪或运行中。
Tier-6/7	无数据丢失，同时保证数据立即自动地被传输到恢复中心。Tier6 被认为是灾难恢复的最高的级别，在本地和远程的所有数据被更新的同时，利用了双重在线存储和完全的网络切换能力。第7层实现能够提供一定程度的跨站点动态负载平衡和自动系统故障切换功能。	第6级	数据零丢失和远程集群支持。数据实时备份，零丢失，系统 / 应用远程集群，可自动切换，用户同时接入主备中心。

表 1.5-1 容灾各层级的恢复时间与成本关系

(3) GB/T 31595-2015

2015年，《公共安全业务连续性管理体系指南》国家标准（GB/T 31595-2015）正式发布，该国家标准也是同等采用了国际标准ISO22313:2012。国家标准（GB/T 31595-2015）针对企业实施业务连续性管理体系中的方法和步骤给出了详细的指导，是帮助企业制定和完善有效的业务连续性计划的得力帮手。

以上两项国家标准的推出也将进一步推动我国业务连续性管理体系与国际接轨。

此外，国信办分别在2004年4月发布《关于加强信息安全保障工作的意见》，2005年4月发布《重要信息系统灾难恢复指南》，对银行及相关行业信息安全提出指导意见。

1.5.3 中华人民共和国网络安全法

2017年6月1日，《中华人民共和国网络安全法》正式实施。该法从保障网络产品和服务安全，保障网络运行安全，保障网络数据安全，保障网络安全等方面进行了具体的制度设计。该法第二十一条、三十四条明确规定关键信息基础设施的运营者应当履行对重要系统和数据库进行容灾备份的保护义务，并在其他条文中规定了相应的处罚细则。

1.5.4 DR 及 BCM 相关认证

规范化是灾备产业发展的前提，为此，针对整个产业的资质认证是必备的。下面主要介绍两种认证。

第一是国内的中国信息安全与灾难恢复(CISDR)，它是灾备技术国家工程实验室、教育部网络攻防重点实验室、中国信息安全认证中心联合推出国家级认证。CISDR认证将作为信息安全与灾备企业申请服务资质的资质，是信息安全与灾备技术人员和管理人员资质评定的重要依据，是各行业信息安全与灾备相关人员专业水平的重要衡量标准。

第二是国际灾难恢复协会(DRI International)在中国举办的关于业务连

续性的资格认证，一般分为两个级别，学员在完成 DRI 课程内容的学习并经考试合格者，经批准后可获得 DRI 颁发的“助理业务持续规划师”资格证书 (Associate Business Continuity Planner，简称 ABCP)。学员具备两年的相关工作经验后，经批准后可获得 DRI 颁发的“业务持续专家”资格证书 (Certified Business Continuity Professional，简称 CBCP)。

此外，第三方的灾备服务商也针对市场需求提供针对企业产品技术的培训服务，如英方股份提供的 i2 Certification STD—初级认证工程师；i2 Certification ADV—高级认证工程师。

1.6 灾备市场规模

1.6.1 中国市场

随着数字城市、智慧城市、电子政务、物联网、大数据、三网合一、云计算、安防监控、医院信息化、人工智能、虚拟现实等趋势在国民经济各领域应用的日益广泛，数据量呈爆炸式增长，而随着数据集中、数据挖掘、商业智能、协同作业等技术的成熟，数据价值呈指数上升。大数据就是生产力，数据作为生产资料已经逐渐成为全行业的共识，这必然导致灾备需求的持续快速增长，使得灾备行业成为信息产业中最具有持续成长性的领域之一。

根据赛迪市场调查显示，2005 年中国灾备市场规模只有三十几亿人民币，2007 年，中国灾备市场规模已经达到 73 亿。根据 IBM 的调研，到 2020 年，全世界产生的数据量将是目前的 44 倍。中国已经从中央层面重视起数据安全，全国各地智慧城市的发展将为创新创业企业提供巨大的商机。据 IDC 的估算，2017 年，灾备市场将达到上千亿元的规模。

根据智研咨询发布的《2017-2022 年中国灾备行业深度研究及市场前景预测报告》指出：数据处理与存储行业在近年来一直保持较高速度的增长。截止 2014 年底，数据处理与存储服务行业市场规模达到 6834 亿元，同比增速 24.67%。2010 年开始，数据处理与存储行业规模仅为 1763 亿元，随着数

据量的增加，数据处理和存储行业市场规模也逐年增长。伴随着我国各行业的全面信息化，数据量的增长速度将继续加快，对存储产品和需求还将保持高速增长趋势，国家的信息化建设成为我国存储行业快速发展的重要保障。

近几年，我国宏观经济发展稳定，各行业对灾备产品需求快速增长，2010 年我国灾备行业市场规模约 49.8 亿元，到 2015 年我国灾备行业市场规模达到了 136.8 亿元，近几年我国灾备行业市场规模情况如下图所示（公开资料整理）：

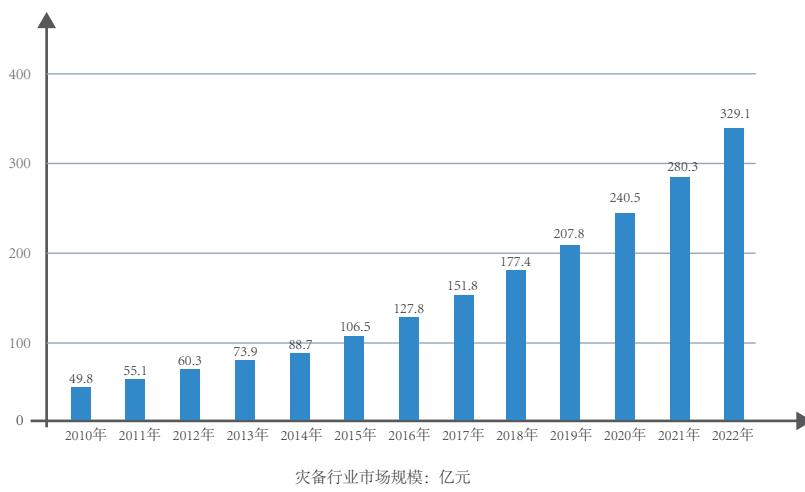


图 1.6-1 2010-2022 年中国灾备行业市场规模情况

2015 年，中国备份一体机市场规模约 11.84 亿元，与 2014 年的数据相比增长超过 19.35%。从 2011-2015 年备份一体机市场规模可以看出，2012 年之前备份一体机市场规模的增长率一度保持了 50% 以上的增长速度，虽然 2012 年之后宏观经济增速下滑，备份一体机市场规模的增长亦有所放缓，但依然保持 10% 以上的增长速度。

2015 年政府、电信和金融行业的市场份额占总体备份一体机市场的 63% 以上，同时也是 2015 年备份一体机接受度以及部署程度最高的三大行业。同时，随着各行业各部门对于风险控制的加强和深化，灾备市场快速增长的格局还将延续。灾备行业标准的颁布，将进一步推动灾备市场容量的持续扩大，政府、军队、军工、金融、电信、交通、能源等领域在灾备方面的

需求潜力不可小觑，未来几年内灾备市场仍会保持增长态势。

1. 6. 2 全球市场

2009 年，全球 IT 外包的规模就已经达到两千多亿美元，其中数据外包的市场规模达到了 991 亿美元。2013 年，中国在存储备份软件这一项的年支出超过 80 亿元，如果一个企业能够在中国占有 10% 的市场，年销售可达到 8 亿元。

根据 Gartner 的预测，预计到 2021 年，使用**备份而非归档**方式来管理企业长期数据的比例将从 2017 的 30% 上升到 50%。

相比传统的灾备市场，云灾备即服务（DRaaS）全球市场呈现出快速增长的态势，Gartner 公开的数据分析报告提到，2016 年市场规模已达 20 亿美金。但是国内 DRaaS 却逊色很多，究其原因，主要有以下几个方面：

1. **网络费用昂贵**，中国网络带宽发展滞后，目前公有云带宽默认是按兆进行售卖，国内带宽价格通常为 20 元 /M 左右（可参加阿里云等云厂商），香港带宽更贵。而国外一般是提供共享带宽，按流量计费，带宽通常是 100M 起。使用 DRaaS 服务的用户，数据量大，一般情况下，使用国内的公有云做 DRaaS 服务非常困难。同时，AWS 同款的 snowball 服务在国内并不完善。

2. **虚拟化** 这是局限性因素。国内的公有云运营商，一般仅支持单种虚拟化方式，比如阿里云和天翼云，默认均不提供不同虚拟化的选项，而从企业角度讲，不一定只使用单种虚拟化，

3. **版权问题**，企业所用的软件，系统，虚拟化等授权问题，存在 mac 地址绑定（比如 erp 系统），甚至还有可能存在盗版问题。

4. 集群问题处理技术不足。使用 DRaaS 的客户，极少是有单台设备的，一般是集群化部署，如何在**公有云实现集群化迁移、部署都是问题**。

5. 成本问题，包含资源租用，平滑迁移，运维人员，容灾演练。

6. 中国缺少一站式解决方案提供商。

第二章 灾备关键技术分类

灾备属于典型的技术密集型产业，技术驱动市场增长是非常显著的行业特征。在云与大数据时代，灾备技术的突破与进步，会撬动更多的潜在市场，让用户在数据保护与业务连续性方面的体验更佳。灾备项目的成功实施，涉及到很多技术的集成，包括数据存储、复制、删除、数据的加密与传输，应用的切换等多个技术的具体应用。本章，我们将全面了解灾备工作所涉及到的主要技术手段。

2.1 数据复制技术

数据复制技术是容灾方案设计中最基本也是核心的技术之一，主要分为基于数据库 / 应用的复制、基于主机的数据复制、基于存储网络的数据复制、基于存储的数据复制。其中，除了基于数据库的数据复制以外，其他的数据复制方式都具有同步和异步两种复制方式。

2.1.1 基于主机操作系统的数据复制

基于主机的数据复制是通过磁盘卷的镜像或复制进行的，业务进行在主机的卷管理器这一层，对硬件设备尤其是存储设备的限制小，利用生产中心和备份中心的主机系统通过 IP 网络建立数据传输通道，数据传输可靠，效率相对较高；通过主机数据管理软件实现数据的远程复制，当主数据中心的数据遭到破坏时，可以随时从备份中心恢复应用或从备份中心恢复数据。

基于主机的数据复制不需要两边采用同样的存储设备，具有较大的灵活性，缺点是复制功能会占用一些主机的 CPU 资源，对软件要求较高（很多软件无法提供基于时间点的快照功能），对主机的性能有一定的影响。

为了避免上述复制问题，提高复制效率，英方股份经过长期的技术研发积累，推出了操作系统内存层面字节级复制技术。

英方独有的字节级数据捕获与复制技术在实施过程中，首先会做初始化

的数据镜像，然后通过核心的复制引擎，开始旁路监听所有文件系统的写操作，例如 rename、SetAttr 等，都能准确的捕获，并通过数据序列化传输技术 (Data Order Transfer，简称 DOT) 异步传输到灾备端，完成整个数据的捕获和复制过程。



图 2.1-1 字节级复制技术原理图

字节级复制的核心引擎工作时，并没有复杂的数学运算，对生产机计算资源占用可以忽略，仅仅是旁路捕获数据，另外，所有的数据都是从内存中捕获，并不涉及生产主机存储的读取操作，因此数据复制过程不占用主机的存储 IO 资源。另外，基于字节级的数据复制粒度最小到字节，因此对于带宽资源的要求极低。尤其适应于面向未来的混合 IT 环境，云化架构中的一种复制方式。

2.1.2 基于应用和中间层的数据复制技术

应用层面的数据复制通过应用程序与主备中心的数据库进行同步或异步的写操作，以保证主备中心数据一致性，灾备中心可以和生产中心同时正常运行，既能容灾，还可实现部分功能分担，但是该技术的实现方式复杂，与应用软件业务逻辑直接关联，实现和维护难度较高，并且使用应用层面的数据复制会提高系统的风险与数据丢失的风险。

独立于底层的操作系统、数据库、存储，应用可以根据需求实现双写或

者多写，从而实现主本和多个数据副本之间的数据复制功能。这种由应用实现的技术，可以在中间件或者应用平台层面进行封装和实现，对上面的应用透明，也可以在应用层面实现；主要好处是可根据需求定制、可实现应用和数据库层面的复制，自主可控；主要不足是目前市场上没有成熟、适合传统IT企业大规模推广使用的中间件产品；如果完全由应用封装平台或者应用来实现，代码的复杂程度提高，增加了应用的维护成本。

2.1.3 基于数据库的数据复制技术

基于数据库软件的复制技术包括物理复制和逻辑复制两种方式，逻辑复制是利用数据库的重做日志、归档日志，将主本所在站点的日志传输到副本所在站点，通过重做SQL的方式实现数据复制。逻辑复制只提供异步复制，主副本数据的最终一致性，无法保证实时一致性；物理复制不是基于SQL Apply操作来完成复制，而是通过redolog日志或者归档日志在副本站点的同步或者异步持久化写来实现复制功能，同时副本站点的数据可以提供只读功能。

开放平台数据库复制技术则是一种基于数据库log(日志)的结构化数据复制技术，它通过解析源数据库在线log或归档log获得数据的增、删、改变化，再将这些变化应用到目标数据库，使源数据库与目标数据库同步，以达到多站点间数据库可双活甚至多活，实现业务连续可用和容灾的目的。

基于数据库的数据复制是对数据库记录级别、表级别容灾高可用的基础技术，英方数据库容灾技术结合了主机复制和数据库日志分析的优点，提高了系统应用的灵活性，可实现数据库应用多活，同时也极大减少了数据库应用的增量数据传输。在细粒度数据容灾、广域云化容灾领域仍然具有广阔的应用前景。例如英方i2Active是基于redolog日志分析技术的Oracle数据实时复制工具，具有简单灵活、高性能、非侵入、低影响、低于秒级延迟，低成本的特点，部署和使用也非常简便。能够帮助用户在复杂的应用环境下完成Oracle容灾备份、数据迁移、业务数据分发、构建大型数据仓库等技术

数据整合等工作。

i2Active 支持 Hadoop 和关系型数据库之间的数据相互转移，可以将关系型数据库（例如 MySQL ,Oracle 等）中的数据同步到 Hadoop 的 HDFS 中，也可以将 HDFS 的数据同步到关系型数据库中。i2Active 主要通过 Hadoop 的 Map Reduce 将数据从关系型数据库中导入数据到 HDFS。

2. 1. 4 基于存储系统的网关的数据复制

存储网关位于服务器与存储之间，是构架在 SAN 网络上的专用存储服务技术。这项技术基于存储虚拟化技术，诞生于 2000 年。

存储虚拟化的直接定义为：在存储设备中形成的存储资源透明抽象层，即存储虚拟化是服务器与存储间的一个抽象层，它是物理存储的逻辑表示方法。其主要目的就是要把物理存储介质抽象为逻辑存储空间，将分散繁杂的
异构存储管理整合为统一简单的集中存储管理，将人们所面对的众多存储问题，由繁化简（其中包括存储的读写方式、连接方式、存储的规格或结构等），由散化整（存储管理）的过程就是存储虚拟化。

存储网关通过对于进入的 IO 数据流提供各类数据存储服务，大幅提升了在服务器或者存储层面难以达到的灵活性、多样性、异构化等多种存储服务能力。利用存储网关，对于后端的存储数据可以提供远程数据复制、异构化存储融合、存储设备高可用镜像、快照服务、数据迁移服务甚至于部分存储网关可以提供精准的持续数据保护连续数据恢复服务。

由于存储网关卸载了服务器和阵列的复制工作负载，它可以跨越大量的服务器平台和存储阵列运行，因而使它成为高度异构的环境下的容灾技术的理想选择。另外，由于针对带宽优化、数据恢复精细化等方面独有的优势，这项技术也成为比较主流的**一种灾备技术**。

这项技术主要争论点在于性能保障能力的发展程度。近年来，随着 SAN 应用的不断普及，SAN 网络中由异构存储设备和爆炸式增长的数据量所带来的管理复杂性、资源利用率低、投资浪费、存储设备自身数据服务能力

力较低等问题促进了存储网关的发展和应用。

2.1.5 基于存储介质的数据复制

通过存储系统内建的固件或操作系统、IP 网络或光纤通道等传输介质连结，将数据以同步或异步的方式复制到远端，从而实现生产数据的灾难保护。

采用基于存储数据复制技术建设容灾方案的特点主要是对网络连接及硬件的要求较高。基于存储的复制可以是“一对一”复制方式，也可以是“一对多或多对一”的复制方式，即一个存储的数据复制到多个远程存储或多个存储的数据复制到同一远程存储，而且复制可以是双向的。

存储复制技术使基于实现在存储磁盘阵列之间的直接镜像，通过存储系统内建的固件(Firmware)或操作系统，利用 IP 网络或光纤通道等传输界面连结，将数据以同步或异步的方式复制到远端。当然，一般情况下这种模式，必须同等存储品牌并且同等型号的存储系统控制器之间才能实现，配备低延迟大带宽也是必要条件之一。

在基于存储阵列的复制中，复制软件运行在一个或多个存储控制器上，非常适合拥有大量服务器的环境，原因如下：独立于操作系统；能够支持 Windows 和基于 Unix 的操作系统以及大型机(高端阵列)；许可费一般基于存储容量而不是连接的服务器数量；不需要连接服务器上的任何管理工作。由于复制工作被交给存储控制器来完成，在异步传输本地缓存较大的时候可以很好的避免服务器的性能开销过大的问题，从而使基于存储阵列的复制非常适合关键任务和高端交易应用。这也是目前应用最广泛的容灾复制技术之一，但这种技术随着闪存存储、开放式存储、云存储、面向对象存储等等混合存储技术的普及和迭代，越来越难以适应新环境下的容灾复制需求。

数据复制技术大比较（一）

数据复制功能层级				
个性化业务层级	业务软件开发商专门编写复制功能	交易逻辑数据	高，需大量修改应用，实施难度大	一般
数据库层级	数据库语言级复制，英方特有的复制技术	数据库中变化的记录（基本等同于交易数据）	低（无须修改应用）	较高（至多损失一个事物）
	数据库厂商提供的整库库级别复制功能	数据库日(2-4倍交易数据量)	低（无须修改应用）	一般（至少损失一个事物）
	第三方提供的数据表级别复制软件	数据库中变化的记录（基本等同于交易数据）	低（无须修改应用）	一般（至少损失一个事物）
操作系统层级	英方特有的系统内核字节级数据复制技术	字节变化量(等同于交易数据)	低（对应用透明）	高(I/O)
	系统镜像厂商提供的卷级别复制软件	数据块（4-8倍交易数据量）	高，修改系统卷，对应用不透明	高(I/O)
	操作系统本身提供的系统级别数据复制	数据块（4-8倍交易数据量）	低（对应用透明）	高(I/O)
存储层级	磁盘阵列厂商提供的数据块级别复制功能（同步/异步）	数据块（4-8倍交易数据量）	低，但对应用不透明	高(I/O)

表 2.1—1 数据复制技术大比较（一）

数据复制技术大比较（二）

数据复制功能层级	主机资源占用	平台兼容性	备注
个性化业务层级	<10%	异构主机 异构存储	运维复杂，开发工作量较大
	<10%	异构主机 异构存储	专有技术保证数据库一致性，图形界面运维简单
数据库层级	<20%	异构主机 异构存储	数据库支持以整库为单位，业务颗粒度大
	<20%	异构主机 异构存储	需要数据库一致校验，运维复杂
	3%-10%	异构主机 异构存储	实时异步技术 轻量级
操作系统层级	10%-20%	同构主机 异构存储	跨平台难度较大
	<30%	同构主机 异构存储	操作系统效率影响较大
存储层级	不确定	异构主机 同牌存储	同品牌同系列盘阵

表 2.1—1 数据复制技术大比较（二）

以上的数据复制技术中，并不能说哪类技术就一定优于另一类技术，“优势”都只是相对的，毕竟只有能够满足企业特定需求的技术才是最好的技术。但是关于数据复制量的对比，图 2.1-2 以一个 300M 的文件修改了 512 字节的场景为例，说明各种技术所复制的数据量的比例——复制传输的数据量之比为 300MB: 64KB: 512B (4800: 128: 1)。

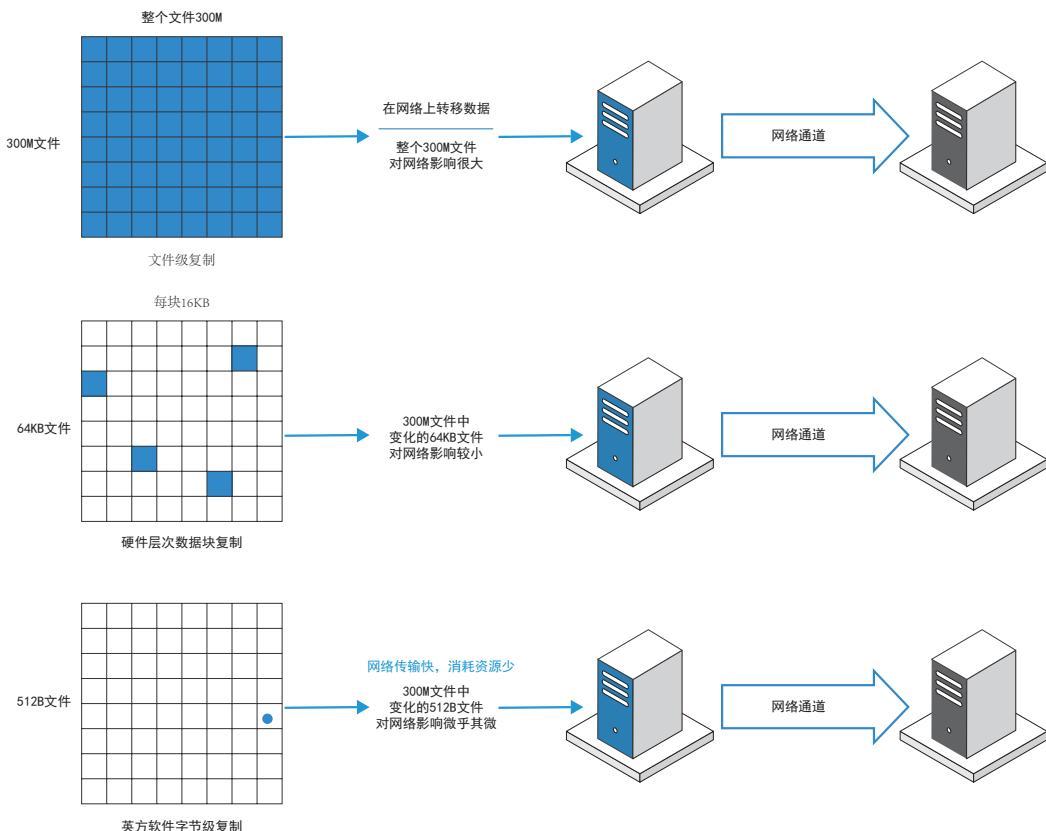


图 2.1-2 三种复制技术的数据量对比

2.1.6 同步与异步复制方式

除了从技术的角度细分复制技术之外，根据内部实现机制的不同，又可以将复制技术分为同步和异步复制两种方式：

同步复制方式

在主 / 备中心的磁盘阵列同步进行数据的更新，应用系统的 I/O 写入主

磁盘阵列后，主磁盘阵列将利用自身的机制，同时将写 I/O 写入后备磁盘阵列，后备磁盘阵列确认后，主中心磁盘阵列才返回应用的写操作完成信息。

异步复制方式

在应用系统的 I/O 写入主磁盘阵列后，主磁盘阵列立即返回给主机应用系统“写完成”信息，主机应用可以继续进行读、写 I/O 操作。同时，主中心磁盘阵列将利用自身的机制将写 I/O 写入后备磁盘阵列，实现数据保护。

采用同步复制方式，使得后备磁盘阵列中的数据总是与生产系统数据同步，因此当生产数据中心发生灾难事件时，不会造成数据丢失。但代价是生产和灾备中心之间必须建立高速低延迟光纤网络，任何灾备存储访问延迟都会对生产系统造成延滞效应。因此，为避免对生产系统性能的影响，同步方式通常在近距离范围内（FC 连接通常是 200KM 范围内，实际用户部署多在 35KM 左右）。

采用异步复制方式应用程序不必等待远程更新的完成，因此远程数据备份对性能的影响通常较小，并且备份磁盘的距离和生产磁盘间的距离，在理论上没有限制（可以通过 IP 连接来实现数据的异步复制）。

2.1.7 快照技术

SNIA(全球网络存储工业协会 Storage Networking Industry Association) 对快照 (Snapshot) 的定义是关于指定数据集合的一个完全可用拷贝，该拷贝包括相应数据在某个时间点 (拷贝开始的时间点) 的映像。

快照可以是其所表示的数据的一个副本，也可以是数据的一个复制品。从具体的技术细节来讲，快照是指向保存在存储设备中的数据的引用标记或指针，换句话说，快照类似详细的目录表，但它被计算机作为完整的数据备份来对待。

快照的一个主要作用是能够进行在线数据恢复，当存储设备发生应用故障或者文件损坏时可以进行及时数据恢复，将数据恢复成快照产生时间点的状态；另一个作用是为存储用户提供额外的数据访问通道，当原数据进行在

线应用处理时，用户可以访问快照数据，还可以利用快照进行测试等工作。

快照在备份、数据保护过程中发挥的作用越来越大。快照技术具有备份和恢复窗口短、性能损失小、容量利用率高等优点。因此，所有存储系统，不论高中低端，只要应用于在线系统，那么快照就成为一个不可或缺的功能。目前主流的快照技术包括镜像分裂快照技术、按需备份快照技术、指针重映射快照技术、增量快照技术等。

快照有三种基本形式：基于文件系统式、基于子系统式、基于卷管理器/虚拟化式，这三种形式存在较大差别。目前，市场上也出现了一些能够自动生成这些快照的实用工具。

数据的迁移离不开数据复制技术，在机房搬迁、停机整改、数据上云等数据迁移场景中，虽然各种数据复制技术都可以实现数据的最终迁移，但是在综合数据迁移两端存储异构、生产是否停机、数据一致性等因素时，优秀的复制技术能够帮助用户节省成本，将迁移工作简单化、透明化。

2.1.8 数据一致性

主本和副本之间根据需求可以是强一致性、弱一致性、最终一致性，不同的需求决定了不同的解决方案，如下：

1) 强一致性

主本和副本的更新在同一个事务中完成，通过 2PC 的分布式事务控制来保证数据的强一致性，如标准的 JTA 协议；如果应用自行设计，可以考虑先更新副本、再更新主本，如果副本失败，则事务直接返回失败，如果是副本成功、主本失败，则设置主本重试次数，尝试数次不成功之后，副本执行回滚操作，事务返回失败；强一致性的操作有点类似前面介绍的同步模式复杂，在事务层面严格保证 ACID 特性，数据的主本和副本之间耦合性增加，性能受副本所在站点的性能、网络带宽、网络延时的影响；同时在事务的控制方面增加了应用的复杂度（即使使用中间件产品中自带的分布式事务功能），在某些异常情况下会出现可疑事务，必要时需要人工干预。

2) 弱一致性

系统并不保证主副本数据之间的实时一致性，不承诺具体到多久之后在副本可以读到最新的数据。

3) 最终一致性

弱一致性的特定形成，在主本数据后续更新的前提下，副本最终与上一次主本最新的值保持一致。在没有故障发生的前提下，主副本之间的时延主要受通讯延时、系统负载、和复制副本的个数影响。

不管是最终一致性还是弱一致性，在事务层面实际上都是打破 ACID 的要求，取代的是 BASE（Basically Available, Soft State, Eventually Consistent）（基本业务可用、柔性状态、最终一致性），主本和副本之间通过异步消息来传递事务信息，异常情况下，通过多次重试的幂等性来实现一致性。

2.2 切换技术

切换（Failover）技术是指在早前运行系统故障或异常终止后，能够自动（通常无需人工干预或警告）切换到冗余或备用信息系统的能力。根据具体突发故障的不同，又可以归类为网络切换和应用切换。

灾备切换是一系列操作的组合，不是单一的技术动作，并且由于“容灾黑盒”的存在，其切换的决策难度非常大。无论是生产中心还是灾备中心，彼此的业务之间都有逻辑的联系，服务的启动顺序也有严格的要求。比如数据库必须先启动，之后才能启动应用程序；应用服务器接管完成，才能进行网络的切换。如果应用程序先于数据库启动，结果肯定会是出错。

灾难的类型多种多样，每一次灾备中心的启用，都需要耗费大量的人力和物力，所以不是每一种灾难都需要启用灾备中心。在发生灾难时，首先需要快速判断灾难的类型、可恢复性和后果，然后根据灾备预案来决定是否启用灾备中心。比如，通过本地备份只需要半小时就能恢复本地的业务，就完

全不需要启用灾备中心。此外，应用级灾备的对象往往是关键的业务，越关键的业务，切换就越需要慎重，因此启动切换决策需要集体的决策，而不是根据单一的个人意愿。

2. 2. 1 网络切换技术

目前，网络切换技术主要有三种：基于 IP 地址的切换、基于 DNS 服务器的切换、基于负载均衡设备的切换。

1) 基于 IP 地址的切换

主备应用服务器的 IP 地址空间相同，客户端通过唯一的 IP 地址访问应用服务器。在正常情况下，只有生产中心应用服务器的 IP 地址处于可用状态，灾备中心的备用服务器 IP 地址处于禁用状态。灾难一旦发生，管理员手动或通过脚本将灾备中心服务器的 IP 地址设置为可用，实现网络访问路径切换。

2) 基于 DNS 服务器的切换

DNS 服务器的切换模式下，所有应用都需要根据主机名来访问，而不是直接根据主机的 IP 地址来访问，从而通过域名实现网络切换。组织对外提供服务的业务，可通过向运营商申请相应的 DNS 服务器，对主生产中心和备用生产中心各申请相应的 DNS 服务，通过运营商 DNS 切换机制实现对外服务的切换。

对于内部提供的业务，生产中心和灾备中心各自部署一台 DNS 服务器，负责所有主机的域名解析。生产中心为主 DNS 服务器，灾备中心为备份 DNS 服务器，两台 DNS 服务器的内容自动保持完全同步。对于每个应用服务器的域名，DNS 服务器上可以保存两个 IP 地址，主 IP 地址指向生产中心应用服务器的 IP 地址，备份 IP 地址指向灾备中心服务器的 IP 地址。

在所有的客户端上设置这两个 DNS 服务器（可通过 DHCP 服务器自动分配）。系统首先查询主 DNS 服务器，如果没有应答，就查询备份 DNS 服务器。当生产中心的主服务器出现故障，主 DNS 服务器发现无法联系到主

服务器时，会自动将 DNS 请求解析至灾备中心服务器的 IP 地址，从而实现单个应用的自动切换。

3) 基于负载均衡设备的切换

通过在服务器集群前端部署一台负载均衡设备，根据已配置的均衡策略将请求在服务器集群中分发，为用户提供服务，并对服务器可用性进行维护。

负载均衡能够按照一定的策略分发到指定的服务器集群中的服务器，或指定链路组的某条链路上，调度算法以用户连接为粒度，并且可以采取静态设置或动态调配的方式。

负载均衡设备能够针对各种应用服务状态进行探测，收集相应信息作为选择服务器或链路的依据，包括 ICMP、TCP、HTTP、FTP、DNS 等。通过对应用协议的深度识别，能够对不同业务在主生产中心和灾备中心之间进行切换。

2. 2. 2 应用切换技术

应用切换是指生产中心由于发生灾难无法作业时，可由灾备中心的备用服务器提供业务接管，确保业务运行的高连续性。实现应用切换的前提条件是：

- 1) 数据已经从生产中心同步到灾备中心，如果数据复制采用的是异步的方式，在网络故障的情况下，就有可能造成数据不一致的问题，导致数据不可用或无法访问。
- 2) 灾备中心配置与生产中心对应的应用软件服务器、数据库服务器和中间件服务器等，且运行正常。
- 3) 灾备中心网络运行正常或能够实现正常切换。

应用切换技术主要有以下几种：

1. 主备集群 (Cluster) 远程技术

集群远程是指通过在生产中心和灾备中心的应用服务器上安装远程集群软件，实现跨广域的多服务器状态的监控，当发生灾难时，实现应用服务器

的自动切换。

集群远程容灾技术为集群的共享数据及业务提供了一种更为可靠的远程保护手段，通过该方案，可以将本地集群中的共享数据通过网络备份到远程灾备服务器上，实现集群数据的异地灾备，在数据备份的基础之上还可以在本地集群不可用时，通过选择自动或手动将本地业务切换至远程灾备中心服务器，从而减少业务的停机时间。

主备集群应用切换方式的主要弊端在于，多种潜在因素（例如集群服务器心跳线中断、网络短时间中断、应用服务器响应不及时等）容易导致在生产中心实际运行正常情况下进行误切换，运行风险高。

2. 双活负载均衡技术

归类到应用切换功能，双活技术是一种利用 IT 资源较多的灾备方案，来源于多中心技术。真正意义的双活指两个数据中心同时处于生产状态，类似于负载均衡技术，但通常的负载均衡针对于业务流量而非数据保护和数据安全，启用所有资源共同承载业务的服务，同时保证了当其中一边发生灾害事件时，另一方的资源可直接接管所有的业务服务。

双活可以保证资源的充分利用和快速的灾备切换，是快速安全的应用级灾备策略，主要用于同城灾备系统。异地双活系统则由于需要考虑系统的合理拆分、数据复制和业务服务的协调、灾备接管策略等，因此也被称为最为复杂的灾备技术架构。

双活技术架构按照业务分担方式，可以分为纯双活系统和准双活系统。纯双活系统为全业务负荷在双活中心的共同承载，在实践中多演变为按照区域负载分担或者按照业务类型负载分担。准双活系统则往往以读写分离的形式存在，由生产中心承载全业务，备份中心则承载可分离的读类型业务，从而较大幅度地利用备份中心的资源并且提升业务切换的指标。因此，从应用切换的角度来解释双活，它更多地属于一种负载均衡技术，而非容灾技术。

2.3 重复数据删除技术

数据去重技术通常用于基于磁盘的备份系统，通过在某个时间周期内删除不同文件中不同位置的重复可变大小数据块，减少存储系统中使用的存储容量。基于磁盘的重复数据删除技术已经被大量应用于灾备存储中，该项技术通过寻找不同数据块中的冗余数据，并通过删除这些重复的数据来对数据进行压缩，某些重复数据压缩技术甚至实现了 20:1 的压缩比，通过重复数据删除技术不但能解决单数据中心多副本占用空间的问题，还可以减少传输备份数据所需要的带宽，重复数据删除技术主要分为基于软件的重复数据删除和基于硬件的重复数据删除两种方式。

基于软件的重复数据删除旨在消除源端的冗余，以此减少带宽的压力。但是，基于软件的重复数据删除维护十分困难，如果想用一个全新的产品来替换原有的备份引擎，就会导致之前的数据完全不可用。

基于硬件的重复数据删除在存储系统本身进行数据削减，具有更高的压缩比，更加适合大型企业使用。正常情况下，备份软件会将专用设备看成一般的“磁盘系统”，并且不会感知其内部正在进行的重复数据删除进程。具有更高的压缩比，更加适合大型企业使用。

重复数据的删除并非是灾备系统中的必备环节，英方股份独有的字节数据捕获与复制技术、增量数据复制技术在源端就可以有效解决数据重复传输的问题。

2.4 数据加密与传输技术

数据级灾备往往依托于多部门、多单位甚至是跨系统的综合协作，因此数据在传输过程或存储介质上的安全性问题也会格外突出。

在灾备工作的具体实践中，英方主要采用基于端及基于传输通道的加密方式进行数据的安全保护，以往的数据灾备更多的是企业自主行为，不管是源端、备端还是传输网络都是企业自有资源，安全性较高，所以很多灾备系

统往往只将注意力集中在可用性和完整性上，对机密性缺乏关注。

现在，在娱乐行业，很多电影、音乐、图书、游戏的数据都保存在云端，业务云化开始不断地提供给大家多种多样的数字生活。但是，在云端的业务数据存在着很多网络攻击、误操作造成数据丢失等风险，因此每个企业或个人，需要对云端的安全性加强防范意识。首先从备份数据存储安全性的角度来看，备份数据如果在存储介质上以明文方式存放，容易被黑客攻击造成数据外泄。其次，从备份数据传输安全性的角度来看，备份数据如果在网络传输过程中以明文或不当的加密方式传输，容易通过数据包截取等手段造成备份数据泄露。

目前，针对数据的加密方式有很多，简单分类后大体可以分为两种加密方式。

2. 4. 1 源端加密

源端加密是对数据的源端产出和目标端的存储进行加密。一个文件系统（比如 Windows 加密文件系统）或者一个数据库对存储在里面的数据进行加密。如果数据存储时进行加密，备份的时候也相应的加密。

简单地说，源端加密主要包括硬件加密和软件加密两种方式：硬件加密技术一般所指的是采用硬件数据加密技术对产品硬件进行加密，具备防止暴力破解、密码猜测、数据恢复等功能，实现方式有键盘式加密、刷卡式加密，指纹式加密等。软件加密则是通过产品内置的加密软件实现对存储设备的加密功能。实现方式主要有软件内密码加密、证书加密、光盘加密等。

在实践中，英方 i2CDP 即采用了目前流行的 AES（Advanced Encryption Standard）加密算法，AES 在软件及硬件上都能快速地加解密，易于应用，且只需要很少的存储器。当然也采用外挂加密算法。

2. 4. 2 传输加密

传输加密是指在备份数据发起端与备份介质之间串联一个数据加密网关，备份数据发起端先与加密网关建立安全隧道，备份数据通过安全隧道以

保证传输安全。同时加密网关以完全透明的方式让数据在备份传输过程中实时被加密。

在具体应用中，最为理想的情况是采用源端加密与传输加密结合的方式，存储设备带数据文件加密功能并提供安全隧道服务。备份数据发起端先与加密网关建立安全隧道，备份数据通过安全隧道进行以保证传输安全。同时在备份数据落地到存储介质前，先对备份数据文件进行加密，保证存储介质上存放的都是密文数据。

根据不同的技术以及加密方式，加密算法和相应的密钥管理体系还有很多内容可以大书特书，由于篇幅有限，本文不再做赘述。如果你正在使用一个基于云的数据加密解决方案，那么就需要确保该数据加密过程是真实有效的，并且将密钥牢牢握在手里。

2.5 三种常见存储形态及对应架构

数据以某种格式记录在计算机内部或外部存储介质上的过程称为数据存储。数据存储对象包括数据流在加工过程中产生的临时文件或加工过程中需要查找的信息。从定义上，存储和灾备并不属于同一领域，但灾备技术的发展依托于存储技术的发展，数据备份的过程也必须涉及到数据的存储过程。

此外，随着市场竞争的加剧，灾备企业和存储企业之间的界限也逐渐模糊，相互之间的市场渗透也在不断加剧。因此谈灾备，必然谈存储。常见的存储方式主要包括：DAS(Direct Attached Storage) 直连附加存储、SAN(Storage Area Network) 存储区域网络、NAS(Network Attached Storage) 网络附加存储、OBS (Object-Based Storage) 对象存储等。

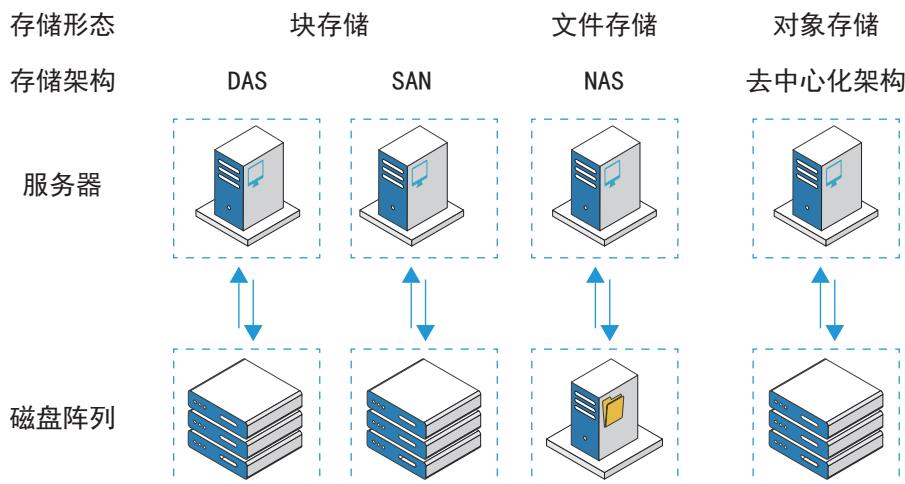


图 2.5-1 常见的存储架构

2.5.1 块存储与直接附加存储

1) 直连附加存储 (DAS)

DAS 这种存储方式与普通的 PC 存储架构一样，外部存储设备都是直接挂接在服务器内部总线上，数据存储设备是整个服务器结构的一部分。

DAS 存储方式主要适用以下环境：

1. 小型网络

因为网络规模较小，数据存储量小，采用这种存储方式对服务器的影响不会很大，并且这种存储方式也十分经济，适合拥有小型网络的企业用户。

2. 地理位置分散的网络

虽然企业总体网络规模较大，但在地理分布上很分散，通过 SAN 或 NAS 在它们之间进行互联非常困难，此时各分支机构的服务器也可采用 DAS 存储方式，这样可以降低成本。

3. 特殊应用服务器

在一些特殊应用服务器上，如微软的集群服务器或某些数据库使用的原始分区，均要求存储设备直接连接到应用服务器。

4. 提高 DAS 存储性能

在服务器与存储的各种连接方式中，DAS 曾被认为是一种低效率的结

构，而且也不方便进行数据保护。直连存储无法共享，因此经常出现的情况是某台服务器的存储空间不足，而其他一些服务器却有大量的存储空间处于闲置状态无法利用。如果存储不能共享，就谈不上容量分配与使用需求之间的平衡。

DAS 结构下的数据保护流程相对复杂，如果做网络备份，那么每台服务器都必须单独进行备份，而且所有的数据流都要通过网络传输。如果不做网络备份，那么就要为每台服务器都配一套备份软件和磁带设备，导致备份流程的复杂度会大大增加。

2) 存储区域网络 (SAN)

1991 年，IBM 公司在 S/390 服务器中推出了 ESCON(Enterprise System Connection) 技术。它是基于光纤介质，最大传输速率达 17MB/s 的服务器访问存储器的一种连接方式。在此基础上，进一步推出了功能更强的 ESCON Director(FC SWitch)，构建了一套最原始的 SAN 系统。

SAN 存储方式创造了存储的网络化。存储网络化顺应了计算机服务器体系结构网络化的趋势。SAN 的支撑技术是光纤通道 (FC Fiber Channel) 技术。它是 ANSI 为网络和通道 I/O 接口建立的一个标准集成。FC 技术支持 HIPPI、IPI、SCSI、IP、ATM 等多种高级协议，其最大特性是将网络和设备的通信协议与传输物理介质隔离开，这样多种协议可在同一个物理连接上同时传送。

SAN 的硬件基础设施是光纤通道，用光纤通道构建的 SAN 由以下三个部分组：

存储和备份设备——包括磁带、磁盘和光盘库等。

光纤通道网络连接部件——包括主机总线适配卡、驱动程序、光缆、集线器、交换机、光纤通道和 SCSI 间的桥接器。

应用和管理软件——包括备份软件、存储资源管理软件和存储设备管理软件。

SAN 的优点

1. 网络部署容易
2. 高速存储性能

因为 SAN 采用了光纤通道技术，所以它具有更高的存储带宽，存储性能明显提高。SAN 的光纤通道使用全双工串行通信原理传输数据，传输速率高达 1062.5Mb/s。

3. 良好的扩展能力

由于 SAN 采用了网络结构，扩展能力更强。光纤接口提供了 10 公里的连接距离，这使得实现物理上分离，异地存储变得更为容易。

2.5.2 文件存储与网络附加存储 (NAS)

网络附加存储 (NAS) 方式则全面改进了以前 DAS 存储方式。它采用独立于服务器，单独为网络数据存储而开发的一种文件服务器来连接所存储设备，自形成一个网络。这样数据存储就不再是服务器的附属，而是作为独立网络节点存在于网络之中，可由所有的网络用户共享。

NAS 的优点：

1. 真正的即插即用

NAS 是独立的存储节点存在于网络之中，与用户的操作系统平台无关，真正的即插即用。

2. 存储部署简单

NAS 不依赖通用的操作系统，而是采用一个面向用户设计的，专门用于数据存储的简化操作系统，内置了与网络连接所需要的协议，因此使整个系统的管理和设置较为简单。

3. 存储设备位置非常灵活

4. 管理容易且成本低

NAS 数据存储方式是基于现有的企业 Ethernet 而设计的，按照 TCP/IP 协议进行通信，以文件的 I/O 方式进行数据传输。

当然，NAS 也并非十全十美，存储性能较低、可靠度低是其主要缺点。

2.5.3 对象存储与分布式存储架构

对象存储系统（Object-Based Storage System）是综合了 NAS 和 SAN 的优点，同时具有 SAN 的高速直接访问和 NAS 的数据共享等优势，提供了高可靠性、跨平台性以及安全的数据共享的存储体系结构。

对象存储系统，可以在一个持久稳固且高度可用的系统中存储任意的对象，且独立于虚拟机实例之外。应用和用户可以在对象存储中使用简单的 API 访问数据；这些通常都基于表属性状态转移（REST）架构，但是也有面向编程语言的界面。对象存储提供了数据上受限操作的访问控制。数据管理员可以在 bucket 层级上（类似于目录）或者对象层级上（类似目录中的文件）应用访问控制。存储对象的授权 / 认证通过云提供商的身份认证管理系统或者你的目录服务来管理。通过后者，可能有一个本地的目录，同基于云的目录服务同步，巩固所有的访问控制角色和进入单一注册库的特权。因此，对象存储被认为是云存储得以快速发展的基础。

分布式存储是利用分布式技术将标准 X86 服务器的本地 HDD、SSD 等存储介质组织成一个大规模存储资源池，同时，对上层的应用和虚拟机提供工业界标准的 SCSI、iSCSI 和对象访问接口，进而打造一个虚拟的分布式统一存储产品。

2.6 相关技术创新

灾备技术并不是孤立的，作为一种在数据中心发生故障或灾难时被触发的技术，涉及到备份、复制、镜像、虚拟化、开源架构、超融合等多种不同技术，系统建设复杂程度高，好的灾备技术方案在综合其他技术可以实现用户的“故障无感知”的效果。

2.6.1 灾备与 SDS

2016 年软件定义成为 IT 领域的关键词，其中又以软件定义存储 (SDS)

的关注度最高。

软件定义存储可以实现存储资源的抽象化、池化及自动化，同时，软件定义与开源软件结合，从而推动创新。以开源的软件定义存储 Ceph 为例，因为 Ceph 采用的是强一致性同步模型，即必须所有副本都完成写操作才算一次写入成功。而如果副本在异地的话，由于网络延迟的存在，那么整个集群的写性能就会比较差，也就无法有效支撑异地复制，较早的 ZoneGroup 和联合集群概念也并没有很好的解决这个问题。

于是从 2015 年开始启动的新功能——RBD Mirror 进了大家的视线，用以解决两个集群间异步备份的问题。

RBD Mirror 原理其实和 MySQL 的主从同步原理非常类似，简单地说就是利用日志进行回放 (replay)：通过在存储系统中增加 Mirror 组件，采用异步复制的方式，实现异地备份。

在说 Mirror 之前，我们需要首先了解一下 Ceph 的 journal 机制。这里说明一下，此处的 journal 是指 Ceph RBD 的 journal，而不是 OSD 的 journal。当 RBD Journal 功能打开后，所有的数据更新请求会先写入 RBD Journal，然后后台线程再把数据从 Journal 区域刷新到对应的 image 区域。RBD journal 提供了比较完整的日志记录、读取、变更通知以及日志回收和空间释放等功能，可以认为是一个分布式的日志系统。

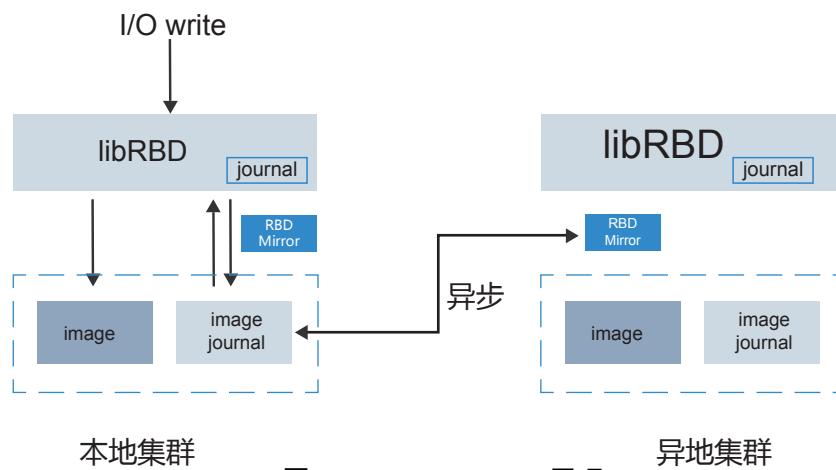


图 2.6-1 RBD Mirror 原理

Ceph RBD mirror 数据异步备份有具体步骤，如下：

- 1.I/O 会写入主集群的 Image Journal;
2. Journal 写入成功后，RBD 再把数据写入主集群回复响应；
3. 备份集群的 mirror 进程发现主集群的 Journal 有更新后，从主集群的 Journal 读取数据，写入备份集群；
4. 备份集群写入成功后，会更新主集群 Journal 中的元数据，表示该 I/O 的 Journal 已经同步完成；
5. 主集群会定期检查，删除已经写入备份集群的 Journal 数据。

这种方式的优点包括：

1. 当副本在异地的情况下，减少了单个集群不同节点间的数据写入延时；
2. 减少本地集群或异地集群由于意外断电导致的数据丢失。

目前社区的 RBD mirror 正在不断完善中，相信未来随着 Ceph 的不断发展，在异地数据备份领域上的应用也将更为成熟。此外，数据备份仅仅是灾备的一部分，一个完善的灾备系统还需要有数据恢复和高可用等方面。目前，这是 SDS 所欠缺的，因此 SDS 如果想要更好的实现灾备功能，还需要在数据库、虚拟化等层面与灾备软件共同配合使用。

2. 6. 2 灾备与容器

开源已经成为目前 IT 领域最重要的一个趋势，不管是大热的以 Docker 为代表的容器技术，还是对标 AWS 的 OpenStack，都为目前的灾备行业的发展提供了借鉴意义。尤其是 OpenStack 在云平台搭建中的逐步深入，正在逐渐成为云计算基础架构的事实标准，在生产环境的部署比例达到 46%，而使用通用开源平台建设的云计算基础架构，便于在双活数据中心的异构设备上灵活切换，并在互联网、证券、电信、银行、制造、医疗、能源等多个行业中得到使用。

让灾备建设与运维更加简单、系统开放可兼容及利旧，以及让灾备资源能够以服务的方式自动完成分配和发放，成为当前灾备建设的新趋势和诉求。

与此同时，IT 正在迎来以云计算为核心的第三次变革，基于 OpenStack 的云数据中心正在以其开放和融合的特性吸引更多企业客户积极投入实践。

包括 RDO、Mirantis、TCPCloud 都提供了基于 OpenStack 的 HA 解决方案，但对于 DR 则暂时没有相应的方案，只有一个概要设计，还处于 Gap 识别和补齐阶段。具体的实现主要集中在 cinder 侧元数据、业务数据同步等方面。

在容器技术方面，作为 Docker 灾备高可用的实践者，英方 i2Availability 已经完成对 OpenVZ 等容器技术高可用的完美支持，并随着业务的进一步实践，将与容器领域的企业一道推动容器在业务上的具体应用。

2.6.3 灾备与超融合

2015 年初，超融合的概念开始在国内兴起，百度的新闻搜索量刚过 2000，相比于虚拟化、云计算、大数据等概念来说，超融合显然还没有形成自己的气候。超融合基础架构(Hyper-Converged Infrastructure，或简称“HCI”)也被称为超融合架构，是指在同一套单元设备中不仅仅具备计算、网络、存储和服务器虚拟化等资源和技术，而且还包括缓存加速、重复数据删除、在线数据压缩、备份软件、快照技术等元素，而多节点可以通过网络聚合起来，实现模块化的无缝横向扩展(scale-out)，形成统一的资源池。所以，这个“超”字，同样可理解为“大”。

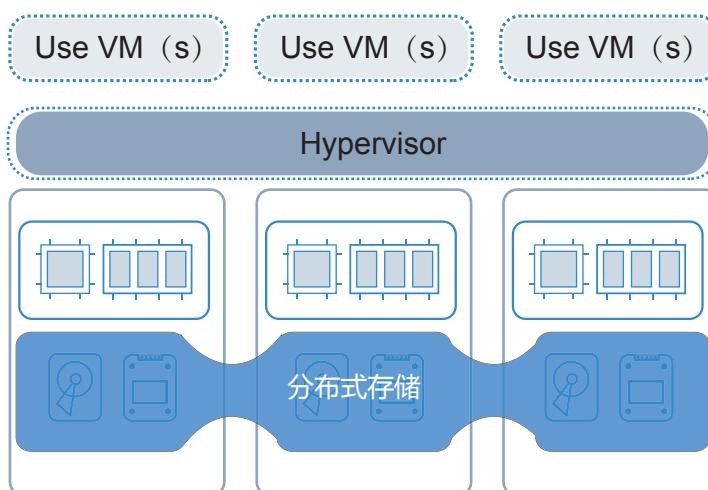


图 2.6-2 超融合基础架构

超融合的实际案例大部分还是在虚拟化环境下的用户群体里，由于扩展环境的诸多限制，超融合架构在升级灵活性和性能可预测性上会存在一些缺陷。正如 TechTarget 的知名编辑 Marissa Comeau 所言，尽管虚拟化已经无可争议地提升了服务器整合效率、增加了工作负载配置与迁移的灵活性，但由于是在更少的服务器上承载更多的工作负载，所以在硬件出现故障时也可能意味着大规模的运行中断。对于那些虚拟化为主的超融合架构，可能缺乏 HA 的支持，因此同样有可能存在单点故障。因此，在超融合的“融合”体系中，灾备将是重要的一环，对于任何 IT 团队来说，都不应该选择没有任何备份的生产系统。

2.6.4 灾备与云计算

云计算作为一种按使用量付费的模式，可以提供可用的、便捷的、按需的网络访问，进入可配置的计算资源共享池（资源包括网络，服务器，存储，应用软件，服务），这些资源能够被快速提供，只需投入很少的管理工作，或与服务供应商进行很少的交互。

云计算的使用，可以大幅度减少用户的 IT 资源与人力成本的投入，同时获得更加弹性和强大的计算能力，对快速拓展业务非常便捷。近些年，云计算的价格在大幅度下降，导致用户上云成为趋势。但是作为一种不可自主掌控的 IT 资源，用户业务数据上云的安全存在诸多隐患，例如网络攻击。根据某国内大型云计算供应商提供的数据，其每天均会遭受大量的安全攻击，据统计，每天防御超过 2 亿次的密码暴力破解；每天抵御 2000 万次的 Web 入侵防御；每天抵御 1000 次以上的 DDoS 攻击。同时，云计算内部的安全机制也相当重要，2017 年 6 月 10 日，荷兰海牙的一家云主机商 Verelox “所有客户”的数据，被前任管理员全删了，并且擦除了大多数服务器上的内容，客户数据恢复希望渺茫。

因此，云灾备正在成为一种云上安全的重要措施。在没有任何的系统是百分之百安全的情况下，永远不要将所有数据放在一个“篮子”里，云备份

与恢复、云端业务迁移、云端高可用这些在用户数据中心机房的灾备场景，在云端同样适用。

但是云计算的数据中心机房由于分布在各地，所以云端的数据复制与容灾高可用相比本地的数据中心容灾要求，在用户庞大数据量传输需求下对带宽及距离有诸多的限制。因此，对灾备技术发展趋势的要求是能够满足不同云计算平台、长距离、大数据量的数据复制、传输和业务从本地到云端、云端到云端的快速接管的需求。

2. 6. 5 边缘计算和云灾备

边缘计算的产生背景之一，是当本地存在着海量数据处理需求的时候，由于本地网络边缘到云数据中心网络带宽、延时的限制，无法通过远端的云计算能力对本地的海量数据进行实时处理。

如果本地的存量和增量数据巨大，云灾备也会因为网络带宽的限制影响数据灾备至云端的实效性。借助边缘计算，可以将海量数据灾备至周边任一物联网终端，同时，通过数据的分块技术，对源端数据在本地进行切分，切分后的数据块在本地完成加密再传输至不同的“边缘”，保证了数据灾备至“边缘”的安全性。

伴随着数据的计算和存储技术的演进，灾备技术也在随之发展。灾备端从本地机房到异地机房，再到云端，未来有可能又回到本地周边的“边缘”，回归的是数据灾备的存储介质，提升的是我们对数据和业务保护的态度和要求。

第三章 云灾备

以云计算为基础的第三方 IT 技术平台正在逐年增加，并成为协助企业转型的重要推力。据 IDC 数据显示，到 2020 年，中国将成为全球最大的第三方平台市场。在云与大数据时代，企业对第三方提供的灾备服务的需求将越发强烈，云灾备作为灾备领域的一个新兴概念，它的出现，为企业在云端的数据备份和业务连续性提供了行之有效的解决方案。

3.1 云灾备

云灾备将灾备看作是一种服务，由客户付费使用灾备服务提供商提供灾备的服务模式。采用这种模式，客户可以利用服务提供商的优势技术资源、丰富的灾备项目经验和成熟的运维管理流程，快速实现用户的灾备目标，降低客户的运维成本和工作强度，同时也降低灾备系统的总体拥有成本。

云灾备与传统的组织单位在本地或异地灾备模式不一样，云灾备是一种全新的灾备服务模式，主要包括传统物理主机、虚拟机等 IT 系统，往公有云或私有云等云端化灾备的趋势，以及新业务形态下，云端，云与云之间的灾备等。在具体的实际场景应用中，云灾备包括了传统的数据存储和定时复制，以及数据的实时传输、系统迁移、应用切换，保证灾备端应急接管业务应用等范畴。

3.1.1 云灾备的定义与发展历史

为了科学、准确的定义云灾备及其服务，根据实际业务部署，本白皮书所定义的云灾备是指灾备业务的云端实现形式，主要包括云备份与云容灾，云备份与云容灾是一个有机的统一体。其中云备份是指备份技术将生产存储数据直接备份到公有云上，进而实现数据备份与恢复功能；云容灾则是指通过数据 / 系统的云端迁移、高可用等方式实现业务的快速接管，保证业务连续性。

现在，我们简要回顾一下云灾备的发展历史。

2006 年 Google 正式提出云计算的概念。同年，亚马逊正式推出网络服务 AWS (Amazon Web Services)，其主要产品 S3、EC2 等相继获得了成功。

2008 年开始，企业信息化建设不断加深，数据的安全与完整已经成为企业信息化体系中的必需元素，数据及业务的灾备也已经成为保障企业稳定发展的重要手段之一。阿里云、腾讯云、AWS、Azure 等云平台提供的云存储目前正在成为全球存储行业的发展潮流之一，虚拟化云存储应用于灾备已是行业趋势和现实，并衍生一种新的灾备理念——云灾备。当然灾备的本质和核心并没有变化，**数据复制依然是灾备技术的核心技术之一。**

2009 年开始，在云计算领域，国内的 BAT 先后建立了自己的云计算平台，其中阿里巴巴的阿里云凭借与 AWS 相似的基因，迅速在国内公有云市场占到了一席之地。

2012 年，经过几轮激烈的价格战之后，云主机、云存储、网络带宽的成本进一步降低，这给了云灾备的发展奠定了基础。云资源用途广泛并且数据比其他 IT 资源更易得到，同时它对于中小型企业来说具有显著的成本优势。

2013 年，国内开始讨论“云灾备”的概念，百度百科词条创建，一些云计算、云存储企业开始在自身业务上涉及云灾备，英方股份以其复制到云的理念，也展开了全面的技术适配。

2014 年，在云计算以及最新的一波创业浪潮的推动下，云灾备开始以一种独立的业务形态开始出现。

2015 年，灾备领域的领导者上海英方软件股份有限公司正式推出旗下的云灾备平台——英方云 (i2yun.com)，该平台实现了企业数据的备份与恢复、系统迁移以及业务的高可用等功能。

2016 年，云灾备成为灾备行业最重要的关键词之一，用户本地到云端、云与云之间的数据迁移、备份与恢复、业务的高可用等需求批量出现，这主

要得益于云计算的普及，以及数据作为组织重要资产的安全保护机制的逐渐建立。

2017 年，云灾备场景应用中的云备份与恢复、业务云迁移、云高可用、云共享、云资源等开始出现在各大公有云市场，用户开始对云灾备选择信任。

3.1.2 云灾备的特点

云灾备结合云计算、云存储的诸多优势，同样具备了多方面的优势：

1) 基础设施减少

抛弃采购传统的灾备服务器，借助云平台供应商提供的计算和存储平台，或者直接采用云灾备 DRaaS 应用服务，如英方 i2yun.com，解决系统崩溃的苦恼，用户也不再需要去采购新的存储，以及随之带来的维护需求和成本。用户甚至可以关闭备份中心，在节省更多的物理空间的同时，也可以节省更多的 IT 资源，如将相关的备份维护人员解放出来，参与到其它的工作中去。灾备系统的维护交给云计算以及类似英方云这样的云灾备服务供应商，由后者定期测试和维护用户的相关灾备系统。

2) 降低 IT 成本

传统的存储系统主要通过 RAID 来实现数据冗余和数据恢复，并且在主机上为每个硬件部分如 CPU、内存、网卡、电源、风扇等配备两个或多个来防止单点失效（SPOF，Single Point Of Failure），如此当某个部件出现故障时，告警机制会通知管理员进行相应故障部件的排查和替换。云存储系统则主要采用大量廉价的普通主机，是基于网络，利用分布式协同软件，将数据分散存储于若干通用存储服务器上，并通过副本或编码方法进行综合管理，向用户提供可靠的统一的逻辑存储空间，但单台云主机故障发生概率也相对较高，所以基于云主机、云存储的容灾机制必须开始就被包含在架构设计和每个开发环节中。根据具体需要采用更为经济、更具弹性的云存储进行备份，免去自建数据中心所带来的硬件购买及维护成本，免去维护各种硬件所带来的烦恼，实现了对资源的精细化管理，进而减少大部分的灾备支出。

3) 按需付费

不同于传统的灾备方案需要建立架构完全对应的灾备中心，云灾备可以采用云基础设施，或者灾备即服务的模式，允许用户自由选定重要的系统和数据。因为底层架构被其它采用同样云计算解决方案的公司所共有，共同分担成本，所以用户只需为实际所使用的资源付费，从而大大减少了资源的浪费，并提升了效率。

4) 高度机动性

基于虚拟化云计算技术，实现了在主节点已经异常而无法提供服务时，仍然在云端保持系统的稳定运行。只要能连上网络，员工仍能继续在原有的服务器环境中工作。这种高度机动性，使得从一个办公场所移动到另一个场所，或短期的在家办公都极为方便。

5) 高度灵活性

云灾备使得业务需求更容易评估，用户可以更准确预估哪个系统、甚至哪个子系统确实需要维护。也可以更细粒度地选择关键的数据来优化自身的备份计划，而不是整个地完全备份，更精确地设置 RPO(Recovery Point Objective)，即能容忍的最大数据丢失量。云中建立的高可用、高容错架构可以提升恢复时间和恢复点目标，基于公有云平台或者开源的私有云技术也可以简便快速灵活地构建灾备节点并将数据迁移或者复制到云端，提升灾难恢复的速度。

6) 快速恢复

对于灾难发生时，多长的停机时间是可接受的，不同的用户针对自身业务特点有不同需求。而如果服务器宕机、长时间的电力中断、光纤挖断或突发的自然灾害，这些意外发生后多久会导致损失，对于很多用户而言答案是立刻。因为即使有传统定制的远程备份，仍然需要时间去做数据的恢复和业务重启，且取决于远程备份的地点远近和远程服务器的性能。随着云灾备云高可用的出现，你可以预先准确估计恢复的时间，确保停机时间在一个可接

受的合理范围内，从而可以制定一个准确的、可交付的 SLA 协议，并可以远程使用云计算和云存储资源。

7) 安全备份

很多公司都有和现有生产系统直接或间接在一起的备份系统。但很多灾难发生时，会同时对当前的网络系统造成冲击，从而也影响到相关联的备份。如相应的系统被网络攻击或篡改数据，则对应的备份系统也不能幸免。而云灾备采用的云平台一般具有高可靠高标准的异地“云端”机房等基础设施，使得备份被安全地存储在异地，简而言之，数据任何情况下都是相对安全的。当然服务商以及云灾备技术选择很重要，比如是否具备云端 CDP 持续数据保护能力等。

8) 服务导向

美国国家标准与技术研究院（NIST）对云计算的定义为：云计算是一种按使用量付费的模式，这种模式提供可用的、便捷的、按需的网络访问，进入可配置的计算资源共享池（资源包括网络，服务器，存储，应用软件，服务），这些资源能够被快速提供，只需投入很少的管理工作，或与服务供应商进行很少的交互。

简而言之，云灾备服务独有的高性能、高可靠性、高扩展性、易维护性、责任风险低以及高性价比的服务特色，为企业和政府数据信息系统“保驾护航。”

3.1.3 云灾备实施注意事项

云灾备虽然特点明显，但是在具体规划实施过程中，还要考虑如下四个问题：

1) 成本问题

如果是选择第三方服务商提供的云备份的话，那么主要支出包括：存储空间、带宽以及数据迁移等费用支出。以存储为例，某云服务商提供的归档服务为例，每 GB 的报价为 0.033 元 / 月，那么每 2T 的数据一年的费用为

($0.033 * 12 * 1024 * 2$) 811 元，而某硬盘厂商 2T 的（消费级）硬盘价格则为 569 元。仅从存储价格来看，云的确不占有优势。云的核心竞争力其实是提供了硬件产品所不具备的快速扩容能力以及节省了硬件安装和维护费用。这些都是成本核算中的重要因素。

此外，数据在云与本地之间的迁移同样需要费用的支出。比如某国外云服务商的数据迁移只在数据离开云平台（下载）的时候是收费的，而英方股份的数据迁移则按照次数进行收费。

2) 时间问题

不管是备份（上）还是恢复（下），云的优势都并不十分明显。虽然专线、VPC 的数据传输率都可以达到 10GB/S，但这更多的是一种高端服务。因此，企业应该明确有多少数据要进行备份？一次备份多少数据？隔多久备份一次？再根据网络带宽得到传输总耗时，在数据恢复的需求中制定准确的 RTO、RPO 规划。例如，虽然有些云平台的数据备份及归档具有价格优势，但开始恢复的准备时间却高达十几个小时，而之后等待数据回传结束还需要更多的时间。

3) 安全问题

安全问题包括两个方面：一是基础架构和网络的安全性，主要需要防止系统 bug 及网络运维问题的出现。另一个方面则是在用户看来更为重要的数据安全，主要危害来自黑客入侵及内容人员的盗取等。数据加密是最常用的数据安全方式，可以在源端、备端以及传输渠道进行加密。其中，核心的问题是密钥如何保存、如何使用等问题。

4) 合规问题

合规问题应该引起大家的足够重视，因为长期备份的数据需要面临归档的问题，虽然**数据归档后**和业务连续性的关系逐步弱化，但归档数据依然要受到合规性的强制约束。以医疗行业为例，根据现行的《医疗机构管理条例实施细则》第五十三条规定：“医疗机构的门诊病历的保存期不得少于 15 年；

住院病历的保存期不得少于 30 年。诸如此类的合规性要求，是云灾备持续发展的基础。

3.1.3 虚拟化及混合云化

用户通过虚拟化可以解决异构存储问题，提高存储的利用率。新型存储虚拟化技术不需数据大量拷贝，降低成本，此外，虚拟化还将进一步促使共享式灾备服务的普及，虚拟化已经成为中国灾备市场技术领域探讨的一个热点。

云环境下灾备技术架构的核心在于所有资源的“池”化，即通过实现服务器、存储、网络、安全组件以及机房等其他辅助设施的资源“池”化，构建一个标准化、可弹性伸缩的资源平台，再借助高效的云调度和管理平台实现各类资源在不同应用间的动态调配。虚拟化管理平台可实现对多达上万个虚拟机的高效管理和集中控制，可针对 CPU、内存、磁盘和网络带宽的阈值及业务需求优先级进行预定义，虚拟化平台的扩展功能也十分强大。同时，虚拟化平台还具备高可用的功能，通过对虚拟机采用的故障切换解决方案保持较高的可用性。

伴随着虚拟化技术的发展，与传统物理主机，云主机并存的广泛应用，混合云化是一个长期并存的事实和趋势，也是云灾备技术应用的典型场景。

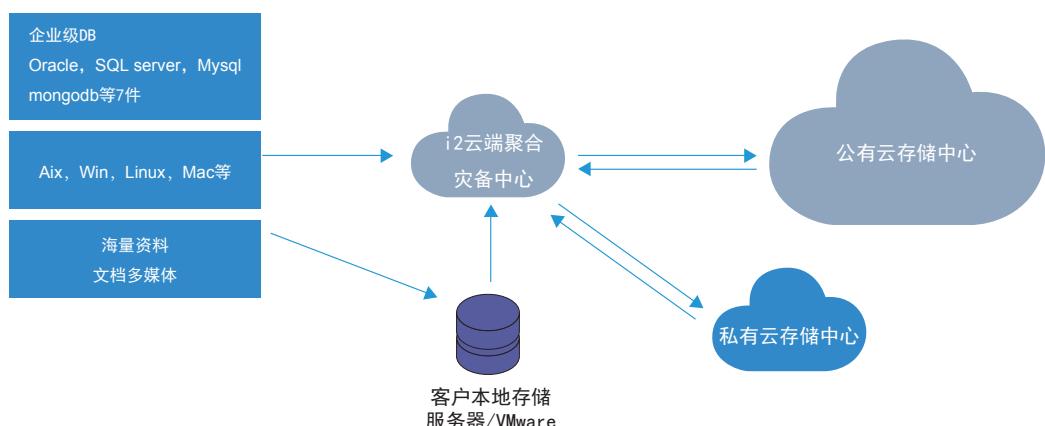


图 3.1-1 混合云灾备架构图

3. 2 云灾备的具体业务模式

在传统的IT架构中，存在着明显的分层，包括存储层、系统层、应用层等，针对不同的层级，也会有不同的灾备方式。这种层的概念，在云计算中同样存在。

3. 2. 1 SaaS 层灾备

SaaS（Software-as-a-Service 软件即服务）是云计算的最上一层，也可以理解为传统IT架构的应用层。我们常用的浏览器、QQ等都可以认为是一种SaaS，所以SaaS的本质依然是软件。通过SaaS这种模式，用户只要接上网络，通过浏览器就能直接使用在云端上运行的应用，并由供应商负责维护和管理云中的软硬件设施，同时以免费或者按需使用的方式向服务商支付费用，所以用户不需要顾虑类似安装、升级和防病毒等琐事，并且免去初期高昂的硬件投入和软件许可证费用的支出。

在灾备的体系中，备份数据的存储方式依然是一个关键，随着云计算的兴起，SaaS企业可以直接在云端购买一个属于自己的数据中心，然后出租给用户，这便是SaaS与公有云云灾备的基本模式DRaaS灾备即服务。以英方云为例，通过与阿里、腾讯、百度、天翼、沃云等云平台合作，英方云可以将自身在灾备上的技术优势直接与云端链接，进而为用户提供即开即用的DRaaS云灾备服务。

3. 2. 2 PaaS 层灾备

PaaS（Platform-as-a-Service 平台即服务）的主要服务方式是通过云将IaaS层资源动态管理和分配，用有限的资源提供身份认证管理、应用资源管理、工作流控制管理、服务总线管理、基础资源调度等服务。PaaS本身就是一种平台化的服务模式，因此在PaaS层的灾备主要是通过对用户服务器进行多机房部署和异地容灾，进而在基础设施上保障了高可用性。比如AWS便在2015年推出了为其云客户提供不中断业务正常运行时的在线备份服务，并为PaaS管理员提供回滚的操作。

3.2.3 IaaS 层灾备

IaaS (Infrastructure-as-a-Service 基础设施即服务) 是云计算的最底层，也可以理解为 OSI (Open System Interconnection) 的物理层及数据链路层。相比于公有云的“公寓”，很多企业在预算充足的情况下，希望可以在云端建一个自己的“别墅”。这个别墅式的云灾备系统就需要更多的借助 OpenStack 等开源代码平台进行搭建。

作为云计算的管理平台，OpenStack 融合了多个模块，因此在具体的灾备部署中，可以通过存储控制节点、计算节点等模块的 API 接口实现数据的备份及高可用切换。比如，在生产环境中，可以将虚机部署在 cinder-volume 或者共享的存储比如 RDB 或者 NFS 上，当虚机出现故障时，可以从共享存储上将其恢复（使用 nova evacuate 功能）。

3.2.4 DRaaS (灾难恢复即服务)

DRaaS(Disaster Recover as a Service 灾难恢复即服务) 相对于可以恢复到本地的异地存储备份，DRaaS 提供基于云的计算能力，不仅可以实现数据的恢复，更可以在云中通过虚拟机启动整个业务系统。

Gartner 预计，到 2018 年，采用灾难恢复即服务 (DRaaS) 的组织机构数量将超过采用传统服务的数量。

未来，灾备行业的魔力象限将包括以下三种云灾备服务模式：

种 类	服务内容
灾难恢复即服务 (DRaaS)	服务提供商管理虚拟机副本，可以选择将来自生产数据中心物理机副本保存到云中，虚拟机 / 物理机在云内激活，在云内进行恢复。
使用基础设施即服务进行恢复	客户管理来自生产数据中心的虚拟机副本保存到云中，提供商管理虚拟机在云中激活，客户在云中进行恢复。
使用备份即服务 (BaaS)	提供商负责从生产数据中心备份虚拟机到云，客户请求虚拟机找回（在云中或者云外），并且客户负责进行恢复（在云中或者云外）。

表 3.2-1 三种云灾备服务模式

3.3 云灾备的主要产品形态

云计算已经成为一种新的底层操作系统，而不管是平台还是操作系统，都需要杀手级的产品，并且只有那些可以为这个操作系统提供配套服务的杀手级产品才能生存。脱离了 IaaS 的 SaaS 和传统软件没有本质区别，只有在 IaaS 的基础上 SaaS 才能获得长足的发展。

平台化的环境下，灾备服务需要打造更强的“云亲和力”，以一种“模块化”的接口、通道的方式建立自己的核心竞争力。灾备的云化需要演变为一种“hub”的概念，通过在云与云之间、云与本地之间打造一个“集线器”的产品形态，进而成为数据的云端输送者。

3.3.1 云迁移

对于众多企业来说，云的优势越来越明显，比如希望通过从不同的地域位置运行工作负载来增加灾难恢复的选择，又或者出于投入成本方面的考虑，甚至是传统供应商的令人不愉快的租赁和繁琐升级问题。这些都可以是企业向“云”看齐的原因，不过，在涉及到本地或云端的具体实施过程时，一个较为重要的问题就是数据的迁移。

据国外媒体最近对 240 位信息 IT 和安全专业人员进行的一次调查显示，尽管在数据中心应用迁移到云服务这个过程中经常会出现应用连接中断问题，但还是有许多机构计划把数据中心应用迁移到云服务中。云迁移不只是从本地到云的转变，还有可能是从一个云到另一个云的迁移，比如从公有云迁移到另一个公有云、从私有云迁移到公有云等等。

目前，云迁移服务可以将复杂的系统迁移工作简单化，且在生产系统不停机情况下迁移现有应用或者整个系统，包括操作系统、应用程序、用户信息、网络配置等所有的数据，整个迁移过程时间可预测，并可在迁移完成后立刻切换到新系统，真正迁移过程服务不停止。当前，云迁移产品可以支持 V2V、P2V、P2P 等多种形式的系统迁移。同时市场上出现的云迁移产品形态众多，支持功能各异，以下几个特点供参考：

1. 无需停机

在应用和系统迁移的过程中，源机无需停止应用或者系统；业务不受影响。支持本地或者长距离远程迁移。

2. 与硬件无关

支持在不同的硬件平台之间进行应用和系统迁移；支持 V2V P2V、P2P 等的应用和系统迁移。

3. 多系统支持

Windows 支持 Windows 2003、2008、2012 上的应用和系统的迁移；Linux 全面支持 Centos、SUSE 10/11 系列、Redhat Enterprise 等。

4. 简单高效

部署简单，易于应用，一键式迁移，确保成功后才切换，整个迁移过程时间可预测，并有图形化监控和管理。

3.3.2 云备份与恢复

云备份的概念最早可以追溯到云计算概念最开始兴起的时候，并且在网盘、手机备份等产品的推动下，云备份逐渐成为云计算最为普遍的一种应用模式。相比于传统的备份，云备份不仅具备了简单的数据存储功能，在增加了相应的分享、恢复等功能之后，云备份更可以将系统灾备软件和云计算平台技术结合为一体，通过云计算资源共享，实现成本低廉、部署迅速、灵活弹性的远程数据灾备服务。

云备份需要依靠迁移工具完成，在整个云灾备的生态中，云服务商往往提供存储、计算、网络安全等服务，用户的数据迁移、备份和容灾需要依靠第三方软件服务商完成。英方云全面支持 Windows 和 Linux 平台以及虚拟平台上的各种应用数据的保护，包括 SQLServer、Exchange、DB2、Oracle、MySQL 等。英方云备份和恢复产品具有以下优势：

1. 高效

快速部署，易于应用，开通功能只需几分钟；随时可变更的主机规格和

带宽，高资源利用率。

2. 安全

AES256 数据加密，压缩传输，提供数据传输的安全性。

3. 可靠

电信级别的服务器运行环境，可达 99.995% 的设计可用度，99.99995% 的设计数据持久度。

4. 高性能

以字节为数据捕捉的最小单位，从而极大地减小了需复制的数据量，从而节省了带宽。

5. 低成本

充分利用云计算平台的成本优势，降低容灾成本投入；不需要初始大规模投入，只需按时付费。

在云备份与恢复场景应用中，公有云、私有云和混合云上的备份与恢复场景最常见。

公有云备份和恢复可选择私有云 + 公有云平台 + 三大运营商云平台的方案，用户可选择把数据实时备份到阿里云、腾讯云、百度云、华为云、青云、沃云、天翼云等云平台。当用户需要恢复时，可直接从云平台进行快速恢复。场景适合接受公有云的企业和个人用户，费用低、免维护、易扩展。

私有云备份和恢复可与企业现有的私有存储对接，或二次开发整合到企业现有 IT 资源中。私有云灾备系统部署在企业自己的服务器上，所有信息由企业自己掌握，部署方便。并通过 API 二次开发整合到企业 ERP、CRM 等现有 IT 资源中。场景适合不上云、高安全性、高要求自主数据控制的企业。

混合云备份和恢复是未来大型用户在云端进行灾备的趋势，混合云灾备兼顾了公有云在灾备建设上的成本优势和私有云的安全性能。在云端，灾难恢复一般采用主从架构，如果都使用私有云，相对运维成本较高。在混合云

的架构里，可以考虑把备用部分放在公有云，用于主服务器宕机时，短时间内保证业务的连续性，同时可以节省成本。

场景应用分两种情况：一些用户（通常是行业用户）会把核心应用放到私有云上，然后将非核心应用或者创新应用部署在公有云；另外一些用户出于安全等因素的考虑，将业务数据放在私有云，而将应用运行在公有云上。

场景适合已有公有云和私有云业务或未来计划上云的企业用户。

3.3.3 云高可用

传统的高可用（High Availability）是指通常一个经过专门设计的系统，从而减少停工时间，而保持其服务的高度可用性。实现方式主要包括：主从方式（非对称方式）、双机双工方式（互备互援）、集群工作方式（多服务器互备方式）三种。

在云计算环境中，高可用的实现方式主要以第二种和第三种方式为主，在保证高可用的同时，利用多机分担负载，也具有高的扩展性（Scalability）。通常来说，云计算的计算资源和存储资源是以集群形式实现的，特别强调可扩展性。英方云高可用，可以帮助客户在云端建立针对应用或者系统的灾备系统，在异地建立一套完整的与本地生产系统相当的备份应用系统当一处系统因意外停止工作时，整个应用系统可切换到另一处，使该系统功能可以继续正常工作。目前，云高可用实现快速（秒级）切换接管的产品凤毛麟角，以下是市场上出现的云高可用产品，具有以下特点，供参考：

1. 自动切换

实时监控源机应用或者系统，发现异常及时通知管理员；根据设置，自动切换到备机系统，可监控，网络、服务、进程等各种资源。

2. 灵活部署

支持本地到云端的高可用，支持云端到云端的高可用。

3. 操作简单

图形化监控，异常告警；一键切换 / 回切，或者自动切换。

4. 低成本

快速部署，易于应用，开通功能只需几分钟；随时可变更的主机规格和宽带，高资源利用率。

云高可用产品应用场景包括：本地到云端高可用场景和云端到云端高可用场景。

本地到云端高可用场景特点是IT系统本地运行，实时数据云灾备，图形化监控，异常告警，一旦本地出现故障，用户可以进行一键切换或者自动切换，实现云平台与本地实现无缝的业务连续性接管。场景适合所有接受公有云灾备的企业用户，费用低、免维护、易扩展。

云端到云端高可用场景特点是在按需分配的基础上，通过云端与云端的灾备，既可大大节省建立多个专有灾备中心的费用，如相关的硬件、软件、电力、冷却以及管理等的费用，又可享受海量存储和高性能云计算的服务。场景适用于与硬件无关的连续数据保护场景。

第四章 灾备业务实施及服务质量评价

在 IT 信息领域，技术从传统的 IT 架构到云计算的驱动发展，是来自终端用户对业务操作体验的选择权。对于由 IT 架构延伸的应用体验，性能的强弱决定着用户满意度的高低，并最终影响到是否能够留住用户。

根据调查数据的显示，1 秒的延迟，会导致页面转换率降低 7%，流量下降 11%，用户满意度降低 16%；如果在完全竞争环境下，57% 的访客在等待 3 秒后放弃，其中 80% 访客不会回来，50% 访客转向竞争对手。从这个层面讲，组织机构对于业务的灾备建设的规划和实施，是确保数据安全和业务连续的有效举措。

本章我们将讨论灾备建设的实施步骤和方法，并根据业界对灾备服务质量评价的体系进行归纳。

4.1 灾备建设三部曲

4.1.1 业务连续性规划

灾备建设的最终目的就是要保护业务的连续性运行，其具体要求需要通过进行业务连续性规划来确定。因此，业务连续性规划是进行灾备建设的大前提。没有业务连续性规划，灾备建设就没有意义，充其量只能做到数据不丢失，不能及时恢复业务运行，而保障业务连续性运行才是真正核心。通过业务连续性规划，分析梳理出各项业务的恢复优先级及其恢复要求（RTO、RPO 以及恢复业务所需的资源等），进行业务连续性规划的方法通常采用国际上流行的 DRI 十大最佳惯例：

- | | |
|--------------|-------------------|
| ①规划启动与管理 | ②风险评估与控制（RA） |
| ③业务影响分析（BIA） | ④制定业务连续性策略 |
| ⑤应急准备及响应 | ⑥编制和贯彻实施业务连续性计划 |
| ⑦认知与培训计划 | ⑧业务连续性计划的演练、审计和维护 |

⑨危机沟通

⑩与外部机构的协调

这是国际通用 BCM 规划的方法，适用于企业和业务功能，当然也适用于信息系统。业务连续性规划确定了保护业务的各项要求（如 RTO、RPO 等），支持业务运行的信息系统自然就要根据这些要求来确定相应的信息系统恢复目标和恢复策略。

4. 1. 2 灾备规划

灾备是通过保障支持业务的信息系统的连续性运行来实现最终保护业务的正常运行。因此，在通过业务连续性规划梳理出业务的恢复要求和恢复优先级后，就要根据这些要求来梳理支持这些业务的 IT 应用，同样需要分析出这些 IT 应用的恢复优先级和恢复指标（RTO、RPO，以及恢复所需的资源等）。

灾备规划采用的方法与业务连续性规划的方法基本一致，主要区别仅在于前者针对的是支持业务运行的 IT 应用和系统，后者主要关注的是业务流程。这里针对 IT 应用和系统的恢复要求应该与针对业务的恢复要求相匹配。通过灾备规划，确定所有支持业务运行的 IT 系统的各项恢复指标，并制定 IT 系统的恢复策略以及 IT 系统的恢复计划。

4. 1. 3 灾备方案设计和实施

根据灾备规划对支持业务运行的 IT 系统提出的恢复要求和恢复策略，来设计灾难恢复技术方案，例如同城灾备、异地灾备、两地三中心、双活、云灾备等等。需要注意的是，评价这些技术方案的适用性时，并非恢复时间越短就越好（恢复时间越短往往成本也越高），满足灾备规划确定的恢复要求（RTO、RPO 等）才是最为重要的。只有满足灾备规划提出的恢复指标要求、技术成熟可靠、成本效益高的灾备方案才是最佳选择。

灾备方案的实施是确保所设计的灾备方案真正有效的重要环节，需要制定详细的工作计划，包括场地选址、产品选型、服务商选择、资源保障、项目管理、验收评审、演练测试等内容。同时还应该根据灾备设计方案，结合

业务连续性规划要求，制定出完整的灾备计划（包括灾难应急响应总体预案、危机沟计划、各系统的专项应急预案等），确保各部门在灾难发生时能够统一协调地行动。

4.2 灾备规划的方法

4.2.1 风险分析与业务影响分析

1. 风险分析

企业需要根据自身所处环境的实际情况，确定 IT 运行环境中存在哪些无法接受的物理威胁或者可能发生的灾难，并对灾难发生的可能性、目前可能的防护措施的有效性和该灾难所威胁的资产价值进行分析，最终得到带有优先级别的需要防范的风险及其分级列表，并制订出可能的处理方法。例如接受该灾难发生时的风险而不进行防范、制订该灾难的预防措施或者采取购买保险等风险转嫁策略。

2. 业务影响分析

在本阶段，通过走访各业务部门的相关人员对各种业务流程进行分析，了解各种业务流程对企业的重要性和时间敏感性。同时根据相关的评判原则，得出在核心流程由于灾难发生而无法正常进行时企业本身的损失情况。这种损失可能是可以量化的，例如单据的丢失、计算的错误而导致的直接损失；也可以是无形的损失，例如客户满意度及竞争优势的丢失。通过对可量化和不可量化损失的综合考虑，得出各种核心业务流程对于灾难受损的可容忍程度，并作为确定其恢复优先级的决策依据，最终确定这些核心业务流程的恢复要求指标，例如 RTO、RPO、DOO、NRO 以及恢复所需的各种资源等。

4.2.2 灾备方案设计

结合分析阶段的分析成果，以及企业本身在灾备上的投入，制订企业短期、长期范围内的灾备策略和目标，并有意识地将企业本身的人员组成和组织架构做出调整以适应策略要求。本阶段最为重要的是制订出灾备的具体实

施方案。

灾备方案可供选择的范围很大，但所有的灾备方案都必须考虑的因素包括恢复时间、实施与维护灾备策略所需的投入等。灾备恢复时间的需求越短，所需的实施成本就越大，实施难度也就越高。

4. 2. 3 灾备计划制定

有了 IT 系统的恢复方案，只能够保证在灾难发生时，IT 系统的恢复能够支持业务的恢复目标，但是业务的连续性并不只是 IT 系统的恢复。因此，灾备方案在设计中还需要涉及包括办公场地、办公设备、紧急流程、指挥架构、人员调度等多方面、多部门的综合考虑。只有业务执行过程的每一个环节都达到灾备目标的要求，才能够认为灾备方案的目标得到了满足。因此，需要制定一个完整的灾备计划，来统一协调各部门在灾难发生时的行动计划。同时制定灾备计划时需要确保其与企业业务连续性计划协调一致。一般来说，每个企业都应该设立一个由领导挂帅，各业务部门和 IT 部门联合组成的一个灾备指挥小组。

4. 2. 4 灾备方案实施

灾备体系的搭建经常需要涉及到公司内多个部门的协调，因此在方案实施的过程中，需要把每项工作的内容、目标要求、实施的方法步骤以及督促检查等各个环节都做出具体明确的安排，具体落实到工作分几个阶段、什么时间开展、什么人来负责、领导及监督如何保障等。

方案在实施的过程中具有很强的规定性，表现在两个方面：一方面，方案实施要根据方案分析和方案设计的具体操作流程进行，而不能是随意进行。有效的灾备操作流程往往可以节省大量的时间和减少错误。反之，就会带来不必要的损失。例如，在虚拟环境下的灾备系统，就要提前规划需要用几台服务器去虚拟出三十、四十，甚至上百的虚拟服务器，而且需要长期运行。如果没有好的操作流程，不利于灾备中心的运维。另一方面，方案实施工作具有强制性，一旦开启，相关部门单位就要按照具体计划认真组织实施。

4.2.5 灾备演练

灾备演练是基于不同灾备类别中某一特定的场景而进行的，灾难场景不同、灾备技术复杂度不同，演练的技术过程与周期也不尽相同。

具体的演练包括：系统更新、调整，原有的灾难恢复预案是否仍然有效；灾备系统是否需要进行有效的更新；系统切换流程、步骤是否有遗漏和错误；灾备系统的切换时间是否可以满足业务的恢复需要等等。

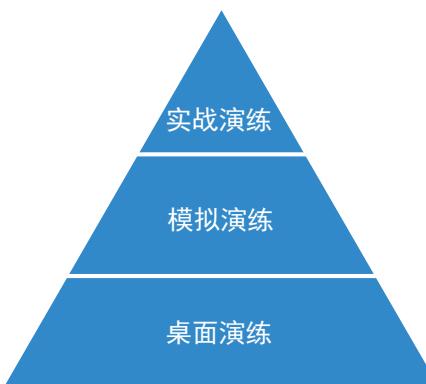


图 4.2-1 常见的三种灾备演练方式

常见的三种灾备演练方式包括：

1. 桌面演练

桌面演练也叫“沙盘推演”，是最基础的灾备演练方式。通过对初始灾难恢复预案的一个理论验证，进而测试急响应预案和灾难恢复体系的完整性和有效性，使相关人员了解应急响应及业务恢复流程，全面验证技术及业务管理指挥、流程操作、协调配合等方面的能力。

桌面演练工作量小，易于实施，可以根据实际需求灵活开展，并可以模拟多个场景。

2. 模拟演练

模拟演练以桌面演练结果为基础，由 IT 部门与相关业务部门参加模拟演练，采用模拟数据和模拟业务系统运行演练。模拟演练的过程高度接近真实灾难发生时的处理过程，通过演练可以检验灾备系统的可用性、灾难恢复

预案的可行性以及增加参演人员对灾难处理过程的感知度与配合的默契度。

模拟演练是一种对现有生产环境没有影响的演练方式，由于需要虚拟出较为真实的使用场景，因此在技术上的要求较高。

3. 实战演练

实战演练需要灾备中心真正接替生产运行一段时间，是在具体设定的灾难场景下，将业务切换到灾备中心及业务恢复环境，并在完成数据、应用及业务恢复后由灾备系统提供对内对外的业务服务，原来的生产环境可以进行必要的系统维护或者为灾备环境提供备份支持。

作为灾备演练的最高的阶段，实战演练的场景最为真实，更易于发现潜在问题并进一步完善灾备系统，但随之而来的就是演练成本的提高。因此，在实战演练中，也会存在很多挑战，这时，关键是使其理解并支持演练能够周期性地进行，同时发现问题及时改进才是成功的演练（无论是否用到真实环境），应避免流于形式的表演。

验证已建成灾备系统的可用性、有效性，通过演练结果来修正、补充、完善灾备恢复预案并为灾备系统的升级建设提供理论依据及数据指标，从而使企业在灾备建设中有据可依，保证建成的灾备系统能充分实现建设的目的、达到建设的目标。这就是灾备演练的意义所在，并敢于考验演练中团队的决策与指挥能力。

4. 2. 6 专家服务 (ADTIS)

1) 定义

专家服务是灾备行业常见的咨询服务，以英方为例，已经推出的专家服务业务，旨在减少中间环节、降低无效成本，并最终实现快速部署、高效可靠的专家级业务服务体系，从 0 到 100，全程专家指导。

2) 特点

- ①针对性强、效力高、可执行；
- ②阶段划分和决策点明晰；
- ③经验证的模块化实施方法；
- ④终身服务。

3) 专家服务的 5 个阶段



图 4.2-2 专家服务的 5 个阶段

1. 评估阶段 (Assessment)

需要对企业的整体灾备目标及投入进行有效的评估，包括 RPO、RTO 的相关指标以及 IT 系统的整体架构，主要以专题会的形式进行，并且就相关事项形成书面纪要，评估阶段主要以免费的形式进行，但由于评估阶段也需要投入大量的资源进行对接，因此部分服务会保留收费的权利。

2. 设计阶段 (Design)

针对评估的具体结果，在双方合作意向明确的前提下，由专家团队主导进入设计阶段。此阶段将会直接影响项目的最终交付。因此，英方将以经验证过、稳定的系统为蓝本提供完善可执行的灾备设计规划，并在此过程中，积极听取需求方的意见。

3. 测试阶段 (Test)

为保证项目的顺利进行，英方将对已经设计好的灾备系统进行实地测试，同时保证在测试的过程中不对用户的现有系统造成影响，测试阶段主要包括软件的具体使用、功能的具体实现以及灾备演练。测试可以暴露灾难恢复计划的不足之处，测试也可以帮助我们评估计划执行人员的快速响应能力和效率，灾难恢复计划的每一个要素都必须测试，保证其恢复过程的准确性。

4. 实施阶段 (Implementation)

此阶段指项目的现场或远程交付阶段，此阶段的主要工作是项目实施人员根据设计、测试阶段确认的具体需求内容进行具体功能的实现工作。在功能实现的过程中，项目实施人员将记录软件实现的详细过程，便于售后服务之用。每一个实施技术人员都将严格按照要求记录、存档。

5. 维护阶段 (Support)

在新需求、新技术的不断涌现以及新的内部和外部规则的变化过程中，IT 系统也会随之改变，所以要确保灾难恢复计划的有效性就必须定期的检查和修改计划。项目上线运行后，系统运营维护的主要工作将交由客户进行，但英方将提供一整套完善的技术支持服务，保证在产品生命周期内有效性。

4.3 灾备服务质量评价

本服务质量评价方法主要借鉴了《云灾备技术与应用白皮书(2017)》，该白皮书由英方股份联合北京信息灾备技术产业联盟联合撰写，由国家电子计算机质量监督检验中心阳小珊、田雄军主要撰写。该评价体系适用范围广，行业知识专业，可以帮助用户在选择灾备供应商或产品时，建立统一、规范的灾备服务质量评价标准。

4.3.1 功能性要求

灾备产品应该能够为用户提供适应基本的、通用的数据保护和业务连续性等功能要求，有相应的容灾备份技术、模式、策略供选择，支持通用的备份对象和备份平台，具有满足对备份数据和容灾系统管理的功能等。如：

- ①运行平台支持；
- ②存储模式支持；
- ③系统管理功能；
- ④定制化支持；
- ⑤管理权限支持；
- ⑥中文 / 外文化支持等；
- ⑦可视化智能监控支持；
- ⑧备份对象、介质、模式支持；
- ⑨恢复演练、投资保护支持。

4.3.2 可靠性要求

根据灾备产品可靠性结构、寿命类型和各单元的可靠性试验信息，利用概率统计方法，评估出产品的可靠性特征量。评估其是否能在规定的时间内以及规定的环境条件下，完成规定功能的能力。可靠性要求是产品安全、稳定使用的基础，灾备产品是以程序运行为主的 IT 软件，可靠性是确保当故

障发生时，灾备产品能够立即发挥功能，将用户的损失降到最低。评价标准包括以下内容：

- ①是否有相关的资质认证；
- ②是否达到实际的使用效果；
- ③是否持续的运行不出现问题；
- ④是否有技术支持服务、快速响应能力等。

4.3.3 性能效率要求

灾备产品应该具备满足用户对数据在物理机、虚拟机、云平台、中间件及各种数据库等IT架构上的容灾备份方面的性能要求，包括时间、容量、耗能、用户指标等。介质包括产品性能效率、网络效率等。如：

- ①支持尽可能少对生产端性能产生开销；
- ②支持多租户的同时接入复制备份和恢复；
- ③RPO、RTO、APIT（任意时间点回退）值尽可能地小。

4.3.4 信息安全要求

灾备软硬件产品应该具备满足国家机构及用户对数据及系统在容灾备份方面的信息安全要求，包括安全功能和安全保证，并取得相应的资质等。如：

- ①安全审计；
- ②配置管理安全；
- ③用户数据保护安全；
- ④身份鉴别和访问控制安全；
- ⑤软件著作权、软件产品证书、3C认证、涉密认证等。

4.3.5 易用性要求

灾备产品应该尽量简单易用，简化运行维护操作过程，提高用户体验。应符合易理解性、易学习性、易操作性、吸引性。如：

- ①完备的产品指导手册；
- ②易于查询的在线帮助功能；

- ③有效性检查输入数据功能或能力；
- ④产品的窗口和界面应符合普通用户习惯且布局合理；
- ⑤产品的界面、图形、文字、信息和标识应易于识别和理解。

第五章 重点行业灾备建设特点及方案分析

单纯从技术需求分析，用户对于灾备的需求无外乎数据的备份、恢复、迁移以及业务的高可用等，但是具体到行业应用场景，可能会因为每个行业的特性而出现不同的解决方案，如医疗行业大量的非结构化数据的灾备需求，公检法海量卷宗类小文件 NAS 存储架构下的异地灾备需求等。因此，根据不同的行业，灾备规划建设解决方案也应有所差别。

中国国家统计局所遵循的国民经济行业分类与代码中列出了 A 至 T 行业分类，面向不同业务环节、不同业务内容这些行业都有若干解决方案。本章节从当前灾备建设比较热的行业的现状分析，从中引出对应的灾备业务相关方案并加以讨论。表 5.1-1 是灾备重点行业涉及领域。

行业	内 容
政府组织	各级政府部门及各种组织机构，如检察院、公安厅、法院、消防局、交通、工商、税务、质量监督、海关、政务中心等。
金融	指经营金融商品的特殊行业，包括银行、保险、信托、证券、会计、审核及相关设备制造商、系统集成商。
医疗	指与人们身心健康相关的所有产业的统称，包含了传统意义上的医疗、保健、养生等产业。
教育	学校、培训机构、教育管理部门、科研院所以及一些教育设备、服务供应商。
制造	指将资源（物料、能源、设备、工具、资金、技术、信息和人力等）进行制造，并转化为可供人们使用和利用的大型工具、工业品与生活消费产品的行业。
电信	包括经营电话、电报、移动通信、无线寻呼、数据传输、图文传真、卫星通信等电信业务和电信传输活动（如服务、微波总站系统单位等）。
互联网	包括移动互联网、物联网等万物互联技术及业务等参与者。
电力	包括国家电网（SERC）系统划分的发电、输电、供电等环节。

表 5.1-1 灾备重点行业涉及领域

5.1 政府及组织灾备建设特点及方案分析

5.1.1 行业概览

电子政务是把现代信息和通信技术引入政府机构，将管理和服务通过网络技术进行集成，在互联网上实现政府组织结构和办公流程的优化重组，创建一个虚拟的政府办公环境，以实现政府政务流程智能为目标的信息系统。随着政府信息化建设进入高速发展阶段，信息系统数据中心资源的整合正在不断加强，各级政府信息化建设的步伐也明显加快，据统计，中央和省级政务部门主要业务电子政务覆盖率已经达到 70%。

近年来，地方政府及组织电子政务建设普遍开展，组织体系不断健全，专业技术队伍建设不断加强。推动政府及组织电子政务发展的政策、制度和标准规范正在完善，许多地方制定了相关法规。围绕经济和社会发展的需要，电子政务应用深入推进，富有成效的典型应用服务不断涌现。

5.1.2 需求与解决方案

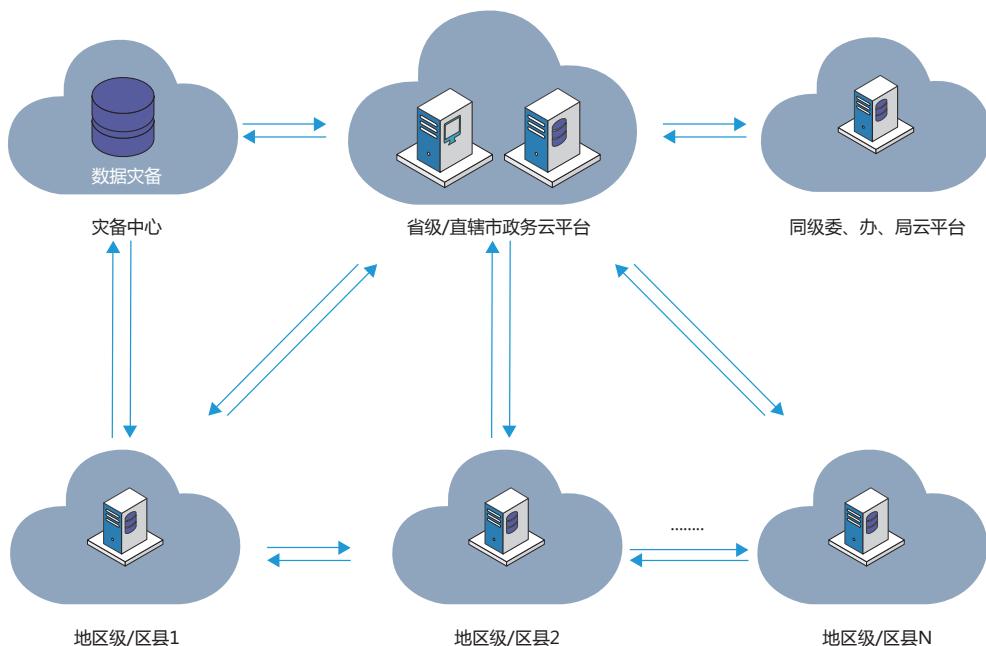


图 5.1-1 电子政务容灾拓扑图

针对电子政务建设的总体目标，需要从政府行业电子政务长远发展的角度考虑，采用云计算技术以及大数据技术的架构理念进行统筹规划，电子政务云的总体建设规划蓝图如下：

1) 构建统一、完善的电子政务云平台

在省级（直辖市）建设大数据中心和统一的政府及组织电子政务云平台，将电子政务基础架构、电子政务应用开发及运行、虚拟化桌面管理、电子政务数据集成和交换等多个服务予以整合。

地市级（区县）也有政府及组织电子政务信息化的需要，在建设省级（直辖市）整体政府及组织电子政务云平台的时候，需要考虑吸纳与整合地市级（区县）的政府及组织电子政务云平台，逐步将其现有的政务应用迁移到统一的云平台上来。从部署角度而言，可以建设地市级（区县）的政务数据中心，但从云平台整体管理角度而言，需要实现全省（直辖市）的统一运维监控。在条件允许的情况下，也可以直接将地市级（区县）的政府及组织电子政务应用和数据直接部署在省级（直辖市）的大数据中心里面。无论是部署在省级（直辖市），还是部署在地市级（区县），从技术上来看，需要将核心业务应用进行两地数据中心之间迁移。

2) 实现与委办局政务云平台的协作

在一些省级（直辖市）组织，各委办局不具备比较强的信息化管理能力，同时也没有独立的数据中心，可以将其所有的政府及组织电子政务应用部署在统一的省级（直辖市）政府及组织电子政务云平台上，委办局的相关办事人员需要通过政务专网访问相应的政务服务和数据。另外一些委办局具备具有独立管理的数据中心，也要充分考虑到与各个委办局的电子政务云（数据中心）之间的互连互通。

3) 建立安全可靠的灾备中心

在全省（直辖市）范围内实现政府及组织电子政务云平台之后，需要考虑到本地数据中心内部出现异常故障状况和重大灾难的时候，做好业务核心

应用和业务核心数据的灾备保护工作。实现方式有很多种，同城或异地的主备数据中心、双活数据中心、两地三中心等方案，不仅将省级（直辖市）的政府及组织电子政务云平台进行容灾备份保护，各个地市级（区县）也需要进行业务系统以及数据的容灾备份保护。

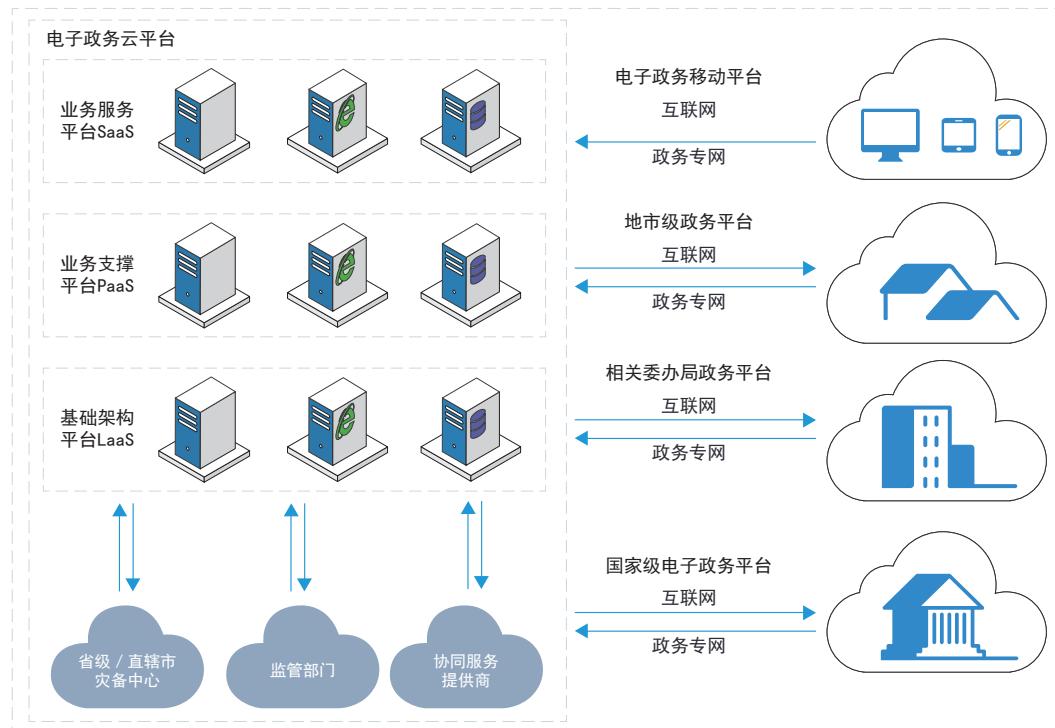


图 5.1-2 政府及组织电子政务云整体架构

电子政务云的架构规划和设计应遵从云计算的相关标准设计模式，电子政务云应包括基础架构平台 IaaS、应用支撑平台 PaaS 和业务服务平台 SaaS 三个层级的设计：

1. 基础架构平台

基础架构平台是整体电子政务云架构的一个关键平台，需要支撑顶层业务应用系统稳定运行、应用服务的资源弹性和调配能力都要依赖于此，更重要的是要满足平台的可靠性、可用性及可服务性的需求。在基础架构平台中，提供资源池服务、资源管理服务、运维管理服务、自主化流程管理服务、虚拟化桌面服务、安全防护服务、计费管理等。

2. 应用支撑平台

应用支撑平台提供电子政务应用的开发与运行服务以及数据管理服务等。在应用开发与运行服务方面，提供了基于云计算标准和技术的开发框架、应用支撑中间件、消息引擎、应用监控及自动化部署管理等服务。在数据管理方面，提供数据库统一管理平台、分布式内存数据运算及分析平台等。

3. 业务服务平台

业务服务平台以统一访问的应用方式支撑着多种多样的电子政务应用，包括了政府门户网站群、办公自动化、行政审批、电子监察、信访管理、电子邮件及视频会议管理等。用户可以通过多种终端设备访问和使用，例如像移动电话、Pad 等移动设备。

4. 多部门上下级的业务协作

电子政务云平台不是孤立存在的，需要与上下级或平级委办局之间在业务应用和盐雾箱数据层面有着良好的互联互通，甚至可以做到相互之间资源共享。

省检察院案例

在国家检察行政体系中，省检察院负责地方各级人民检察院和专门人民检察院依法履行法律监督职能，保证国家法律的统一和正确实施。因此，很多地方的省检察院往往也是县市级检察院的业务数据存储与管理的统一机构，如果省检察院的数据文件丢失，将会给案件的进程带来严重的影响，因此检察院的容灾等级非常高，很多地方不仅设置同城双数据中心的容灾模式，还会在异地进行两地三中心的建设。

该省检察院在经过前期的灾备环境调研后，提出了四个需求：一是保密需求。检察院属于国家涉密行业，其信息化发展过程中应确保数据 100% 安全。伴随着检察信息成为检察发展的重要战略资源，“信息获取、使用和控制”已成为了检察信息化发展和完善的核心。根据国家保密局涉密信息系统的管理制度 BMB17、BMB20 等规范，确保物理安全、运行安全、信息安全

保密，特别对备份与恢复有明确的规定。因此要求备份和灾备方案实施厂商应有涉密信息系统产品检测等相关行业资质。二是数据实时备份需求。数据实时备份即将检察应用系统的数据实时备份到本地，再由本地的灾备机实时将业务数据备份至异地，通过较低的成本实现对数据实现实时备份保护，数据备份后，可以随时按需要恢复到任意源端或异地的服务器上。三是应用级集容灾保护需求（业务高可用）。当工作机异常或者宕机时，由本地的备用服务器接管应用，对外提供服务，实现应用级的快速恢复。如果本地工作机以及灾备机均出现问题，由异地备份机器接管服务，保证业务的连续性。四是实现应用级一对一云灾备，即将每个工作机都对应到云灾备系统的一台服务器上。能快速地实现应用级切换，可将 RTO 缩短到秒级。

通过对省检察院当前系统状态的分析以及对应用未来的发展与安全的分析，特提出构建一套应用级高可用灾备系统并结合英方自身的 CDP 功能实现应用级与实时数据级的双重保护。分阶段实现全部核心业务系统应用级别的容灾，即核心系统 RTO 和 RPO 都接近于 0 的远期目标。

本地应用高可用与数据持续保护实现方式与过程在本地数据中心的核心电子印章系统部署一套 i2Availability 软件（主备机均需要部署），同时进行软件配置，首先同步两端的业务数据，而后对于主核心业务系统的业务 IP 进行实时监控，制定高可用切换配置规则。在部署了 i2Availability 的机器上开启 i2CDP 功能（此功能需要目标端一定的数据容量存储空间），对于源端写入的字节级 IO 数据进行实时捕获并做有序地传输，i2CDP 可以精确到百万分之一秒的记录与恢复粒度，大大地减少了由于逻辑错误、误删除导致的数据丢失，同时也将数据丢失量较少到最小（约等于 0）。

异地灾备实现方式：在异地容灾数据中心部署一台容灾服务器，同时将本地数据中心核心应用系统数据同步到异地容灾数据中心服务器上，整个同步过程首先是全量镜像同步，后续均为字节级增量方式实现，同时在容灾服务器也可以配置相应的应用程序参数，在本地数据中心服务器发生了灾难之

时，可以快速地将应用系统在异地容灾数据中心启动。

异地云灾备实现方式与过程：为了更好的满足用户未来云平台的部署，可以选择在异地采用云平台的方式构建其异地灾备环境，通过英方软件无缝融合云平台的资源，实现资源共享，成本低廉、部署迅速、灵活弹性的远程灾备服务，在对数据安全性进行严格管理的同时，实现对数据、应用提供最大高可用保证。首先在本地服务中心与本地灾备数据中心之间建立应用高可用保护，数据通过实时同步传输至本地灾备数据中心，然后在本地灾备数据中心与云平台建立云灾备保护，通过在云平台上部署的虚拟机建立对本地灾备数据中心灾备服务器的一对一式的保护，当本地灾备数据中心出现服务器故障或者数据丢失时，可快速从云平台将数据恢复，同时云平台也可将数据恢复至本地服务中心。

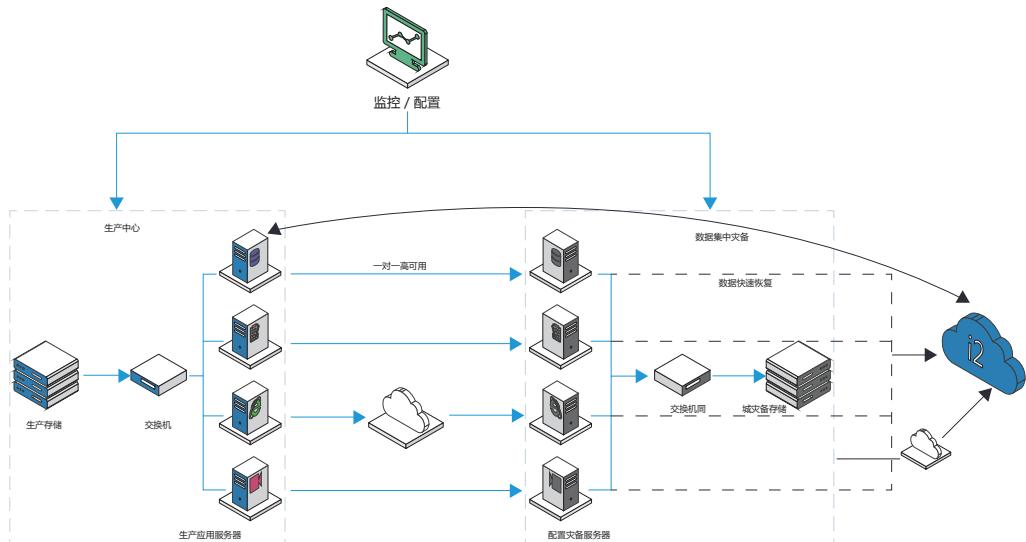


图 5.1-3 业务系统容灾备份架构

本地灾备一体机与未来扩展：本地的灾备服务器可选择一台 i2BOX 容灾备份一体机。它集英方容灾备份产品平台和物理硬件于一体，提供一体化的业务容灾和数据备份保护，通过先进的字节级增量数据同步及持续数据保护技术，以及先进的应用层高可用切换技术，帮助用户快速地将服务应用无缝动态地切换到应急中心，实现业务连续性。内嵌的 CDP 技术可实现任意

历史时间点状态回溯；英方软件结合虚拟化技术实现应用层一对一的高可用保护。i2BOX 容灾备份一体机可以无缝连接业内各个著名 IaaS 平台，提供了稳定、高性能、大容量、弹性扩展的终端硬件基础，为客户提供了使用方便灵活、维护简单、经济实惠的一体式容灾 / 高可用 / 云灾备体验。同时未来可根据用户需求，将异地灾备迁移至云端，i2BOX 一体机很好的结合各个 IaaS 平台，方便用户选择所需要的云平台，将数据存储至云端，快速方便的实现云灾备。

整个解决方案既提升业务数据和业务系统的安全性与可靠性，又能通过无缝融合的云平台资源，实现成本低廉、部署迅速、灵活弹性的远程灾备服务，并且创新地引入云灾备建立“两地三中心”的模式，为当前很多省检察院花费巨资建设两地三中心容灾工程给出了新的启示。

智慧城市之智慧政务云灾备案例

数字互联网城市（智慧城市）—智慧政务云项目以建设集约、高效、便捷、智能新型政府为目标，依托云计算、大数据、移动互联网等技术，提高政府办公、服务、监管、决策四个领域的智能化水平。某市建立智慧政务展示中心、智慧城市建设样板示范基地、兄弟城市和友好城市交流的先进平台、市民体验智慧政务好处的体验中心、政府各机关交流智慧政务经验的学习基地，将市政务云平台打造成为国内领先的“智慧政务示范与体验中心”。

“电子政务云”通过云计算的技术嫁接，在垂直方向上升华专业领域内政务应用软件，在水平的方向上打造一个统一的平台，并优化政务系统的运营方式，使政府部门之间办公和对社会、企业的服务能够加快，提高效率。通过云计算统一资源管理，为智慧的应用提供基础平台，建立“应用商店”整合应用，并改变运营方式，提供数据共享和交互服务以实现跨部门分析，将软件供应商迁移应用到云端，IT 服务商利用云平台打造更多智慧应用。这一切，需要一个安全稳定的云灾备平台确保各单位的公文系统及网站的安全与业务连续性。

经过前期的环境调研，英方将容灾客户端安装在相关主备服务器上，利用 i2CDP 与 i2BOX 等优势产品主要针对各类数据文件，如 Domino 数据库等提供持续的、不间断的保护，并可根据需求将数据快速恢复到之前的任意时间点。i2CDP 再将变化的数据实时复制到灾备中心，同时也将数据的任何变化以日志方式记录下来，实现对数据变化的可回溯性查询。

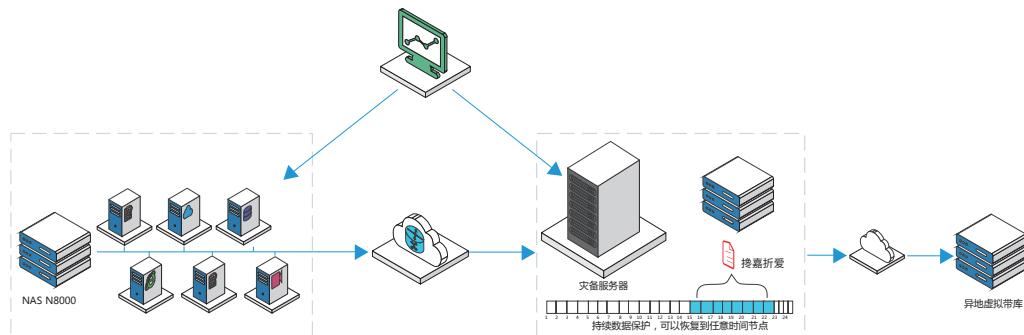


图 5.1-4 业务系统持续数据保护架构

在实施过程中，i2CDP 将办公系统的重要数据集中实时备份到云灾备中心，并由云灾备中心复制到异地的虚拟带库中，实现对数据的两地三中心保护，且无物理距离限制。

5.1.3 行业趋势

2016 年 4 月，国家领导人在网络安全和信息化工作座谈会上强调，关键信息基础设施安全保障体系的构建需要进一步加快。按照相关政策的进一步部署和要求，未来各级政府组织需要跟踪信息网络技术发展趋势，建成并不断完善适应机关政府电子政务应用需要的资源共享技术支撑体系即电子政务云；加强统筹整合解决因部门分散建设信息化所造成的系统问题；推进跨部门信息交换共享，基本建成政府监管和服务所需基础信息共享数据库；推进跨部门业务协同，加快网络环境下一体化政府建设进程；大力拓展和深化电子政务应用，推动政务模式创新，进一步畅通民意渠道、深化政务公开、强化行政监督、规范行政行为、优化政务流程、提升政府服务，推动电子政务向世界先进水平迈进。这些线上业务的安全运营，需要政府部门建立统一

的灾备体系，并结合云计算、大数据、人工智能等前沿科技实现业务的安全、高效运行。

5.2 金融行业灾备建设特点及方案分析

5.2.1 行业概览

金融业是指经营金融商品的特殊行业，它包括银行业、保险业、信托业、证券业和租赁业。金融业具有指标性、垄断性、高风险性、效益依赖性和高负债经营性的特点。我国的金融监管部门可以简称为“一行三会”，即中国人民银行、中国银行业监督管理委员会、中国证券监督管理委员会和中国保险监督管理委员会。当银行、证券、保险等机构发生包括系统运行的安全事故时，会由上级管理机构进行通报、警告和惩罚。

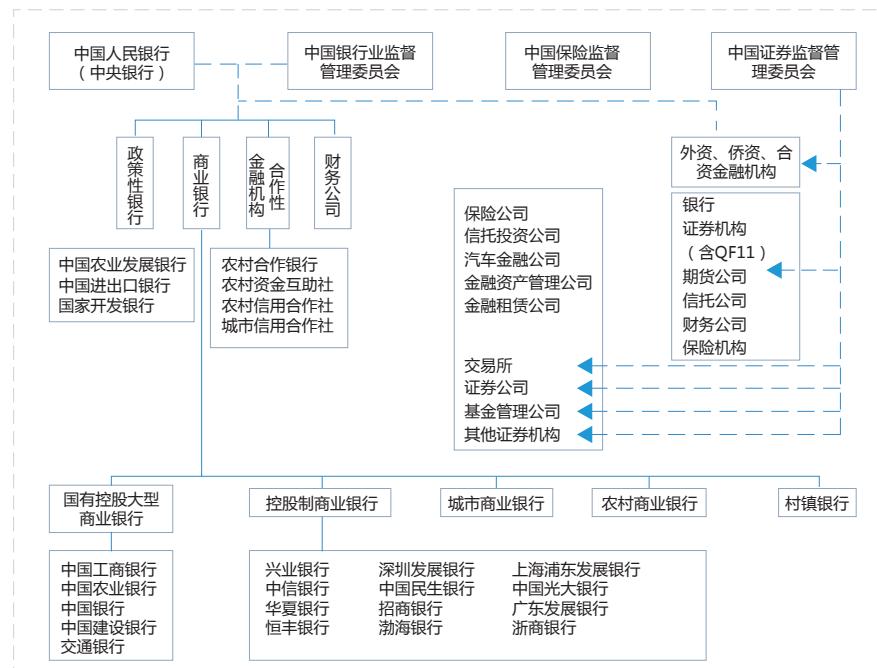


图 5.2-1 中国金融体系统结构

金融行业特征之一是信息化程度非常高，涉及的数据庞杂，对信息系统依赖性极高，所以金融机构的信息系统安全与业务连续性遭受网络攻击、人为误操作、自然灾害的挑战越来越大。互联网金融业务的快速普及与高频交

易使得 IT 系统长期超负荷运载，而金融机构能够预留的停机时间窗口却在减少，如何保障金融业务、办公、财务、管理等信息系统的安全高效运行，不仅要选择适合自身生产环境的技术方案，还要考虑不同信息系统采用不同灾备方案，以达到 TCO 的最优化。例如核心业务系统采用热备方式，非核心系统采用冷备模式。

金融行业另一个特征是对安全性要求也非常高，对于银行、证券等机构，都要求严格按照等保要求规划建设灾备中心。2011 年银监会就出台了 BCM 监管指引，对商业银行的 RTO 和 RPO 提出了明确的量化指标。根据业务重要程度实现差异化管理，确定各业务恢复优先顺序和恢复指标。商业银行应当至少每三年开展一次全面业务影响分析。商业银行应当识别重要业务，明确重要业务归口管理部门、所需关键资源及对应的信息系统，识别重要业务的相互依赖关系，分析、评估各项重要业务在运营中断事件发生时可能造成的经济损失和非经济损失。原则上，重要业务恢复时间目标不得大于 4 小时，重要业务恢复点目标不得大于半小时。

单位	政策文件
银监会	2006.08 《银行业金融机构信息系统风险管理指引》 [2006]
	2008.04 《银行业重要信息系统突发事件应急管理规范（试行）》 [2008]
	2009.04 《商业银行信息科技风险管理指引》
	2010.04 《商业银行数据中心监管指引》 [2010]
	2011.12 《银行业务连续性监控指引》 [2011]
人民银行	2006.4 《关于进一步加强银行业金融机构信息安全保障工作的指导意见》 [2006]
	2008.02 《银行业信息系统灾难恢复管理规范》

表 5.2-1 银行业务连续性及灾难恢复的相关规定

与此同时，在国家相关规定出台时，金融机构也投入大量资源进行灾备中心建设，并在数据集中处理，应急管理，人员培养和灾备部署等诸多方面

取得了显著成绩。比如金融行业在上海、东莞、北京、广州等地都有灾备中心，灾备规模与建设力度全行业名列前茅。

金融领域由于对安全性要求非常高，因此灾备建设的各项要求也非常严格，任何系统宕机、网络攻击、停电等所导致的数据丢失与业务中断，都可能给用户带来严重的损失。为此，金融行业的灾备建设要求 RPO 与 RTO 尽可能地接近于 0，对灾备相关服务商的技术实力提出非常严苛的要求，要经过反复论证，技术对接，以及执行严格的验收流程等。

5.2.2 需求与解决方案

金融机构的灾备需求，会根据机构系统的重要程度划分，由于涉及的子系统太多，我们可以将其划分为业务系统和非业务系统。一般情况下，核心业务系统会采用热备模式，采用多活保证高可用，给予业务系统多重保障；非核心业务系统采用冷备模式，定时或实时备份数据，以及数据恢复和业务高可用切换接管等。对于灾备等级要求高的金融机构，也会需要远距离异地容灾、两地三中心等灾备模式。

银行业

银行核心业务系统、综合前置系统、后督和影像系统等应用的数据存储特性各有不同，关键数据除了高可用、容灾保护之外，银行核心系统业务持续运行要求不断提高。核心系统向 X86 平台迁移将成为趋势，因而提高 x86 平台的数据保护是重点之一。在数据生命周期的不同阶段，如何选择最佳业务系统的容灾备份方式，既能确保生产系统性能、可用性的同时，又能降低数据丢失的风险等压力；同时，备份系统如何适应备份数据的增长，备份数据能否快速、便捷的恢复都是金融机构面临的挑战。

银行核心应用双活 + 两地三中心方案

大型银行核心业务系统被视为以客户为中心的，关乎国家经济命脉要求数据的绝对安全、可靠，能抵御任何灾难风险。

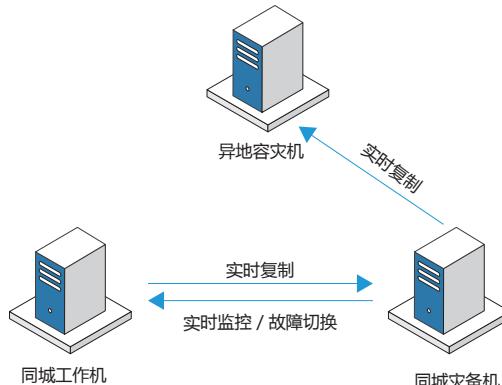
核心系统一般包括的模块：客户信息、额度控管、存款、贷款、资金业

务、国际结算、支付结算、总账、卡系统、对外接口等。

要求整个 IT 基础架构包括存储系统，有最高的可用性，保证 7*24 小时的连续性，保证客户对业务系统的随时访问。

要求支持“一键式”切换，系统能提供方便的快照备份数据保护，以保障关键的数据在逻辑错误及任何灾难发生时不会丢失。

两个同城生产中心支持实时同步工作即生产中心双活方案，异地生产中心可保证数据绝对安全可靠。



- 提供核心业务等本地高可用的切换及异地容灾的全面性安全保护
- 完全能支持保护单台服务器，物理机房，甚至区域性的容灾
- 提升产能并减少数据的丢失

图 5.2-2 银行核心应用双活 + 两地三中心

双活 + 两地三中心方案对银行的价值

稳定可靠的基础架构满足银行业日益增长的业务需求，可以更加快速灵活地动态支撑业务拓展；

更高的数据的安全性，确保数据完整、可用；防范运行风险，实现服务能力的高可用性；

建设同城备份中心和异地灾备中心，增加安全性。提升客户体验感和满意度，为现代化银行打下坚实的 IT 信息化基石。

银行次核心应用，采用主备模式，核心和非核心的应用采用实时性和定时结合的备份策略对数据从不同维度进行保护。

针对金融行业细分领域对安全等级的不同，以及不同客户生产环境存在的差异化，灾备解决方案也会有所不同，下面列举部分灾备方案系统，供参考。

1) 两地三中心及异地多活模式

两地三中心是指数据中心 A 和数据中心 B 在同城作为生产级的机房，当用户访问的时候随机访问到数据中心 A 或 B (A 和 B 会同步做数据复制，两边的数据完全一样)。但由于是同步复制，所以两个数据中心的距离不能太远（小于 60km），否则同步复制的延时会比较长。

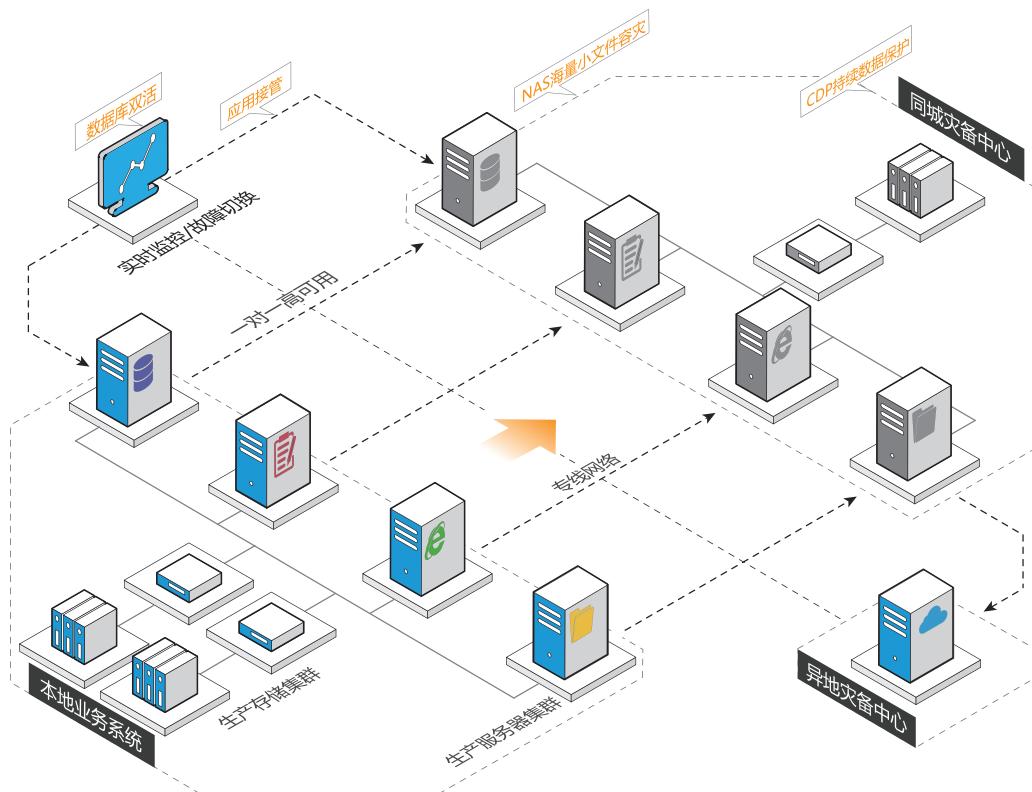


图 5.2-3 两地三中心拓扑图

异地备份数据中心通过异步数据复制来实现，银行两地三中心的特点是异地备份数据中心一般不作为关键应用宿主地，某些情况下是完全冷备，有些机构的做法是将统计分析和非关键的内部管理系统放到灾备机房。对于关键业务应用异地灾备中心不对外服务，所以用户不会访问到异地节点。原因

是因为数据从生产级数据中心到异地的节点是异步去复制，所以整个有延时。

另外一种模式为异地多活模式，也是目前正在兴起的一种模式，对于某些大型银行的核心关键应用已经在此模式下进行了成功验证。异地多活首先是要做到同城双活或者同城多活，就是数据在同城网络环境下进行高速备份，也可以在做楼宇级同步，一般在 10ms 类的数据差异。异地多活需要多个跨地域的数据中心，距离需要达到 1000 公里以上。

2) 同城交易系统灾备系统模式

同城交易系统为某些金融机构重要的业务系统，多采用 Window+MSSQL 结构。在数据量变化方面，场景变化可以设为总容量约 500G，每天增量 30G 左右，同时清算操作会删减近 20G。

同城交易系统目前多采用冷备系统，即灾备机日常处于冷备的状态，当程序运行所在机器发生故障后，通过另外一台机器人工操作重开报盘程序的方式完成故障切换，从而重新对外服务。此方案故障切换完全依赖手工，增加了切换过程中人为失误的风险，如果能实现全自动切换则能大大减少 RTO、RPO 值。

i2Availability 是一种自动切换的灾备解决方案，它提供针对多种应用、任何距离内的高可用性服务。即当生产系统出现异常时，它将生产系统上的应用按需自动切换到灾备服务器上，实现应用级快速切换，减少服务的中止时间，保持业务应用的高度可用性。整个过程中不会出现停机切换，做到应用连接不中断，应用数据不丢失。

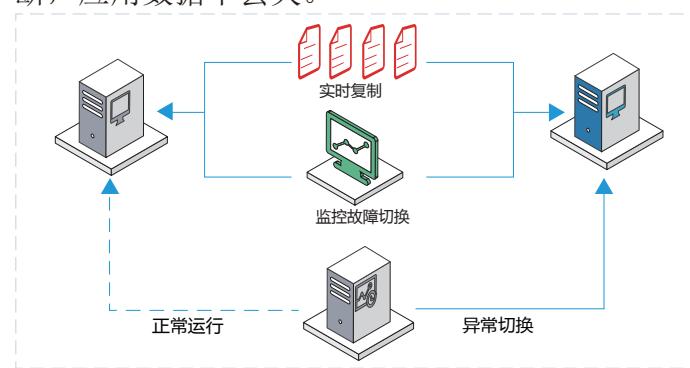


图 5.2-4 i2Availability 工作示意图

证券业

证券自营资管系统两地三中心方案

自营资管系统为证券行业一个关键应用，常用为 Window+MSSQL 或者 Linux+Oracle，用户通过灾备技术方案进行应用保护，可以实现异地机房数据库的远距离实时同步和两地三中心的灾备保护。

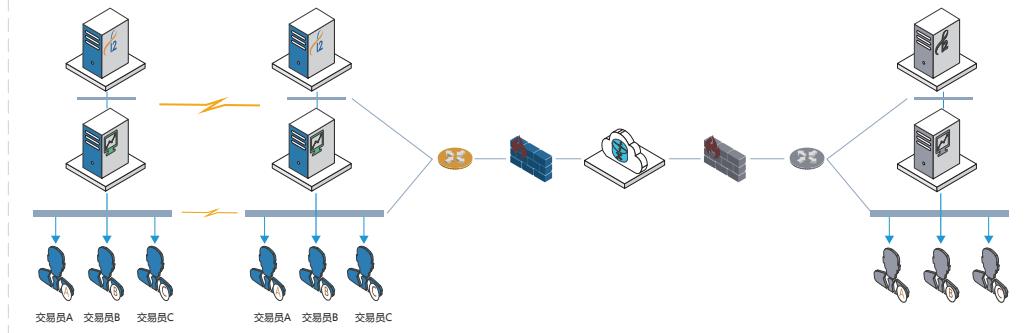


图 5.2-5 证券系统两地三中心容灾方案

证券行业细分方案汇总

融资融券系统

数据的实时复制：秒级内同步到备端的数据库；

应用的高可用：异常时在秒级以内将数据库切换到备机数据库，并提供对外服务；

多点数据容灾：提供同 LAN 以及同城异地数据容灾；

如果当前数据库损坏，可以将数据库恢复至某一历史状态，确保数据一致性后再启动，然后对外提供服务。

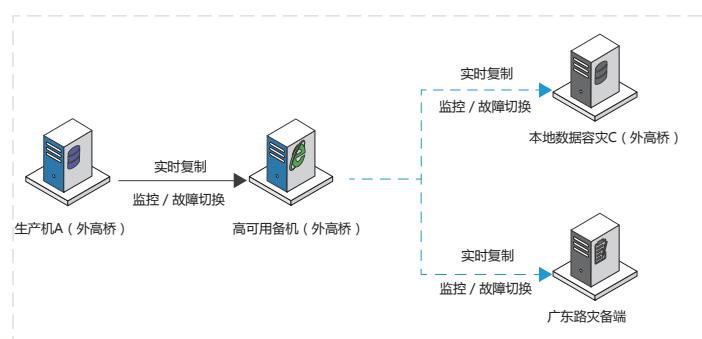


图 5.2-6 融资融券系统容灾方案

PB 投资系统——本地高可用，历史数据保护

数据的实时复制：生产端的数据更新秒级内同步到备端的数据库；

应用的高可用：生产端宕机或异常时可在分钟以内将数据库切换到备机数据库，并提供对外服务；

如果当前数据库损坏，可以将数据库恢复至某一历史状态，确保数据一致性后再启动，然后对外提供服务。

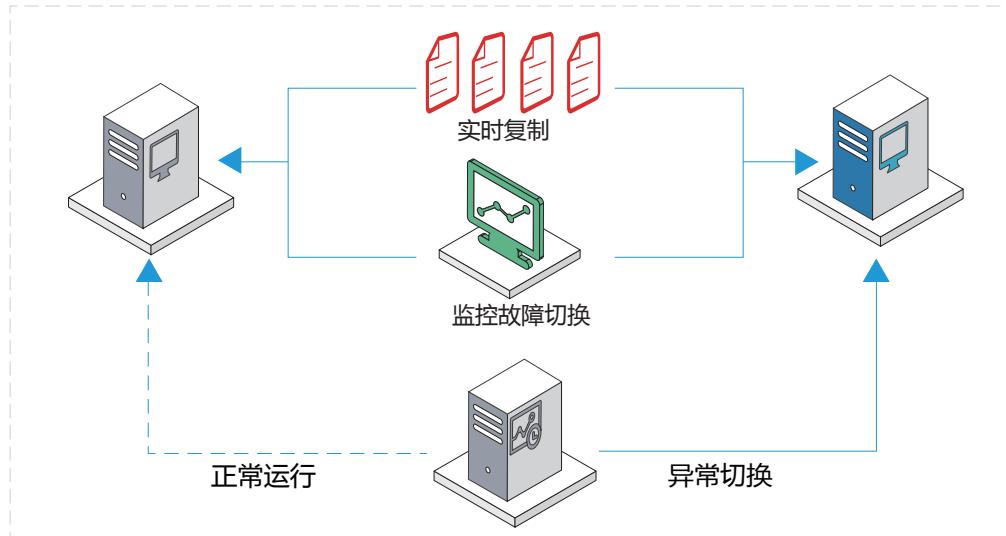


图 5.2-7 PB 投资系统容灾方案

证券资产管理系统——同城高可用，异地灾备

图形化管理：管理及监控方便，

数据的实时复制：生产端的数据更新秒级内同步到备端的数据库；

应用的高可用：生产端宕机或异常时可在分钟以内将数据库切换到备机数据库，并提供对外服务；

方便的管理：可通过短信及邮件发送告警信息。

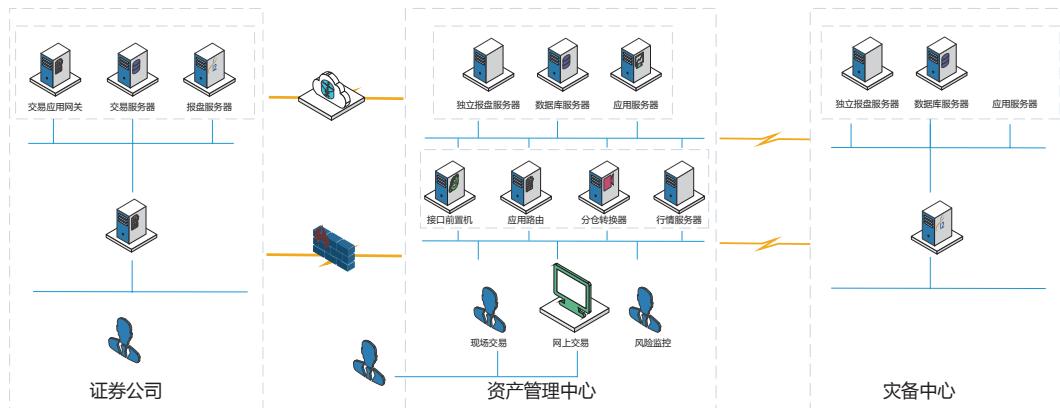


图 5.2-8 同城高可用, 异地灾备方案

自营系统——同城高可用, 异地灾备

异地机房数据库的远距离实时同步，（两地三中心，A-B-C模式）；
 数据的实时复制：生产端的数据更新秒级内同步到备端的数据库；
 应用的高可用：生产端宕机或异常时可在分钟以内将数据库切换到备机
 数据库，并提供对外服务；
 方便的管理：可通过短信及邮件发告警信息。

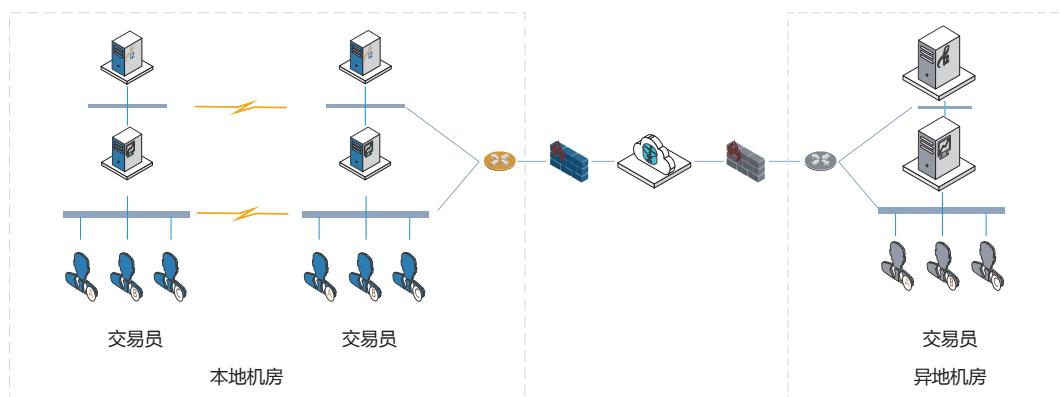


图 5.2-9 同城高可用, 异地灾备方案

个股期权报盘口库——同城高可用, 异地灾备

数据库应用高可用：客户的数据在写入生产端数据库的同时，在秒级内
 同步到本地灾备端的数据库，并且可以在分钟以内
 将数据库切换到备机数据库，并提供对外服务；

远距离实时同步：异地机房数据库的远距离机房实时同步（两地三中心）

同城三机房机房，上海机房 - 深圳机房，A-B-C 模式；

带宽低占用：对网络传输压力小，适应远距离窄带传输；

方便的管理：可通过短信及邮件发告警信息。

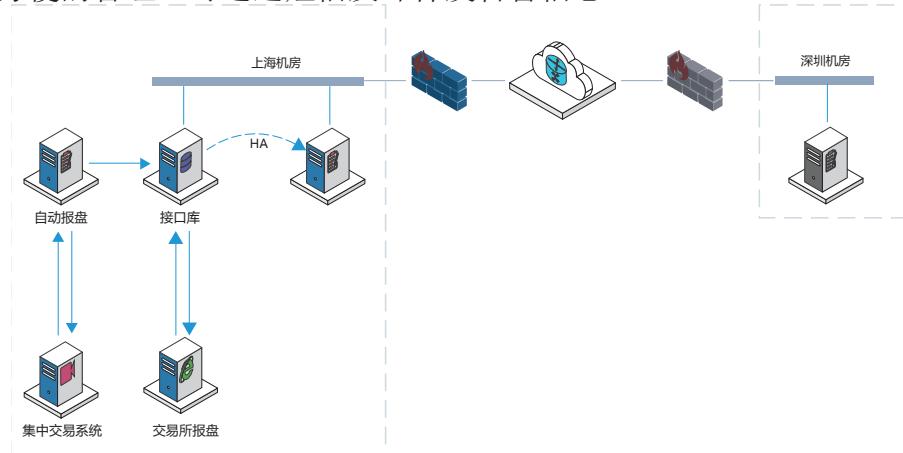


图 5.2-10 同城高可用，异地灾备方案

报盘系统——同城高可用，历史数据保护

数据的实时复制：生产端的数据更新秒级内同步到备端的数据库；

应用的高可用：生产端宕机或异常时可在分钟以内将数据库切换到备机数据库，并提供对外服务；

如果当前数据库损坏，可以将数据库恢复至某一历史状态，确保数据一致性后再启动，然后对外提供服务。

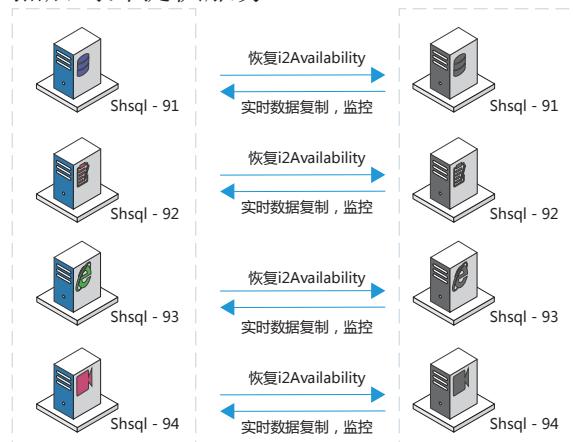


图 5.2-11 同城高可用，历史数据保护方案

影像系统——数据实时同步，异地数据容灾

影像文件实时同步：客户的纸质凭证转换成电子凭证图像时，从各分支机构获得的各类文件（影像文件、电子文档）上传至本系统服务器，在秒级内同步到本地灾备端的文件服务器；

出色的扩展性：未来可平滑扩展到异地灾备模式；

方便的管理：可通过短信及邮件发告警信息。

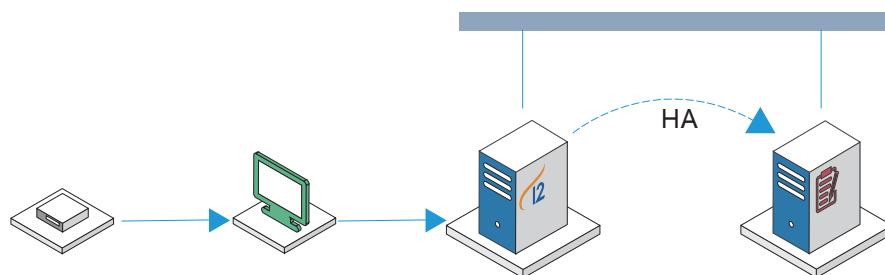


图 5.2-12 数据实时同步，异地数据容灾方案

行情分发系统

证券行业的实时分发系统实时性要求很高，往往一点点的延迟就用户的体验造成极大的影响，一般传统的灾备软件在数据变化频繁，数据量大的情况下实时性就会极大的下降。

数据的实时复制：源端数据系统在接收到交易中心的数据的同时，在毫秒级内同步到各个营业厅的客户端系统；

恢复历史数据：如果当前最新数据损坏，可以将数据恢复到损坏之前的正确状态。

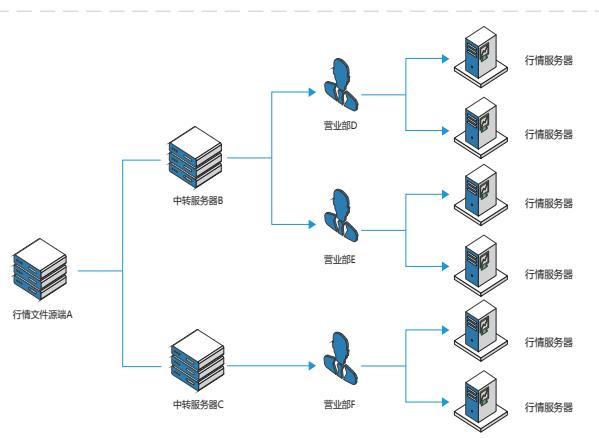


图 5.2-13 行情分发系统模式

5.2.3 行业趋势

未来几年，中国金融行业的灾备建设需求将增加，灾备模式将呈现多样化、低成本化，主要趋势如下：

1) 中小金融机构灾备需求增长明显

中小银行，即城市商业银行、区域性银行，在新一轮做强、做大、向全国性银行扩张的过程中，面临的运营风险、操作风险进一步加剧。因此，他们深刻意识到灾备建设对于持续运营业务，提升抗风险的能力，再造竞争优势的推动作用。在保险、证券等行业也具有相同趋势，越来越多的中小保险公司、证券公司、基金公司开始进行灾备体系建设。实时数据复制、异地高可用业务接管、行情分发与数据恢复会成为金融用户的主要灾备需求，并最终以降低 RPO 与 RTO 值作为参考。

2) 灾备范围进一步扩大

虽然我们看到越来越多的金融企业已经进行灾备预案体系建设，但是预案数量和备份系统范围非常有限（大多只是核心系统），其最终的灾难恢复能力也将是非常有限，一旦发生灾难，预案很有可能无法满足灾备需要。这种情况在一定程度上说明，中国金融企业的灾难恢复意识还不够强，投入的人力、财力、物力还不够多，这需要行业主管机构更多的指导和规范，更需要企业高层管理者进一步提高灾备管理意识和危机管理意识，进一步扩大备份 / 恢复范围，把核心系统之外的重要系统也逐步纳入备份范围，并进一步完善灾难恢复预案。

3) 灾备演练成为常态化

灾备演练能够最大限度地对灾难恢复及业务连续体系进行全面的检验，考验技术支持团队和各部门的协同处理能力，进一步完善灾难恢复体系，提升业务连续管理能力和应急管理能力。部分金融机构要求至少每三年对全部重要业务开展一次业务连续性计划演练，国内审计要求一般是每年至少一次。商业银行应当至少每年对业务连续性管理体系的完整性、合理性、有效性组

织一次自评估，或者委托第三方机构进行评估，并向高级管理层提交评估报告。对于交易所和登记结算公司还可能每季度要求全网参与机构进行一次切换演练。商业银行在完成业务连续性计划的全行性演练后，应当在 45 个工作日内向监管机构提交演练总结报告。

现在，大连银行、北京银行等一些灾备建设领先的金融机构已开始进行灾备系统的实战演练，有实战演练需求的企业也在迅速增加。实战演练正在成为一股流行趋势，被众多金融企业所接纳。

4) 混合云灾备更加频繁

基于安全性考虑，很多大型金融机构都有自己的私有云（行业云）。为了充分利用云计算的优势，越来越多的金融客户正在利用本地和私有云、公有云之间的异地数据中心的特点，构建混合云的灾备模式。这种模式不仅充分利用了云计算的优势，还能够将安全的主动权掌握在手中，同时有效地降低灾备建设的成本。

因为灾备通常采用主从架构，如果用户都使用私有云，相对建设和运维成本较高。在混合云的架构里，可以考虑把备用部分放在公有云上，用于在主服务宕机时，短时内保证服务的连续性。这种场景分两种情况：一些用户（通常是行业用户）会把核心应用放在私有云上，然后将非核心应用或者创新应用部署到公有云上；另外一些用户出于安全等原因，将业务数据放在私有云上，而将应用运行在公有云上。

5.3 医疗行业灾备建设特点及方案分析

5.3.1 行业概览

医疗行业的信息系统是一个数据量大、数据类型复杂和事务并发多的实时系统，由于医院业务的特殊性，任何人为或自然因素所导致的应用或中断，都会造成医院巨大的经济和声誉损失。因此，医院对 IT 系统的持续稳定，即业务持续性和系统稳定性提出了非常苛刻的要求。

根据国际统一划分，医疗信息化建设主要分为三个阶段：医院信息管理（HIS）阶段、临床信息管理（CIS）阶段和局域医疗卫生服务（GMIS）阶段。我国医院信息化建设的重点开始从以费用、管理为主的医院信息化初级阶段，逐步过渡到以医院临床信息为主的高级阶段。医院信息系统的开发和应用正在向深度发展，从早先的侧重于经济运行管理，逐步向临床应用、管理决策应用延伸，逐步实现“以收费为中心”向“以病人为中心”的数字化医院转变。

HIS 系统模块发展趋向完善，除提供收费、划价、门诊（住院）医生工作站、护士工作站、药房、药库管理、物资管理外，还引入一卡通、LIS、PACS（RIS）等常见系统，部署方式也多采用双机热备方式，有条件的医院开始部署独立的备份系统，如通过备份软件备份到磁带或者磁带库，做数据离线保存。部分医院引入多点群集、多数据中心、双活数据中心、虚拟化部署甚至云计算部署，部分应用也迁移或者部署到云端。

传统方式保护医院信息系统存在的问题

大多数医院采用双机热备技术来保证服务的持续运行。但传统的群集解决方案采用共享存储架构，存在单点故障风险，一旦磁盘阵列发生故障，则整个系统将停机；即使建设了多台磁盘阵列，由于缺乏远程或异地灾备的能力，仍然存在巨大风险。另外，部分用户还有一种片面的认识，认为只需要双机热备份却忽略数据备份的重要性，结果当磁盘阵列发生故障或人为误操作导致数据丢失时束手无策；即使做了额外的磁带备份，但受限于磁带恢复和还原数据的冗长时间，业务恢复时间过长。

5.3.2 需求与解决方案

医疗行业的灾备建设过程可以分为三个阶段：

第一阶段是单服务器数据备份——该阶段为原始阶段，通过数据库或者操作系统自带备份工具实现本地数据备份，或者手动导出备份，做到定时本地备份。

第二阶段是 HIS 等重要系统部署群集模式——对 HIS 等重要系统做出

MSCS、RAC 等群集配置，对服务器系统应用故障做 HA 策略，在本地机房实现了一定的业务连续性。备份多采用本地数据库或者操作系统备份，部分医院部署了独立的备份服务器，将数据定时备份到磁带或者磁带库。此种解决方案，数据恢复比较慢，且数据一致性校验困难。

第三阶段是重要系统异地备份——随着医院业务发展，多院区建设或者多数据中心建设，重要数据实现多副本保存成为常态，部分医院开始对重要数据进行异地备份，或者数据实时复制，高级别要求的医院开始部署异地群集。

简而言之，简单的数据备份或者数据集中备份已经不能满足医院信息化业务连续性要求，针对某一个具体的系统做业务连续性无法满足医院信息化连续性要求，必须从全局角度设计业务连续性方案。

1. 构建本地和云端的高可用架构

医院信息系统发展至今，已经成为医院基础建设的重要一环，核心系统如 HIS、EMR 等的业务连续性在大中型医院开始部署，异地容灾系统开始实施。医院多个业务系统之间关联性极强，对数据中心整体容灾成为当前医院管理者们需要解决的问题，是建设多院区之间的双活数据中心，还是容灾到虚拟私有云，甚至将业务部署到云端，都成为当前医院管理者们需要讨论的问题。

为保障业务系统的高可用，不仅利用云平台自身的漂移、快照等功能，还提供云灾备的解决方案，对关键业务实现系统和数据的容灾和备份。

某三甲医院从相关系统的重要性和严格性出发，通过灾备软件实现相关数据的保护，即利用服务器上的备份软件通过 IP 网络实现数据的远程云端复制。对数据及应用进行灾备保护，确保数据的实时保护以及应用的高可用性接管。

在此项目中，关键的应用 / 数据通过千 M 专线实时灾备到广州联通的五星机房中，实现对数据以及应用的实时灾备保护。通过将软件安装在相关

主备服务器，主要针对相关数据实施实时保护，在各自主备两台机器之间实现数据实时复制保护，异常时快速恢复相关数据。其中的生产服务器包含番禺和广州市区的数据中心的相关业务服务器，在其上均安装英方客户端软件，通过英方客户端软件对实时备份目录提供数据实时或定时容灾保护。当异常情况时，部署在广州联通云端的灾备系统即提供数据快速恢复服务，将数据快速恢复到选定的服务器（原机或新的服务器）上，并保证数据的可用性，无论番禺或者广州机房发生断电、系统异常等情形时，均能通过该灾备系统实现对数据的灾备保护。

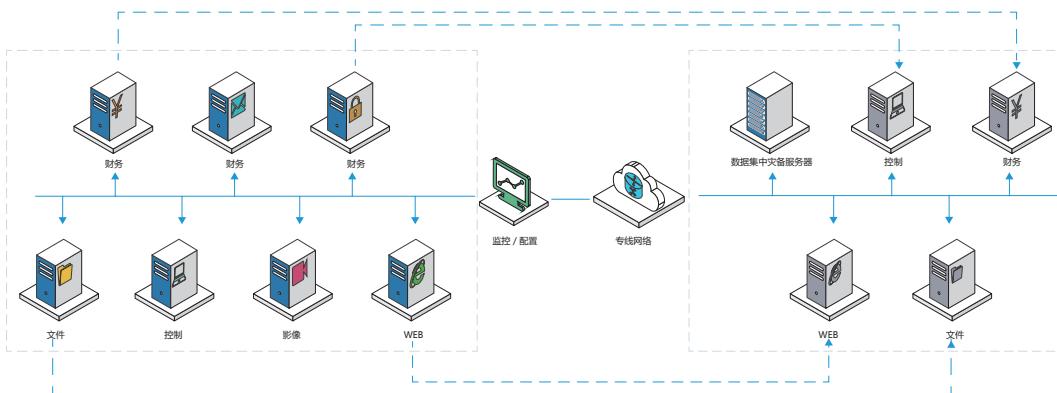


图 5.3-1 某三甲医院容灾拓扑图

2. 海量非结构化数据迁移至云端对象存储

医疗行业信息系统门类众多，包括 CIS 临床信息系统、HIS 医院信息系统、PACS 影像归档和通信系统、EMR 电子病历、PEIS 体检管理系统等。这些门类众多的系统所产生的数据特点不一，其中最明显的就是医院每天产生的海量的结构化与非结构化数据的存储方式的差别。

存储增长速度的统计显示：二级医院每天是十几 GB，几十 GB；大型三级医院每天是几百甚至是 TB 级增长速度。医疗行业的大数据时代，80% 就是来自于 PACS 的驱动力。为此，医院的信息科工程师会抱怨影像数据越来越多，而管理越来越复杂，而影像科医生是希望在分院区尽快地获取影像检测结果，不让患者等待太久的时间。

面向对象存储是一个不错的选择，优势在于与网络连接的设备不需要文件系统的介入（传统的 NAS 存储是基于文件系统的，面对海量文件时，存储容量和访问速度成为瓶颈），具有一定的智能自动管理其上的数据分布，它提供的性能是目前其他存储结构很难达到的，直接通过 URL 进行访问，访问速度快，并具有很好的可扩展性、安全性。

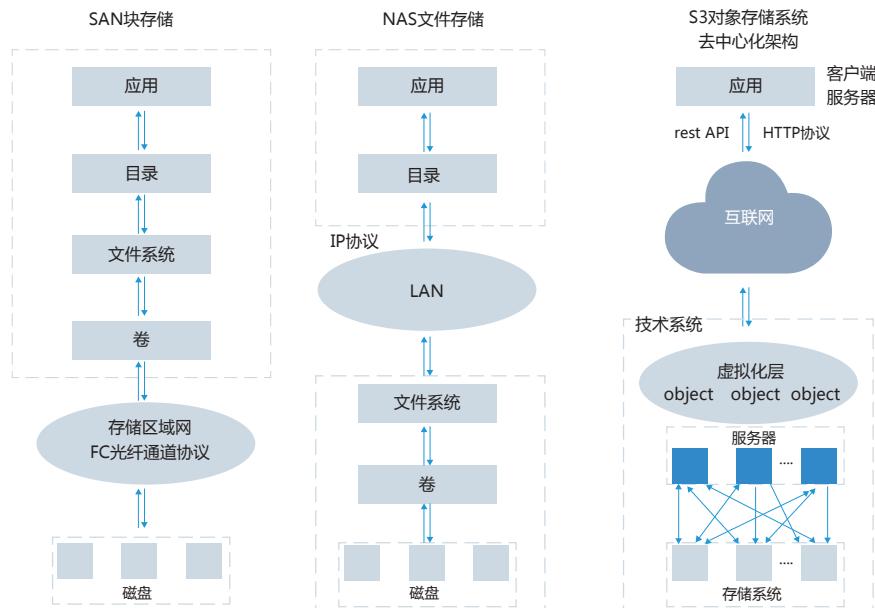


图 5.3-2 非结构化数据到对象存储的迁移

那么，如何将 PACS 影像归档和通信系统等数以万计的数据文件、业务系统迁移、灾备至云端，并且确保在迁移过程中业务如何不受影响，甚至运维管理、成本控制等后期工作能够顺利展开，其实这是要解决从传统的文件系统怎样迁移到**面向对象的存储系统**。

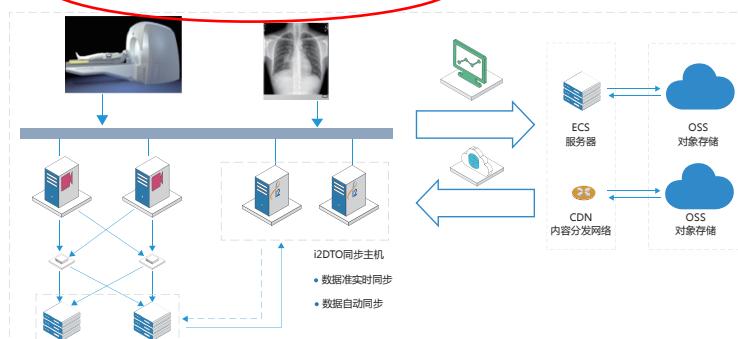


图 5.3-3 某三甲医院混合云存储实践

i2DTO（面向对象存储管理软件）适用于医疗行业 PACS 系统海量影像数据同步的应用场景，有多重保障机制。首先，支持数据的完整性校验，保证同步到云端的数据与本地是完整一致的；其次，目录结构的一致性，同步过程中严格将文档的目录层级完整继承到云端；最后，添加同步主机，主动向本地存储发起访问请求，对原来的业务生产系统无任何影响。

完整的 PACS 环境一般包含 PACS 和 RIS 部分，如 PACS/RIS 数据库服务器、影像服务器和中间件服务器。针对两种不同类型的数据采取不同策略做同步。

影像文件同步（非结构化数据）

影像文件具有三个显著特性：

①数据量大，动辄上亿的文件数量；在没有优化算法的情况下，读取的效率很难提升；

②文件琐碎，一个患者的影像文件在同一个文件夹下，一般都是分隔为多个文件来保存，且单个文件的占用空间都不大；文件的数量及单个目录下文件的完整性需要做到万无一失；

③文件目录层级结构与 RIS 数据库中的索引有对应关系，若打乱原有的目录结构。用户信息读取很容易出错。如何在数据全部同步的基础上，能够完整的继承本地目录结构是一个大难题。

i2DTO 软件轻松应对海量小文件，将影像图片同步到对象存储 OSS。同步机制分为以下 2 个过程：

第一步，存量数据传输。对于已经在本地保存的动辄几百 T 的影像文件，利用 i2DTO 直接与 OSS 提供的标准 S3 接口对接来做传输；

第二步，利用 i2DTO 产品实时增量备份的方式，将新增影像数据同步到 OSS 中。

在以上的同步过程中有三个至关重要的技术点，a. 数据的完整性；b. 同步后目录层级的严格一致性；c. 同步过程对原有生产系统的影响程度。

RIS 数据库同步（结构化数据）

针对 RIS 数据库，使用云端主机来同步本地的结构化数据。

通过多重机制保障 RIS 的内容高效的传输到云端 PACS 中：

字节级增量复制，可以将最小的传输单位细化到字节。能够以最小的资源高效的将数据实时同步到云主机；

作为医院核心业务系统，每天面临着包括误操作、误删除、系统感染病毒在内的一系列威胁。配置了持续数据保护后，可以按照用户需求将 RIS 数据库恢复到历史正常的状态。

5.3.3 行业趋势

2016 年政府工作报告提出“不断提高医疗卫生水平，打造健康中国”的目标，医疗行业的信息化也成为“十三五”期间国家发展的重点领域。《电子病历功能规范》、《电子病历应用等级评审标准》为代表的若干标准和规范的出台，为智能医疗和数字化医院提供了理论体系；医院影像设备的快速发展使放射科图像数据量激增，国家规定的医疗数据保留年限要求，给存储容量带来的挑战将日益增加，而数据需要备份容灾和异构存储环境的现状也越加突出，迫切需要更可靠、更高性能、更灵活的灾备系统来满足。

随着行业需求的提升、技术的发展及对信息安全的考量，容灾备份及业务连续性管理建设目标将至少包括几个方面：

1. 多副本数据需求，不论是同城容灾、异地灾备，或是云端灾备，数据零丢失是不变的主题；特别是数据上云后还要考虑云端主机到主机的数据灾备场景，不同云之间的数据灾备场景，甚至是云端到本地的数据恢复能力等；同时，要求具备持续数据保护的能力，以此规避误删除、误输入等误操作。

2. 信息系统 7*24 小时业务不间断要求，帮助用户一套连续性规划，使中断的威胁降到最低或消除中断威胁，充分考虑最关键需求的优先级，并将恢复时间降到最短。

3. 简单的容灾演练，优秀的方案必须结合高效的管理制度，实现容灾设

计目标。确定恢复业务所需要的关键人员、资源、行动、任务和数据。容灾系统需要处于开机阶段，当有访问需求时，可随时启动容灾业务端，同时一个暖启动状态的容灾系统，具备完善的，应用级别的数据一致性校验手段。

5.4 教育行业灾备建设特点及方案分析

5.4.1 行业概览

教育活动的参与者数量庞大，学生、教师、学校、管理者、政府、机构、企业，提供给这些参与者和所使用的信息系统都可称为教育行业的解决方案。

按照教育对象区分，教育行业大致分为：学前教育、基础教育、高等教育和职业教育等。专业培训机构在本文中我们将其归类为企业，在此不做赘述。不同教育对象关注的信息系统各有侧重，典型分布图如下：



图 5.4-1 不同教育对象对应关注的信息

学前教育指的是对学龄前儿童的培养。主要软件应用包括园区管理系统、多媒体教学系统、在线教学等。目前以上应用在十二五期间已经在幼教中逐步普及，由其信息化发展的状况来看，学前教育对数据安全及保护的要求将日益增高，未来市场的需求也会逐渐增大。

学历教育主要分为基础教育和高等教育。根据十二五教育行业信息化发展要求，普教信息化发展的主要方向有校园信息系统、电子学籍、互联课堂、移动校园和数字图书等。普教信息化发展起步较晚，对数据安全与保护的意识还不足，但随着信息化建设的普及，数据安全与保护将成为普教不可忽视的重点。

职校主要包括中职与高职，其信息化应用建设主要包含以下几个方面：校园 ERP、在线学习和移动校园等。党的十八大胜利召开以来，教育部深入落实推进职校信息化进程，已经取得了阶段性的进步，但是目前仍存在灾备技术发展水平不高，灾备机制建设较为落后等问题。

高教信息化建设起步早、发展快、国家投入大，近年来取得了很大的成绩。灾备在高校领域普及程度较广，但目前仍然存在一些问题。高校在运用数据保护技术时往往存在一种误区，当数据中心出现某种需要保护的对象时，便采取针对特定对象的灾备技术，如针对虚拟化的保护，采取虚拟化容灾保护技术；针对存储的保护，则采取存储复制技术。学校为了保护而保护，没有统一的灾备策略，会使得整个数据中心存在多套灾备产品，加大了管理难度，造成了灾备孤岛。高校目前需要通过对自身业务系统 RPO 以及 RTO 要求的分析，结合不同的保护模式，对自己的数据中心及业务系统制定完整的灾备方案。

5.4.2 需求与解决方案

根据具体业务及各教育机构的不同灾难恢复能力，常见的解决方案大致包括三种：

1) 双活数据中心灾备方案

随着高校信息化建设在教学、科研、对外交流中的深入应用，校园规模的逐步扩大使得很多高校现有的设备已经无法满足同一学校多个校区的需求，同时存在单数据中心资源利用率低、数据丢失率高、业务中断时间长、数据恢复时间长等痛点。针对这些痛点，双活数据中心灾备方案应运而生。

后者主要具有以下几个特点：

- 业务双活访问，充分利用资源；
- 业务不中断，数据零丢失；
- 易扩展，便于升级；
- 设备统一管理，维护成本低。

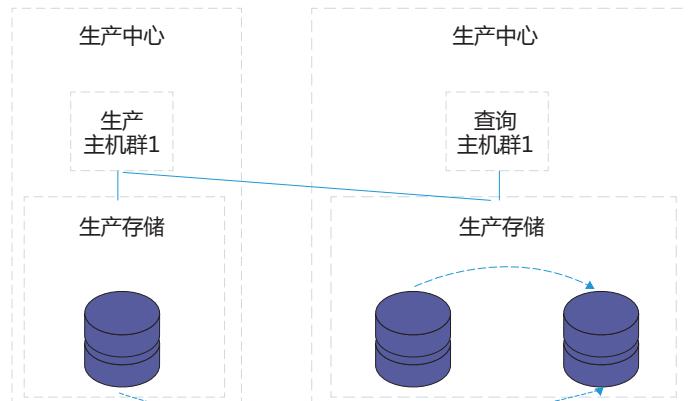


图 5.4-2 双活业务中心

2) 同城灾备解决方案

目前在教育行业中，无论是高教还是职教，大部分学校的业务主要在一个地方开展，若是希望在预算有限的情况下满足数据的一致性，则可以考虑同城灾备的解决方案，即将数据中心与灾备中心安排在同一区域。

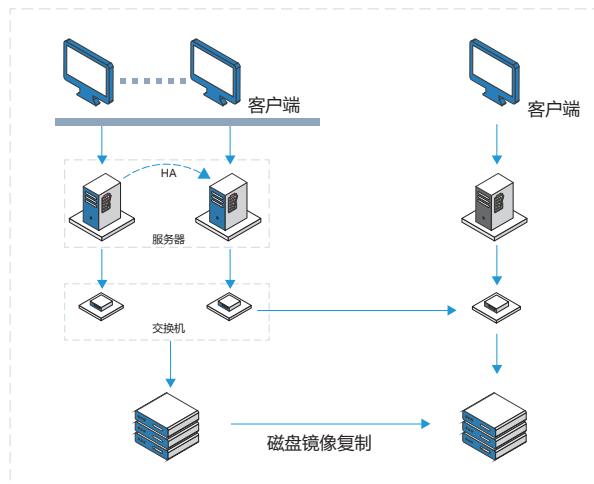


图 5.4-3 同城灾备解决方案

如上图所示，左边区域为数据中心站点，右边区域为灾备站点，数据中心站点配备两套数据库服务器保证业务的高性能，快速响应及高可用性。同时，磁盘数据通过同 / 异步复制技术将数据复制到同城灾备中心。此方案可以实现较好的 RTO 与 RPO 值的降低，能有效保障数据的一致性以及服务的可用性。

3) CDP+HA (High Availability) 解决方案

教育行业的某些重要应用对于业务连续性以及可用性的要求很高，如一卡通系统、财务系统等。如何在这几类应用出问题时对数据以及业务进行恢复是一个很重要的课题。目前灾备行业技术沿革已发展为 CDP（持续数据保护）阶段，CDP 的定义主要有以下三点：首先，可以捕获任意的数据变化；其次，至少可以备份到另外一个地方（异地容灾）；第三，可以恢复到任意时间点。

HA（高可用）作为保障业务连续性的又一法宝，能对服务器资源状态进行实时监控，在发现业务系统异常时，可以自动或手工切换至灾备服务器，保证业务的连续性。CDP+HA 的解决方案中，HA 保证业务接管，CDP 保证数据的可靠性，两者协同工作能确保用户在遭受网络攻击、系统宕机、误操作等威胁事件发生时，快速解决数据丢失、业务停顿的问题。

宁波教育局方案

随着校园的智慧应用不断增加，对 IT 基础设备的建设方案也提出了更高的要求：必须做到可伸缩、易扩展、性能与容量可以简单的叠加等特点。该市教育局云机房项目就是利用云计算技术，彻底打破原有的笨重的 IT 基础设施在支撑学校业务效率与成本方面的束缚与障碍，把传统硬件设备改造成为一个高度简化、标准化、自动化和弹性的云数据中心，使得校园的 IT 支撑系统从校园的“成本中心”转型成为推动智慧校园应用不断发展的引擎。

根据前期调研分析可以看出，市直属学校信息化水平仍有较大差距，以基础资源为例，由于各学校财政状况和对信息化重视程度不一，各学校机房

环境、网络设备、服务器状态和数量差距明显，这不利于保障各学校教育教学和管理系统的信息安全和稳定性。所以统一逐步为学校配备可信、安全可靠的云机房服务，有利于推进宁波教育信息化建设、进一步促进地区教育公平发展。

市教育局直属学校（单位）云主机、智慧教育统一监控、云录播、云桌面对底层资源需求，是对宁波市智慧教育二期云平台能力的扩展和外在补充要求，对底层计算、存储和网络资源的需求而提供服务。

市教育局云机房平台上所承载的业务系统会通过孵化不断的累加。因此，其负载也会随业务上线的不断加入而不断的变重，这对 IT 基础设备的建设方案提出较高的要求：必须做到可伸缩、易扩展、性能与容量可以简单的叠加等特点。

根据现有院校情况，采用系统迁移的方式先将院校的整个系统迁移至电信的云平虚拟化平台 VMware 上，此方式采用 1 对 1 的迁移方式，将每个学校的每台应用服务器迁移至云平台，待迁移完成后，将在电信云平台部署一套私有的云灾备管理平台，该平台的作用是实时的在线的将各个院校的数据集中备份至云平台，每一个学校提供一个账户，该账户具备 5TB 的云存储空间，针对学校的每台应用服务器，均需要安装英方软件客户端，该客户端的作用是捕获用户的任何 I/O 操作，将数据实时同步至云平台，根据用户不同的结构化和非结构化数据，采用不同的配置策略，比如 MSSQL SERVER 数据库数据，只需要保护 MSSQL\DATA 目录下对应 *.mdf 数据文件和 *.ldf 控制文件，比如 Oracle 数据库，需要保护 datafile、controlfile、logfile 这三个的所在目录 /u01/app/oracle/orcl/。

云灾备系统平台，该平台可以通过无缝融合云平台的资源，实现资源共享、成本低廉、部署迅速、灵活弹性的远程灾备服务，在对数据安全性进行严格管理的同时，实现对数据、应用提供最大高可用性保证。

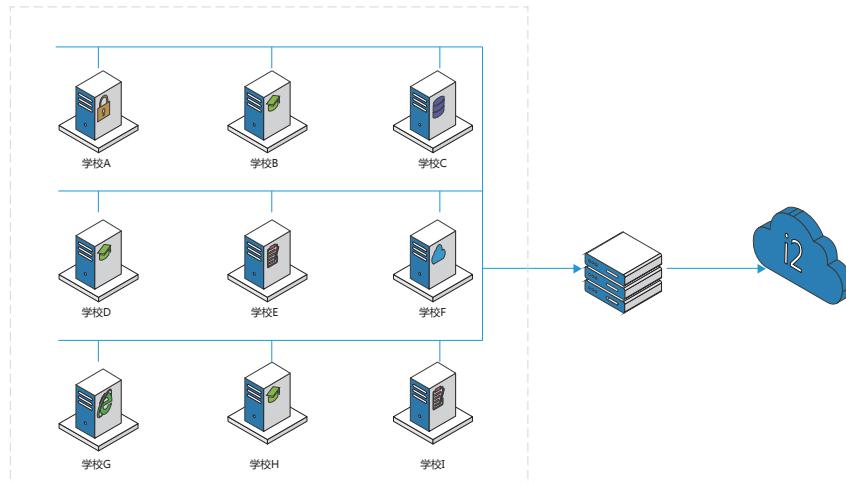


图 5.4-4 宁波教育局容灾拓扑图

整个方案，用户达到很好的收益：

一是按需使用，降低用户使用灾备服务的经济门槛。无须投入大量的建设资金和后续的维护管理成本，只需支付服务费用即可获得完整的备份服务。

二是节省部署时间，降低用户使用灾备服务的能力门槛。终端用户无须部署硬件、软件等资源，无须聘用专业技术人员，在云灾备平台注册，做简单配置后，即可享用云灾备服务。三是多租户操控平台，集中管理。市教育局直属管辖的每个学校用户拥有独立账户对企业的数据进行备份管理，包括数据、应用和系统的备份，迁移和容灾高可用。

中国地质大学方案

该校为全国知名地质大学，为配合数据的集中管理，提高数据备份的有效性和效率，有必要对数据备份进行整合。对备份进行整合可以面向学校用户的核心应用需求，综合设计横跨各个教育系统的数据综合保护策略，根据不同数据备份要求来采用适当的备份手段和软、硬件设备。这样做可以较大程度上降低备份系统的复杂程度，加速关键数据的备份和恢复效率，提高备份设备的综合利用率。

根据院校情况，将采用集中备份的方式把每位老师和同学的关键数据统

一同步到云灾备管理平台，该平台的作用是实时在线地将各个老师和同学的数据集中备份至云平台，每一个用户提供一个账户，该账户具备一定的云存储空间，该客户端的作用是捕获用户的任何 I/O 操作，将数据实时同步至云平台，根据用户不同的结构化和非结构化数据，我们还能采用不同的配置策略。

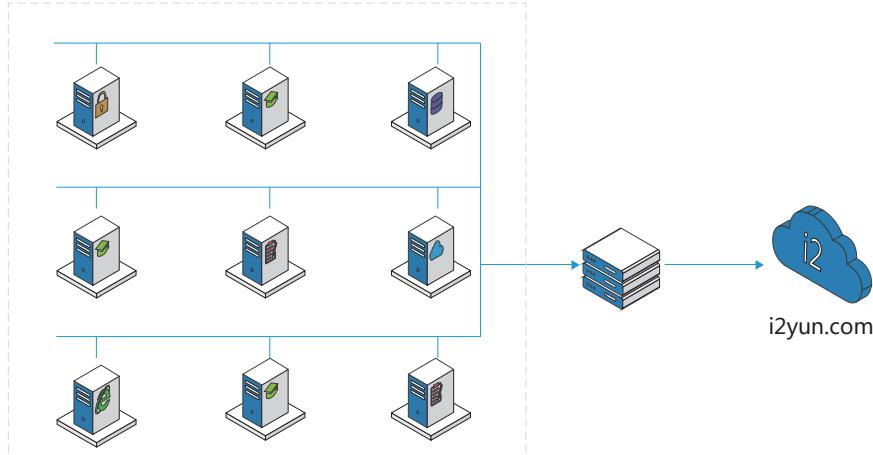


图 5.4-5 中国地质大学容灾拓扑图

通过该方案，该高校获得以下收益：一是节省部署时间。终端用户无须部署硬件、软件等资源，在英方云灾备平台注册，做简单配置后，即可享用云灾备服务。二是按需使用，降低投入。无须投入大量的建设资金和后续的维护管理成本，只需支付服务费用即可获得完整的备份服务。不论因数据增量需要扩容空间，还是停止业务不再备份，都可以灵活选择。三是多租户操控平台，集中管理。中国地质大学的每个教师和学生拥有独立账户对本自己的数据进行备份管理。地质大学 IT 管理人员的主账户可对各个独立账户进行管理和权限设置，便于集中管理。

5.4.3 行业趋势

数字时代带来了学习方式的变革，教学技术的革新、学习管理系统的增加、虚拟实验室的推广和云平台的广泛应用，都将产生大量的应用和数据。而灾备和数据是分不开的，未来灾备的热点将会根据数据中心的发展而发生

变化。

随着数据中心集中式架构向分布式架构的转换和云的进一步普及，未来学校对灾备及业务的连续性要求将会越来越高，并呈现出从单活到多活，从本地到云灾备的发展势头。此外，云端多活数据中心也将是未来教育行业灾备发展的重要方向。

5.5 制造行业灾备建设特点及方案分析

5.5.1 行业概览

制造业是指机械工业时代对制造资源（物料、能源、设备、工具、资金、技术、信息和人力等），按照市场要求，通过制造过程，转化为可供人们使用和利用的大型工具、工业品与生活消费产品的行业。小至食品加工大到石油化工，在完整的制造流程中，包括了产品设计、原料采购、制造生产、仓储运输、订单处理、批发经营、零售等。

制造业主要分类有 30 多类，直接体现一个国家的生产力水平，具有漫长的发展历史和企业基数。据统计表明，中国有 80% 以上的制造业属于中小型企业，有 43.8% 的企业拥有 15 台以内的服务器，只有 12.5% 的企业拥有 500 台以上服务器。此外，IT 硬件基础环境已由传统的单机、双机运行，逐步转向虚拟化平台，小型机在企业中也将渐渐被 X86 平台替换。而随着企业的劳动力成本，及各种生产经营成本的上升，资源利用率高，灵活性和扩展性均较强的云计算平台将被越来越多的企业所使用，企业生产系统业务云端化是新的趋势。

随着互联网对全行业的渗透，传统制造业开始转向互联网，除了核心的生产系统，基于互联网的业务系统开始承担企业营销宣传的重任，互联网业务 / 电商平台变得极其重要，为了确保高频交易、高并发，以及 7X24 小时无休的业务连续性运营，具有冗余功能的存储网络建设和数据集中存储备份、容灾的需求越来越紧迫。但是制造行业属于大型门类，在灾备建设领域还有

诸多不足，譬如：

企业决策者对灾备需求认识不足，预算投入低

在制造业企业的整体工作链条中，数据及系统这种隐形产出并不能直接体现在最终的销售利润上，而多数制造企业的 IT 设备也较为简单。在企业的预算中，IT 被认为是一个消耗公司利润的部分。因此，在很多企业不管是 CEO 或 CIO 都没有提供足够资源及预算来保证灾备项目的实施。但是随着数据资产的重要性越来越明显，以及网络攻击越来越频繁，企业管理层的灾备意识已经在提升。

生产中心区域化对于灾备数据中心距离的挑战

随着企业规模的不断扩大，基于对人力、运输、政策、成本等诸多因素的考量，企业的生产架构在逐步演进，从集中生产加工制，转变为分区域、单元、厂区、产线的制造模式，灾备中心也随着企业格局的转化在不断转变，规模在不断扩大，如何支撑多点分区域型数据中心的灾备建设，解决灾备距离产生的灾备难点，同时促进企业内部各区域之间的信息化互通，为企业发展提供坚强的护盾，构建统一的灾备数据管理及灾备运维中心，是当前 IT 管理者面临的重大挑战。

灾备软件、硬件种类繁多无从选择

目前市场上有各种各样的灾备软件，有基于存储虚拟化的，有基于备份软件的，有基于快照的，有基于 CDP 的，有数据库文件层面的，有事务日志层面的，种类繁多，良莠不齐。如何选择适合企业的灾备产品，如何在有限的资源下为企业提供更高的数据及业务保障，避免灾备软件对硬件的兼容性需求，降低硬件的投资成本，提升投资回报比，这是一个令众多 IT 经验并不丰富的制造业企业决策者头疼的问题。而随着制造业整体向互联网的转型，未来制造企业的 IT 环境中各种数据库平台、中间件平台、互联网业务等应用的容灾必须要进行统一规范的灾备建设，这样更有利于灾备管理与成本的降低。

企业信息化变革带来的灾备特性要求

科技强国之路的概念在逐步影响着中国制造，也在慢慢改变中国制造，随着人力资源的稀缺、成本的逐步增高及各类产线的衍生，高效、智能化的生产制造设备及模式被逐渐引入到制造行业，同时引入的还有信息化建设及灾备概念，信息化的建设作为支撑企业稳健发展的中坚力量，业务系统及数据的安全性保障问题在助力信息化建设的过程中显得尤为重要，传统灾备模式覆盖面有限及单一特性在应对产线系统、管理系统及各类数据库复杂度的灾备要求时，渐有力不从心之态，例如基于 Oracle 或 SQL 的 MES 系统、DB2 及数据库集群的 ERP 系统，与企业转型所涉及的电子商务系统，以及通过其它关系型数据库构建的模块化产线子服务系统，如何在满足不同业务系统特性的要求下，进行有限的灾备资源覆盖，实现分数据、应用、系统、平台等层次结构清晰的灾备等级保障，对于灾备建设提出了更高的要求。

5.5.2 需求与解决方案

集中统一的容灾备份策略是制造企业的基本需求。但是由于企业规模的不同，灾备模式也会不同，比如规模型大企业，会慢慢建设私有云平台，或者将非核心业务系统搬迁至公有云上，在本地与云端之间对核心业务系统及非核心业务系统进行容灾备份。但是对于中小型企业，由于场地、人员、资金等方面预算有限，在灾备模式建设上以简单高效为主，比如服装设计、食品加工、医药制造、橡胶和塑料制造、汽车制造、零件制造等，仅需要对业务系统进行本地容灾，或对 ERP、OA 等系统进行异地容灾，采用简单的灾备一体机等灾备解决方案。

此外，随着大数据时代下海量数据的增加，数据迁移在整个灾备过程中变得非常重要。一般而言，企业会借助专业的迁移工具完成结构化和非结构化数据的本地到异地，或本地到云端的迁移。

在灾备方案建设方面，虽然涉及的领域非常广泛，但是由于其等保要求远低于金融类，所以灵活性更大，方案也会简单得多，比如集中的备份管理，

企业可以根据自身需求进行定期或实时的数据备份，二两地三中心、异地多活等大型灾备方案很难出现在制造行业。下面是几种简单的容灾备份的方式（当然也是适合其他行业的通用型灾备模式，我们集中统一到制造行业分析）。对于很多制造企业，可能会选择其中的部分模式，或者全部选择，完全取决于企业对灾备的需求。

1) 数据及业务系统迁移

由于新建机房或者企业上云等需求，为了确保两端数据的一致性、完整性，数据及业务系统迁移需要依靠专业的迁移工具协助完成。区别于传统的从 A 盘拷贝到 B 盘（或磁盘阵列），现在的企业更多讲究在线热迁移，即在不停机的情况下，将企业的数据及业务系统源源不断传输到备端（包含了迁移过程中新增的数据），包括操作系统、应用程序、用户信息、网络配置等所有的数据。

2) 企业个人电脑重要数据共享存储和保护

制造行业有一个很显著的特点，往往个人电脑的数据就是企业的重要数据，比如服装设计师的设计文件，如果不能够及时有效地备份，一旦丢失也就是公司的损失。因此，企业个人的电脑重要数据共享存储与保护也非常的重要的。因此，通过在备份服务器上配置管理控制台，将每个台式机或笔记本上安装客户端代理软件进行定时或实时备份管理，使得台式机或笔记本电脑用户的数据可自动复制到网络共享资源中，用户无论是在办公室或是路途中，都可以根据自己的需求存放数据。例如，对于有主备生产中心的企业，可以在生产中心放置一台服务器作为共享文件服务器，提供诸如 NAS 的文件访问和共享等功能。

3) 业务数据恢复

备份的目的是为了数据的恢复，但是随着互联网对业务的影响越来越大，生产数据的生成速度正在成倍提高，如何保障备端数据的安全，以及主备端数据的一致性和完整性，就需要数据恢复技术的与时俱进。比如在生产端发

生人为误操作、病毒攻击等逻辑错误时，备端不可避免犯同样的错误。这时，如果借助持续数据保护 CDP 技术，就能够将数据恢复到任意时间点，确保数据的安全。

4) 业务的高可用

在生产制造加工企业中，流水线上的员工加班是家常便饭，甚至很多企业把其看成是正常的生产时间，这说明任何时间任何原因导致的停工对企业而言都是一种损失。据相关数据表明，关键应用的宕机给用户带来的损失是巨大的；50% 以上的大型制造企业每小时关键业务宕机时间损失超过 1 万美元；55% 以上的中型制造企业每小时关键业务宕机时间损失超过 4 万美元。为此，在 IT 系统故障导致的业务停顿必须要找到合适的灾备方案予以解决。对制造类企业而言，双机架构和异地高可用接管都是很实惠的选择，前者确保业务应用跑在两套相同的系统上，后者确保当生产端出现故障时，备端能够快速接管起来。

以上四种是比较通用的灾备方式，在具体的案例中，双方往往会根据需求进行整合，比如在一个案例中，同时出现四种灾备方式。

5.5.3 未来趋势

随着企业数字化转型的加快，制造企业数字化、互联网化、云端化会成为趋势，企业的生产效率将成倍的提高，数据资产因此成为制造企业重要的生产资料。

未来 IDC 的灾备需求更灵活，制造企业需要定义备份数据流走向，灾备建设不只有备份的功能，还具有数据管理、备份数据分析、数据报表等功能，备份系统应整合数据管理系统，成为提供统一的数据备份和管理的平台。云端应用、桌面虚拟化等趋势也将影响用户容灾备份解决方案的选择。

5.6 电信行业灾备建设特点及方案分析

5.6.1 行业概述

随着互联网的兴起，目前电信行业正面临新的竞争格局和市场变化带来的行业变革。电信巨头们也在极力寻求转型，一方面要把管道做好，做到管道平台化、智能化；另一方面积极在互联网领域开发新的商业模式，培养新的业务能力，以更好的接受市场的挑战。以大数据、云计算、物联网、边缘计算等为代表的新技术应用是电信运营商发展趋势，经过几年的技术研究和发展，运营商对云计算技术和大数据已形成一定的积累，并已经开始尝试内部应用和对外服务，对内提供业务支撑、运营、管理、大数据分析等服务，对外提供弹性云计算、云空间、云备份、云迁移和云容灾等多样化服务。

运营商平台包容性强，对新技术、新事物的接受能力更强，也更注重平台安全、架构安全。传统的运营商平台业务安全架构主要包括：双机热备技术、存储底层复制技术、传统备份技术、数据库复制技术等。当前，运营商在持续利用传统安全技术加强云计算环境中的网络和平台设备的安全能力、健全安全体系的同时，还为了满足新业务模式下的数据安全，对业务和数据保护有更高的要求，如数据实时复制、CDP（连续数据保护）、云平台业务高可用、自定义多租户云备份服务等各种定制化服务需求。另外，通过规范安全运营、构建体系化的云计算安全服务的风险评估和评测体系，在降低业务运营风险的同时，对提高用户对云服务的安全认知度，提高云服务产品的市场竞争力也大有益处。

电信运营业务复杂、规模庞大、根据业务特征可笼统的分为三大类：基础业务、互联网化业务、ICT 业务。

基础业务——包括电信基础通信服务以及后台运营管理部分。

基础通信服务涉及端到端的信息语音传输，如通话类服务、分组交换数据传输服务、电路传输服务、传真服务等。此类业务通过多中心冗余、多节点冗余、链路冗余提供业务连续性保障，对容灾软件需求较少。

运营管理部分通常包括几个系统：BSS、OSS、MSS、BI。BSS 即业务支撑系统包括计费、帐务、客服、营业厅、客户关系等；OSS 即运营维护管理系统包括资源管理、网管、网优等；MSS 即企业内部管理系统包括人事、财务等；BI 指经营分析系统，用于经营分析、决策支持等；这类业务属于核心业务，且数据量大，对计算性对要求较高，对数据的使用修改较为频繁，所以灾备级别要求较高，通常采用本地备份加异地容灾多种保护手段进行保护。

互联网化业务——包括运营商自主运营业务和资源租赁业务。自主运营业务如中国移动八大基地（音乐、阅读等），电信的天翼视讯、天翼阅读等；资源租赁业务包括 IaaS 资源服务：如物理机托管、租赁；PaaS 资源服务：提供弹性云计算资源服务、云存储服务等；SaaS 资源服务：提供云迁移、备份、容灾、云与云与线下机房业务高可用等应用服务。

ICT 业务——运营商面向政企客户的增值电信业务服务、系统集成服务、流程咨询与开发实施服务，此类业务涉及行业较多，平台各不相同，对于灾备要求不一，大部分由运营商合作 partner 提供一体化的灾备方案。

5.6.2 需求与解决方案

电信行业现有的业务系统如 BSS 业务支撑系统、OSS 运营支撑系统、MSS 人务财务资源管理系统等，底层对应的各类数据库系统（如 SQLServer、Sybase、Oracle、DB2、MySQL 等）的正常运行和公司的正常运转息息相关，任何系统的宕机都对企业事业单位的运营影响巨大，所以要求每个系统要有可快速恢复的灾备配置。

另外政府或企业自建灾备机房成本较高，而运营商云平台是可信度较高的服务提供商，将数据或业务迁移到运营商云平台，在内部 IT 机房和运营商云平台之间做灾备，可使数据安全和业务的连续性等得到保障。

除了基础业务系统外，运营商云平台和一些商务应用运营平台，比如移动八大基地，电信的医疗云等，随着规模的扩大和数据量的增加，必须要进

行灾备系统的建设，以确保出现意外时，业务能够正常运营或能够恢复正常运营。

通过使用英方 i2CDP+i2Availability 模块，基于内核级的数据复制技术，实现 RPO 接近于零 RTO 控制在秒级的应用级容灾目标。同时针对数据的备份，在备份端进行数据再备份，不但解放生产机的备份压力，还可对数据进行多重保护。针数据库数据、文件数据、应用软件实现连续保护。

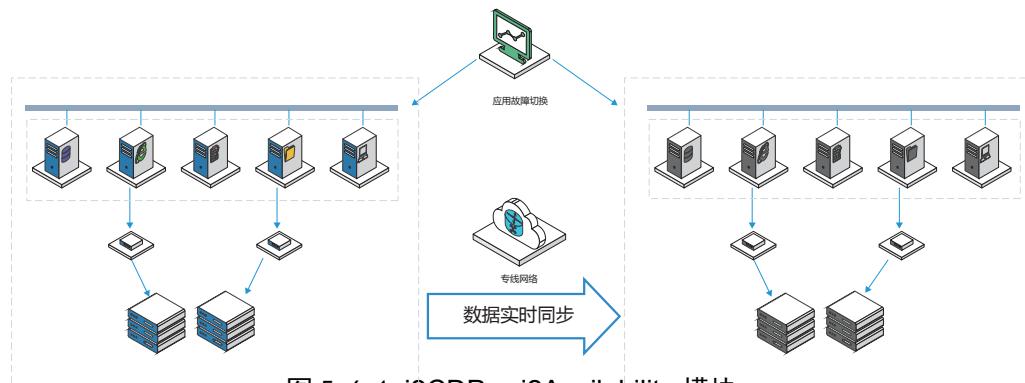


图 5.6-1 i2CDP + i2Availability 模块

英方软件 + 运营商云平台的云备份解决方案允许为任何企事业单位应用 / 数据制定高效、可靠的灾难恢复计划。在按需分配的基础上，通过云备份，既可大大节省建立多个专有灾备中心的费用，如相关的硬件、软件、电力、冷却以及管理等费用，又可享受海量存储和高性能云计算的服务。此外，云备份还实现了和硬件无关的连续数据保护。当数据或者应用出现异常时，可通过图形化管理工具快速实现恢复。恢复粒度可以是单个文件、整个应用系统或数据库等，同时，还可以按照实际使用量来进行计费，永久解决了业务增长和信息系统之间的不匹配而导致的不断扩容的问题。

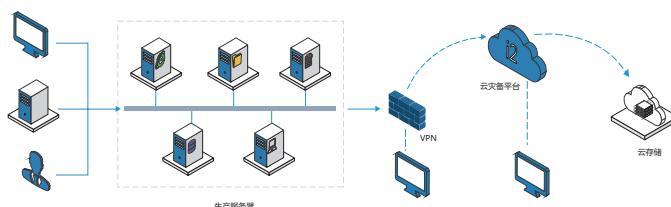


图 5.6-2 英方软件 + 运营商云平台的云备份解决方案

电信异地灾备中心

为了避免地震、水灾、人为破坏、误操作、宕机等对电信基础业务连续性的影响，需要在较远的异地之间通过专线做灾备，并且要实现多个核心系统在这两地之间能够快速地执行应用级容灾的切换，并且要求应用软件层与数据库的两种类型数据都要进行实时数据同步。

沙特运营商 ZAIN

沙特运营商 ZAIN 的生产中心放在了首都利雅得，灾备中心则放在东部城市达曼，达曼西南距首都利雅得 410 公里。采用了 i2CDP+i2Availability 的解决方案，在达曼灾备中心的 Linux/Windows 的主机上安装英方控制机，利用 i2CDP 实现数据的实时备份，无备份时间窗口的情况下时刻保证有一份当前最新数据用于即时恢复。在应用高可用管理监控平台则通过英方控制机监控，采用 i2Availability 进行高可用系统容灾，确保在源端生产主机出现任何问题时，可手动分组切换进行相对应的业务接管，有效规避由于源端问题而导致业务中断的情况。

一是实现异构平台数据同步：不同型号配置物理服务器、不同厂家虚拟化平台主机层之间进行数据同步。二是字节级实时数据复制：适用于远距离窄带环境中数据同步与一致性（结构化数据与非结构数据）。三是管理简单、图形化切换：英方控制台基于 B/S 架构，方便管理，提供手动、自动、分组切换等功能。

某省电信云灾备管理平台

随着近几年众多宕机事故的发生，越来越多的企业开始更加重视企业在数据安全以及业务连续性方面的保障，越来越多的企业开始在灾备建设上进行投入。然而，传统灾备工程因其复杂性高、前期投入过大、业务不断变化带来容灾运维等问题，对于那些计划启动灾备建设的企业来说，如何平衡成本与收益可能是他们进行灾备投入前首先需要面对的问题。

在英方云和某省电信合作建立的电信云灾备平台上，有一家地方市银行

和地区农村商业银行均使用其云灾备服务保障重要数据和业务的高可用，并将灾备投入降低到可控范围内。据悉，这是国内银行系统首次真正使用云灾备技术来保护数据和业务连续性，这类地方银行的云端容灾案例对其他企业平衡灾备投入与收益方面有很多借鉴作用。

依托省电信的数据中心资源，采用英方云的云端灾备技术，双方合作建立的电信云灾备管理平台提供本地或云端的应用级高可用、云灾备及各类业务系统的持续数据保护与快速恢复。实施简单，上线快，兼容性强，缩短企业容灾进程外，还提供自助式的服务。

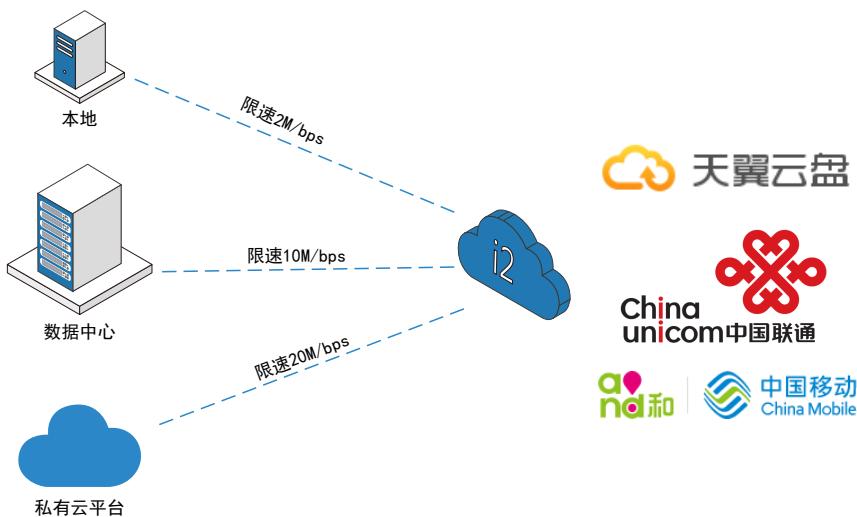


图 5.6-3 i2Cloud 灾备管理平台

该平台采用了基于操作系统内核中文件系统驱动层面的数据捕获技术。对于客户端所需要保护的目录及文件，在完成了初次的全镜像后，基于文件系统驱动层面的数据捕获模块能够实时感知到上层应用写入到磁盘的所有 I/O 操作及数据，并将这些信息正确发送到云端，由云端再一摸一样的对云端磁盘执行这些 I/O 操作，由此实现了客户端数据实时同步到云端存储。依据特有的数据序列化传输技术，严格保证了客户端和云灾备中心数据的一致性和完整性。

平台提供了云迁移，云高可用，云 CDP，云备份和恢复等功能，具备传输效率高，占有资源少，传输加密，无须停机，兼容性强等特点。

以兰州市银行为例

该银行采用了该平台的 i2CDP 解决方案。i2CDP 通过监控被保护数据的变化，将数据持续不断复制到省电信云灾备平台，无须自购备份服务器或建立异地机房，实现数据的持续保护。同时，也将数据的每一次变化以日志的形式记录下来。i2CDP 引擎分析捕捉的日志以及相关数据，计算出文件变化的部分，将其保存到 CDP 数据保护区中。当数据要恢复时，可以直接指定要恢复的时间点，或者通过日志上下文来辅定位要恢复的时间点。一旦时间点选定后，通过配置并按您的需求恢复到不同的硬件或虚拟服务器上。

以某地区农村商业银行为例

该农村商业银行采用了该平台的 i2Cloud 解决方案。i2Cloud 将系统灾备软件和省电信云平台技术融为一体，将整个灾备平台建于省电信云端，避免了在异地建立物理灾备机房的模式，通过云计算资源共享，实现成本低廉、部署迅速、灵活弹性的远程灾备服务。对数据安全性进行严格管理，也实现了对数据和应用的最大高可用性保证。同时，i2Cloud 通过多种数据加密方式，对用户数据进行有效保护，并结合省电信所提供的高安全存储，充分避免了信息的泄露。除此之外，i2Cloud 通过特有的 DOT 数据序列化传输技术，严格保证数据在云存储上的一致性。

CloudOpera IES（ICT 基础设施使能系统）智能云专线灾备

这个结合灾备、云计算、智能网络相关技术的创新应用，是为了解决这样的用户场景——传统的行业用户通过传统专线连接云端进行数据灾备，但传统专线难以满足其对带宽的弹性获取需求。例如医疗行业会将影像等非结构化数据备份到云端对象存储，此时需要高带宽尽快完成备份；而其他时间数据量少对带宽要求不高，因此如果长期租赁高带宽则费用昂贵。

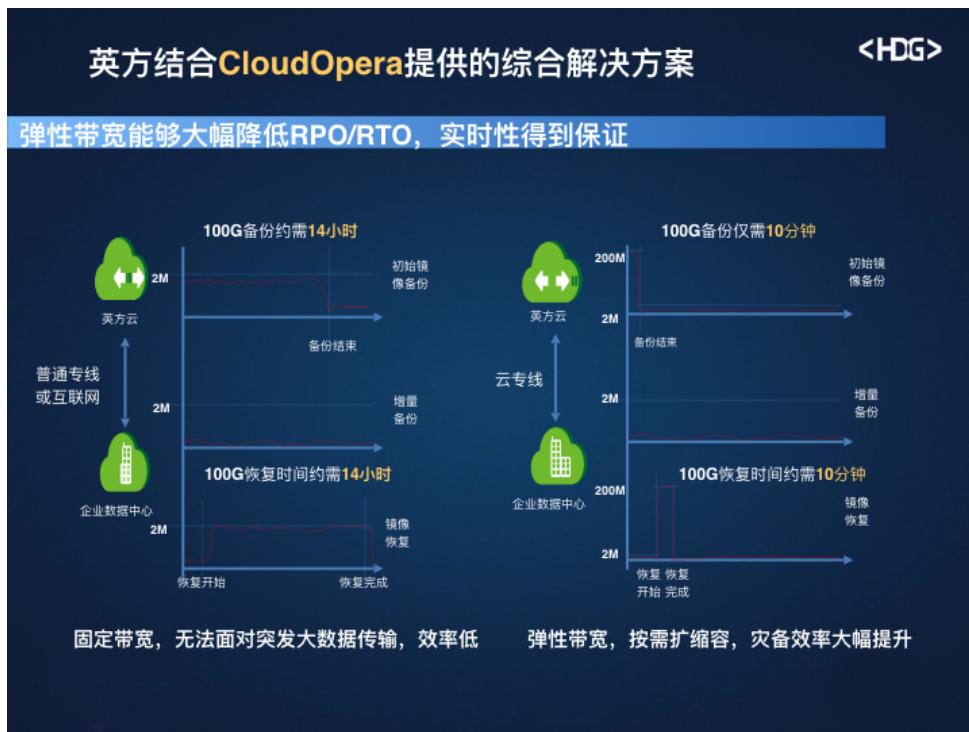


图 5.6-4 智能云专线灾备示意图

据此，英方股份和运营商、华为通过强强合作，推出了创新的智能云专线灾备解决方案。整个方案的创新之处在英方股份通过运营商电商网站自助申请智能云专线带宽升级业务后，IES 系统根据指定策略编排 ICT 资源，将带宽自动从 2M 升级到 100M，整个升级过程从原来的 7 天缩短到 4 分钟，备份 100G 数据到云端，从原有 100 小时缩短到 2 小时，备份结束后恢复到低带宽。

这种资源弹性的使用方式不仅能够满足云灾备的传输要求，而且比长期租用高带宽更具性价比。敏捷、智能、高效、开放的全面云化网络是运营商实现商业转型的关键，今后全面云化网络战略推进企业云端灾备的智能应用将是运营商灾备业务的趋势。

中国移动手机阅读基地

除了结合运营商进行灾备项目的建设，对于运营商互联网化运营平台的灾备建设也是一个行业特点。中国移动手机阅读基地现有主备两个数据中心，分别位于杭州的三墩和滨江两地，两边的存储为异构存储，内容库部分的数据容量约为 40 亿 TB（截至 2017 年 11 月），文件数量超过 20 亿个，每一天的数据增量超过 10GB，现需要将位于三墩主生产中心的内容库数据文件实时同步到滨江的备数据中心，且不能影响业务的正常运行，即对外阅读业务不能停止。且要求在灾备系统中能实现考虑到未来磁盘和服务器的弹性扩展以及两边灾备切换演练的需求。

英方软件将相关数据以增量方式实时复制到备端 NAS 存储上，具体数据流向以图中虚线 1、2、3 步所示，第 1 步为应用对数据的修改访问，数据的变化被英方软件截获后，通过第 2 步发送到备端，然后再通过第 3 步实时存储到数据中心。两边存储可异构，部署时无需停止阅读应用，实现数据的动态同步复制，具体架构如图：

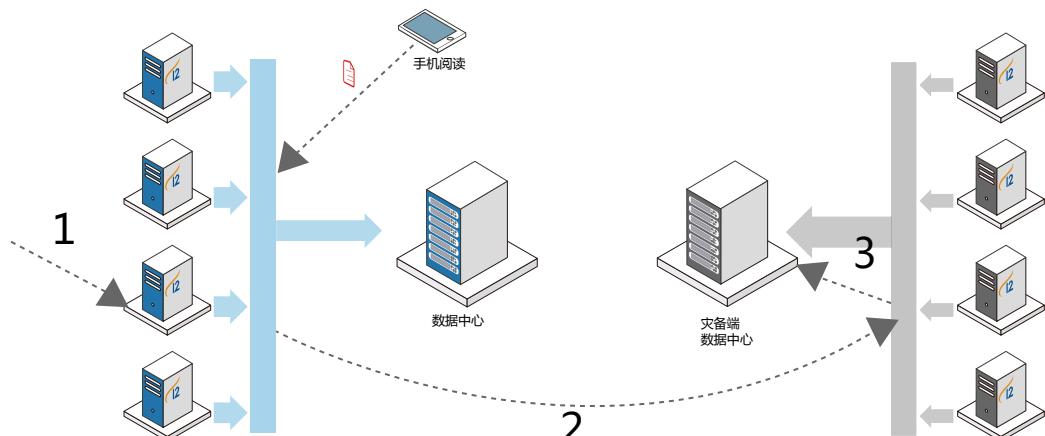


图 5.6-5 中国移动手机阅读基地容灾拓扑图

5.6.3 行业趋势

未来，运营商将大规模发展云平台服务。中国移动将投入数百亿资金加大云计算技术设施的投入，在哈尔滨、呼和浩特、贵州等地建设大规模数据中心，同时推进云计算商务应用。中国联通计划在全国部署十大云数据中心，

总机架数超过 20 万架，总带宽超过 20T。中国电信天翼云也将在近两年着力建设电信特有混合云，以便能够迎合企业和政府客户的需求。未来云计算服务市场将保持高速增长态势。

云服务也将向更多行业渗透，SaaS 服务是未来的主要方向，而云灾备是将灾备看作一种服务，由客户付费使用灾备服务提供商提供灾备的服务模式。采用这种模式，客户可以利用灾备服务提供商的优势技术资源、丰富的灾备项目经验和成熟的运维管理流程，快速实现用户的灾备目标，降低客户的运维成本和工作强度，同时也降低灾备系统的总体拥有成本，所以转变成灾备服务提供商一种创新的服务形式，也是运营商未来的发展方向。

5.7 互联网行业灾备建设特点及方案分析

5.7.1 行业概览

广义的互联网行业所涉及的范围非常广泛，很多传统行业也正在纷纷转型为互联网行业。本文所指的互联网行业主要是指那些通过互联网、物联网开展产品展示、销售、支付等业务的企业。与传统企业不同，互联网企业最大的一个特点就是用户从消息的获知到商品比较再到最终的购买行为、售后服务等都是通过企业自身或第三方的网站进行的，电商是互联网企业最重要的交易方式，比如淘宝、携程等。因此，对于网站架构及应用的灾备建设成为互联网企业的最重要的内容。

主备同步、数据同步是互联网行业较为常用的灾备方式，两个数据中心服务器部署完全一样，每次发布都要在两个数据中心同时发布，以保证运行系统版本一致。两个数据中心有主备之分，数据通过准实时的同步系统从主站不断同步到备站。当主站发生灾害性故障导致完全不可用，则将域名解析切换到备站。

互联网行业的龙头企业在高可用架构建设上经历了 3 个阶段：第一个是同城的双活；第二个异地只读及冷备；第三个是异地多活。由于异地机房距

离较远，数据库要实现数据实时同步就非常困难，因而一般的互联网企业是在应用层实现了数据的分片，底层数据库还是相互独立的，普遍场景是应用双活+DB容灾，但带来的问题是一旦跨域访问DB可能引起很高的延迟累积。

在异地项目中，由于技术瓶颈仍有不少互联网企业采用冷备方案，主要在于异地双活数据的正确性很难保证。数据在多点同时写的时候，一定不能写错。如果应用出故障了，顶多是用户不能访问。但如果数据写错了，对用户和企业来说就彻底乱了，而且这个故障是极难恢复的，因为无法确定到底哪里写的才是对的。所以，第一原则是业务层故障可以接受，但是不能接受数据故障。

5.7.2 需求与解决方案

互联网企业发生事故，可分为机器级和机房级两类。前者主要原因是系统架构不是很好，遇到访问量过多会带来宕机；后者则主要是外部攻击造成的，结果比如会造成机房的瘫痪。机器级的故障主要是实力较弱的互联网企业会遇到；大企业面临的主要威胁一般就是机房级的故障，如2015年支付宝光纤挖断事件。

因此，互联网企业数据经常会有多个备份，包括本地服务器同城机房、跨城机房、云端以及内网。对于尚处初创期的互联网企业来说，云技术是非常普遍的选择，除了自建的私有云技术，还有应用服务的云技术、数据的同城容灾和异地云备份等。

主要需求可概括为：

易扩展性：对多层架构应用系统的灾备支持，在面对应用分离、性能拓展、体系重构的场景下，无需对现有的灾备系统进行重组，更好的支撑业务系统的横向或纵向扩展。

完整性：在跨地域及异构云平台的场景下，实现字节级的数据实时同步，针对不同应用系统，不同数据，实现全方位的数据及业务连续性保障。

易管理性：在多应用实例，主、备区域分离场景下，实现灵活配置、动

态监控、统一管理的便捷化管理功能，同时满足不同层次的管理需求。

典型解决方案

1) 混合云灾备

以某互联网企业项目为例，采用 i2 软件安装在相关主备服务器上，针对各类数据和应用程序实施实时保护和切换，各自主备两台机器之间实现数据 / 应用实时复制，同时，实时监控并且根据具体设置进行故障切换。针对阿里云多台主机实现云端到云端的实时数据保护，当单一节点故障时，可由其灾备节点提供业务支撑，实现整个业务架构在云端的高可用接管。

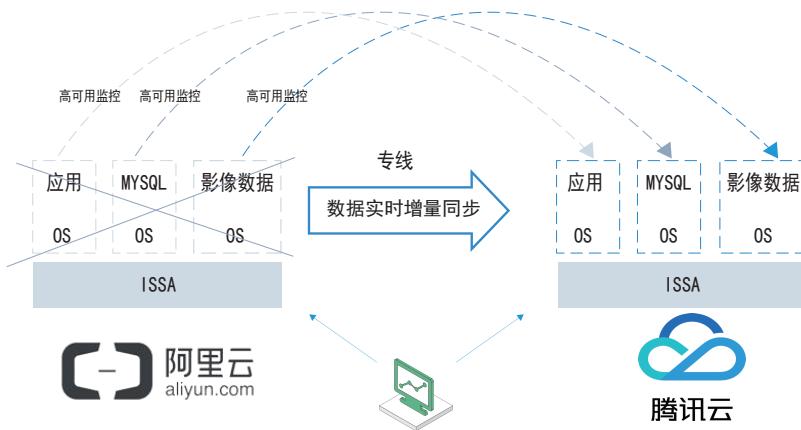


图 5.7-1 混合云灾备场景

2) 多对一数据集中灾备

服务器名称	操作系统	备注
日志收集服务器 A1-A6	RHEL5.8 64 位	工作机
灾备存储服务器 server1	RHEL5.8 64 位	灾备机, 控制机
日志收集服务器 A7-A8	RHEL6.5 64 位	工作机
日志收集服务器 B1-B8	RHEL6.5 64 位	工作机
日志收集服务器 C1-C6	RHEL6.5 64 位	工作机
灾备存储服务器 server2	RHEL6.5 64 位	灾备机, 控制机

表 5.7-1 软硬件信息表

该方案使用 i2COOPY 软件的实时数据复制技术，使得每一笔流水日志得到实时保护。另外，该灾备架构易于扩容，当用户投入一台新或旧的服务器时，只需在其上安装连续数据保护软件，即可文件数据实现连续数据保护。具体说明如下：

N 台日志收集服务器——在其上均安装 i2COOPY 客户端模块，通过客户端模块实现应用实时监管，保护业务连续性。

1 台灾备机服务器——在其上均安装 i2COOPY 虚拟机客户端模块，通过客户端模块实现连续数据保护。

新增灾备服务器——随着数据增加，未来可以增加灾备服务器数量，只用安装 i2COOPY 插件，图形化简单配置即可。

弹性带宽调节——通过流量控制功能设置工作时间的灾备可用带宽，甚至暂停复制；工作时间外可以随意放宽限制，避免对生产系统的带宽冲击。

部署简单——所有的配置和监控可通过灾备控制机实现，通过 WEB 的方式实现灾备的配置、流量监控、恢复等。控制机可以是网内的任一台服务器，其上安装英方灾备控制机模块，该服务器必须和所有被管理的服务器可达。控制机软件模块一般安装在灾备端。

易扩容——在未来的系统扩展方面，只需在新的需保护的系统上安装 i2Soft 模块即可，无需采购同构的硬件或其它灾备模块。

3) NAS 共享存储场景的海量数据容灾

互联网行业显著的特征是业务互联网化，前端应用直接服务于批量的线上消费者。因此，线上业务平台的在线服务时间必须保持得到保障，并且当系统出现故障时，要保证业务数据丢失是最少的。但是，很多互联网企业由于对外提供服务一般是多集群的前端互联网业务平台，并且采用性价比高的 NAS 存储集群架构，而在海量数据环境下，NAS 存储集群架构很难做到异地实时数据复制备份。

从数据安全管理角度来看，从 NAS 上复制文件是一件让人头痛的事情。

如果使用 NAS 厂商的相关复制功能，那么就必须有一套相同的 NAS 系统复制。而现有的 NAS 系统只能在文件管理系统层次进行复制，无法做到按需选择按需复制。实际环境中，用户更希望针对特定文件进行相应的管理。比如，对相关的文件进行实时的备份，但是因为前端业务集群服务器主机可能会同时读写同一个 NAS 文件夹中的数据，造成无法实现数据的实时保护。另外，亿万级的海量小文件，如何确保复制数据在主备两端的一致性、初次全镜像的同时如何确保镜像过程中增量部分的同步，都是困扰 NAS 架构下海量小文件数据容灾的难题。

以某信托公司项目为例

实时同步方案的数据复制流程分解如下：

首先是在若干台前端业务服务器上面都安装软件客户端；

其次是单独使用 1 台服务器（取名监控服务器）映射挂载 NAS 存储共享目录；当任何一台前端业务服务器对 NAS 目录修改数据时，本地客户端会将修改的文件名和存储路径通报“监控服务器”，并由监控服务器读取数据复制到容灾端。

该解决方案是旁路监听，客户端只监控当前业务服务器对 NAS 共享目录文件的修改事件，本身不产生性能开销。

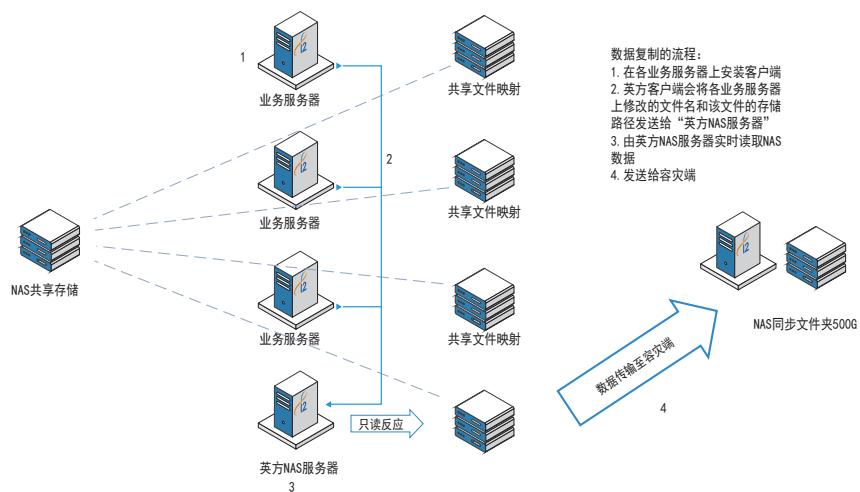


图 5.7-2 基于 NAS 的实时同步方案

如图，前端有三台业务服务器，假设第一台产生数据修改，则立刻通报监控服务器，然后会率先进行传输；当第二台完成数据修改后，复制任务就会进入监控服务器传输队列，依次类推……监控服务器得到数据修改确定的落盘指令后去读取对应目录，再由 TCP/IP 网络将变更后的生产数据发送到容灾端的服务器。

在 NAS 服务器集群环境下，通过监控服务器作为业务服务器 I/O 变化的合并节点，能够实现秒级同步数据的效果。

该方案既解决了实时同步的问题，又解决了海量数据情况下数据复制时间窗口的问题，确保当生产环境 NAS 存储出现故障时，用户的数据安全，业务连续。

分布式数据库场景

互联网企业经常需要做大数据分析，联机分析处理（OLAP）系统是数据仓库系统最主要的应用，专门设计用于支持复杂的分析操作，侧重对决策人员和高层管理人员的决策支持。以某项目为例，灾备软件能够实时灾备 GreenPlum 数据库集群的各个节点的数据，实现对数据的有效保护。同时，配合灾备软件的高可用模块，可以实现当主节点业务中断时，能够有效启用备机上的业务，实现业务连续性保证。

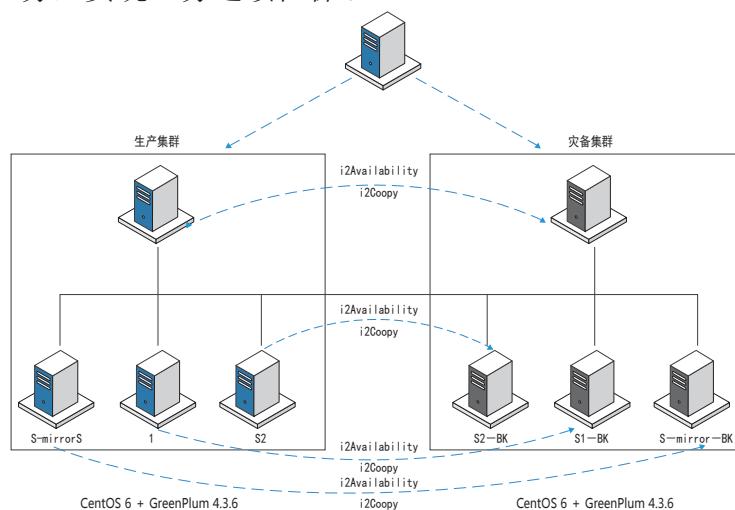


图 5.7-3 虚拟平台测试环境

数据插入过程中模拟生产集群宕机，灾备集群接管后，数据没有丢失。如果灾备集群的某些节点由于异步复制的关系导致某些数据没有同步过来时，灾备集群 GP 服务这时仍能正常启动，数据仍能正常查询，但某些节点的数据或会少量丢失。

分布式文件系统场景

分布式系统（如 Hadoop FS、Hbase、MapReduce 等）常见于互联网企业，多采用 Master-Slave 架构。hdfs 有两个核心 namenode(一个主节点),datanode (多个从节点)。datanode 主要是存储数据，namenode 一是管理文件系统文件的元数据信息（包括文件名称、大小、位置、属性、创建时间、修改时间等等）；二是维护文件到块的对应关系和块到节点的对应关系；三是维护用户对文件的操作信息（文件的增删改查）。Hadoop 节点宕机退服，对系统的影响较小，系统会自动将数据在其它节点扩充到 3 份，即 datanode 具备自身的保护机制；而 HDFS NameNode 的高可用方案实现和配置方式比较复杂，英方灾备软件可以针对 namdenode 进行数据复制和实时保护。

5.7.3 行业趋势

相比于其他行业，互联网行业可谓是“近水楼台先得月”。在云计算的大趋势下，相较于传统灾备模式，云灾备由于其具备的弹性优势，能够在更大程度上保障客户业务连续性等特点，已经成为众多互联网企业所青睐。此外，互联网行业也是云灾备的塑造者，只是因为互联网新业务的不断涌现，才使得云灾备得以进一步落地。

未来，互联网用户在云端进行灾备规划的场景之一可能是将生产业务放在同云之间，由云服务商提供同云之间不同区域进行备份与高可用，或者放在不同云之间，以确保其中的一家云计算服务商出现问题时，另外一家云服务商能够快速接管业务。这两种模式都能实现云端的备份与高可用，并构建云端的两地三中心模式，问题是这涉及到专业的实时复制容灾技术，以及缺少相关的符合国家容灾等级的行业资质。

5.8 电力能源行业灾备建设特点及方案分析

5.8.1 行业概览

能源行业主要涵盖电力和石油石化，中国能源行业以国有企业为主，规模庞大、业务繁多、地域分布广。

电力行业作为国民经济发展的战略产业，较早使用 ERP、MIS 和 OA 等系统，基本实现了计算机自动化管理与监控。这些自动化信息系统在给电力生产效率带来极大提升的同时，如何确保系统运行的安全性也成为了保障电力安全生产需要面对的重要问题。为此，国家安监总局和国家电网专门出台了《电网调度系统安全性评价》、（2006）34号《电力二次系统安全防护总体方案》、《电网调度安全分析制度（试行）》、《电网调度二次设备分析制度（试行）》等文件，从制度上保障电网安全生产。

电力生产由发电厂发电，经过升压送入智能电网进行统一调配，输送到各地，再降压送到终端用户使用。这一系列过程中，电网的监控与调配起着核心关键作用，它保障了整个电网的协调运行。我国电网调度采取了分层设计，分为县级、地区级、省级、大区级和国家层级。其中最重要的是大区级调度中心，如华北、华中、华东、西北、西南电网等等，这些大区调度中心承担着具体的电力监控调度职能。我国自行研制的 Open3000、DMIS 或新一代的 D5000 电网调度自动化管理系统是电网的核心监控调度系统。作为一个调度平台，其包含了众多的子系统，包括 SCADA 数据采集与监控系统、FES 前置系统、PAS 数据分析与处理的高级应用系统、EMS 能量管理系统、国产数据库系统等等。这些调度信息系统部署在我国的各大电网片区的调度中心以及其他各类调度中心。

石油行业的信息化建设进程同样面临 IT 系统建设不断投入，系统维护难度提高，维护成本难以为继的问题。勘探开发系统涉及地理信息系统、地震资料处理分析系统、测井资料处理系统、油藏综合描述系统、地质绘图系统、地址模拟系统等，数据类型多、复杂性高。面对全球激烈的市场竞争，

石油行业必须进一步促进数据、人力和流程的全面整合，及时作出市场反应，降低运营成本和提高国际竞争力，这是行业信息化建设的当务之急。

能源行业领域，除了核心系统外，还应用了大量的信息系统，用于承担各类业务，如协同办公系统、人力资源管理系统、生产和营销管理系统、财务系统等等。近几年，虚拟技术发展迅猛，其在电力行业也得到了广泛应用，许多不是很重要的业务系统均移到虚拟化环境下运行，提高了资源的使用效率。

5.8.2 需求与解决方案

在不同的网路分区中再建设一套独立的统一灾备平台，对现有业务系统及数据进行额外保护是一种比较常见的解决手段。采用虚拟化的灾备平台，针对每套业务系统独立分配相应的灾备机，实现数据的实时同步；灾备平台实时监控原有业务系统的运行状态，一旦探测到原有业务系统不可用时，灾备机立即接管业务，对外提供服务，确保了业务的连续性。

从技术上来看，主要有两种技术实现以上的业务高可用模式：

基于虚拟机的半热备模式：该模式定时（最短可达分钟级）将主机的所有数据和状态备份到虚拟机镜像文件里，一旦主机宕机，灾备平台会自动启动备份虚拟机，待虚拟机启动完毕，并且加载业务系统完毕后，即可接管业务。

基于数据实时复制的双机热备模式：该模式可以采用物理机或虚拟机作为业务系统的灾备机，并建立复制规则实时（毫秒级）将主机的数据及状态实时复制到灾备机。一旦主机宕机，灾备平台会立即启动相对应的灾备机上的业务系统，接管业务。

以上两种模式可以看到，半热备模式需要加载虚拟机并启动操作系统，且数据复制不是实时的，因此其时效性较差，对一些要求很高的业务系统来说不适用。第二种热备模式，其数据是毫秒级实时同步，而且当需要接管业务时，操作系统已经就绪，仅仅需要启动业务系统，因此时效性很高，接管速度快，且数据丢失量能达到最小，非常适合于对关键业务系统的保护。

目前，双机热备的保障模式已在某些大区调度中心得到了应用，该模式能够很好的与原有的业务系统热备模式相兼容，实现了对关键业务系统及其他系统的多层次保障，减轻了系统运维的压力。

目前，绝大多数的电网调度系统实现了应用服务的双机热备，部分重要的业务系统之间（如 scada、fes）还运用了互为冷备；同时，电网的调度系统现在都是主备调，备调都是建设在异地，主要包含 scada、fes 等重要的业务系统，系统数据与主调保持同步、采样数据独立，实现了重要业务及数据的异地容灾。

电力业务系统搬迁

某电力系统打算搬迁服务器，将本地的双机架构分开，将其中一些服务器放置在异地，然后实现异地高可用保护。业务主管充分考虑电力系统业务现状，如何保证在业务系统搬迁时，本地单机服务器在突发故障时能避免因故障而导致的损失，以及确保业务系统的完整性是目前考虑的重点。目前，已经采用应急故障一体机来解决搬迁过程中因生产业务服务器故障而导致的业务中断，但是当灾备中心服务器配置完毕后，解决在线系统迁移是客户面临的一大挑战。

为了实现业务的持续运行和在线系统迁移，用户要求容灾解决方案能实现在出现灾难，比如服务器硬件宕机、损坏的情况下，业务系统能自动切换到灾备系统上继续运行，确保应用系统的持续运行，并且可以实时地将生产系统的数据和系统数据搬迁至灾备中心，以保证系统和数据的安全稳定。

针对用户电力系统的现状，建议采用在线服务器迁移解决方案，i2Move 将复杂的系统迁移工作简单化，且在生产系统不停机情况下迁移现有整个系统，包括操作系统、应用程序、用户信息、网络配置等所有的数据，整个迁移过程时间可预测，并可在迁移完成后立刻切换到新系统，真正迁移过程服务不终止。

考虑到用户现状和国家对相关单位等级信息容灾的要求，以保证系统和

数据的安全稳定，容灾备份及业务连续性管理建设目标至少包括以下几个方面：

实时备份——对电力系统内的服务器上的数据库和文件进行自动监控，连续捕获和备份数据变化，只要数据发生变化，便实时、准确的备份下来。

业务连续性保障——恢复时间目标 RTO~0，让系统在出现故障后能快速恢复业务系统对外服务。即当生产系统出现异常时，将生产系统上的应用按需自动切换到灾备服务器上，实现应用级快速切换，减少服务的中止时间，保持业务应用的高度可用性。

在线热迁移——一些老旧服务器由于硬件老化随时宕机，同时机器的业务厂家无法联系，在线热迁移服务可以为老旧服务器上的数据、服务提供可靠保障。

双机双柜——无共享磁盘的双机双柜，解决共享磁盘模式的单点数据故障问题，任何一点出现故障，发生切换，都不会影响到其他部分系统的正常运行，并且在切换过程中无需人为干涉。

任意回退——电力系统的各应用下存在很多表以及很多的配置文件，这些都是由用户维护，很容易出现误操作，当任何一台服务器内发生逻辑错误时，可按任意操作步数或时间点进行数据快速恢复，回到数据的任何状态，从而能够找回误删或者损坏前的数据。恢复后的数据要 100% 可用，确保事务完整。

结构化和非结构化数据区别备份——为了保证数据库的备份准确和可用，对结构化的数据库要通过独立的专用模块进行实时备份，需能进行数据库的任意时间点回退；对非结构化的接线图、图元等数据进行定时备份，保证这些数据的完整性。

能源企业数据集中灾备

中国能源建设集团公司总部拥有包括 OA、Mail 等十多个信息系统，其中财务、人力资源等系统为公司统一部署系统，对公司各地子公司的业务运

营 进行集中支持和管控。

随着各系统全面推广和深化应用，以及新业务系统的建设，公司的数据量将越来越大，对信息系统的依赖性 越来越高，信息系统的业务连续性和数据安全性对公司的正常运转日趋重要。通过英方灾备硬件一体机设备将各信息系统的数据库、数据文件等进行集中备份和持续数据保护。同时，通过打通灾备一体机和英方云平台，在云端构建云灾备主机，利用英方字节级数据传输技术实现本地数据中心数据实时传输到云灾备主机中，将数据传输到公有云端保存。保证应用系统的业务连续性和数据安全性，总体达到 3 级灾难恢复能力等级考虑。

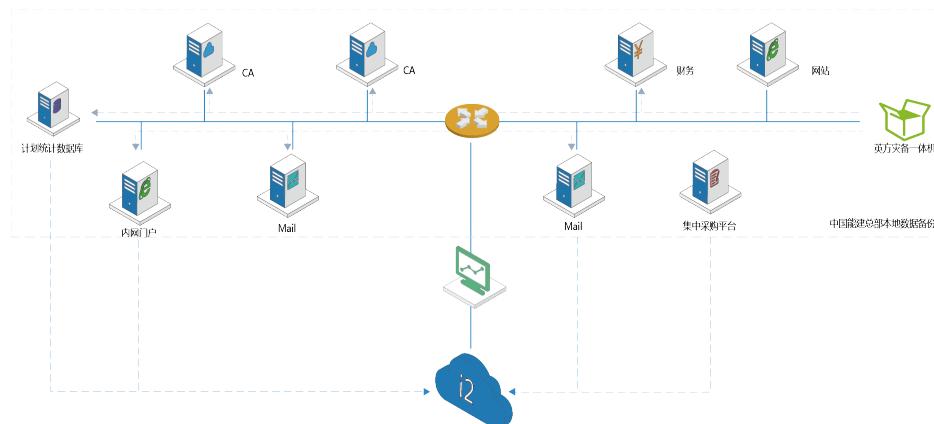


图 5.8-1 中国能源建设集团容灾拓扑图
方案特点：

集中备份：可以将多台服务器上的数据集中实时备份到此容灾备份一体机上；

低耗资源：对主数据压力小，系统采用消息机制，只有在数据发生变化时才触发，只传数据的变化部分；

安全可信任：容灾备份系统将会毫无保留的接触及获得用户的所有数据，要坚决杜绝后门，特别是有保密要求的数据及单位，数据的安全性尤其重要；

TCO 合理：易用易维护易扩展易升级。

5.8.3 行业趋势

灾备技术总是在追求更安全、更高效的目标中前行。未来，无论是电力还是石油企业，目前的生产系统自动化水平高，但管理信息化应用水平却有待提升。完善集中、统一、稳定的信息采集渠道，建立覆盖行业各环节、各区域信息共享体系是发展方向之一。

由于能源企业的地域分布特性，信息化程度的加深必然产生大量的远程数据交互需求，因而数据和应用的灾备会朝着集约化、平台化的方向不断发展。针对重要调度系统需要持续完善灾备生态体系的建设，建立从完善本地机房到同城灾备再到异地灾备的三级灾备体系。系统既在机房进行本地灾备，同时还进行同城灾备及异地灾备，最大程度满足数据及业务的安全性、管理的便捷性、灾难响应的快捷性。

第六章 灾备技术及行业未来发展趋势

在最后一个章节，我们将通过前五章的内容梳理归纳出灾备技术及行业未来发展的若干趋势，希望可以为灾备行业的广大从业者提供一些借鉴。

6.1 云灾备将成为主要形势之一

根据 TechTarget 2015 年云存储调查，接近一半的企业使用了云存储服务，平均来讲，有 24% 的数据放到了云上，可以肯定的是，云存储的发展将进一步刺激云灾备的发展。在数据备份方面，63% 的受访者表示基于云来实现，44% 提到了灾备。有预测显示，目前全球数据量以每两年翻一番的速度增长，到 2020 年全世界需要管理的数据将达到 35ZB（1ZB 约为 1000 亿 TB）。

云计算、大数据等新技术和应用为该领域提供了新的发展机遇，云计算的核心思想是将大量资源统一管理和调度，向用户提供按需服务。基于云计算技术，灾难恢复系统成本更低，恢复速度也更快。

在 Gartner 最新发布的魔力象限表明，当前的数据备份及恢复应用呈现出可以针对数据中心的各类负载的备份及恢复工作趋势，而传统工作的观察重点则倾向于以某项企业应用为重点。虽然企业的工作负载变得越来越多，如文档处理、文件分享、邮件、数据库、操作系统、CRM、ERP 等等，但各类负载正在向云环境的适应性却在增强，并形成数据中心的工作负载发展的明显趋势。为此，备份及恢复服务供应商对云环境的亲和性、对于云环境的适应能力以及在满足数据中心工作的可扩展性等方面都成为未来该领域的竞争热点。

6.2 智能化成为灾备的下一个趋势

灾备智能化是一个涵盖智能动态带宽调节、智能弹性计算、智能切换监测等在内的统一灾备系统。它基于英方等灾备企业提供的智能灾备管理平台，

实现整个 IT 系统数据安全、业务连续性的智能化管理。灾备智能化将更加满足云计算、大数据时代下数据在不同物理机、虚拟机、中间件、数据库、云平台、不同混合环境下对数据自由流动、保护、分享的实际需求。

1) 灾备带宽智能化

在智能灾备的管理下，用户可以根据需要自动调节带宽的多少，比如全备份时需要 100 兆，非全备份时需要 2 兆，目前英方联合华为和运营商的 Cloud Opera IES 方案，已经实现落地应用。

2) 灾备计算智能化

在云灾备的环境下，生产端往往承担较大负荷，比如服务器承载的各种应用，但是在灾备端是没有什么负荷的，只是接受数据，只有当主机发生故障时，备端才需要进行切换接管，备端对 CPU 的占用资源很少。对于用户而言，智能化灾备可以快速对 CPU 的数据进行增减，以匹配生产端的业务应用。

3) 业务切换的智能化

灾备不仅是数据的复制，还有业务的连续性，这涉及到业务的高可用切换。智能灾备可以监测到业务的停止需不需要切换，让切换更加智能，并且在灾备演练和客户真实发生故障时，都能够达到秒级高可用切换，帮助用户实现 RPO 与 RTO 接近理想值。

灾备智能化的目的是为了帮助从业者能够更加便捷、安全、高效地使用灾备产品，无论何种方式的智能化，用户对安全可靠又好用的产品永远不会拒之门外，这是值得所有第三方灾备供应商借鉴的模式。

6.3 灾备是网络安全的重要保障

党的十八大以来，以习近平同志为核心的党中央高度重视网络安全和信息化工作，把完善互联网管理领导体制作为十八届三中全会确立的 60 项改革任务之一，成立中央网络安全和信息化领导小组，统筹协调各个领域的网

络安全和信息化重大问题。

信息安全是国家安全的重要组成部分，已经上升到与政治安全、经济安全、领土安全等并驾齐驱的战略高度。《中华人民共和国国民经济和社会发展第十三个五年规划纲要》中明确指出要：强化信息安全保障，包括强化重要信息系统和数据资源保护，加强数据资源在采集、存储、应用和开放等环节的安全保护，加强各类公共数据资源在公开共享等环节的安全评估与保护等。而对于信息安全、数据安全，灾备是最基础的技术需求，几乎所有的信息资产都需要灾备保护，以确保在任何意外故障情况下，信息系统的正常运转。

金融、能源、电力、通信、交通等各关键领域、关键部门的关键信息基础设施是经济社会运行的神经中枢，是信息安全的重中之重，也是可能遭到重点攻击的目标。“物理隔离”防线可被跨网入侵，电力调配指令可被恶意篡改，金融交易信息可被窃取，这些都是重大风险隐患。不出问题则已，一出就可能导致交通中断、金融紊乱、电力瘫痪等问题，具有很大的破坏性和杀伤力。因此相关的灾备系统一定要尽快落实到位，作为数据安全的最后一道防线，灾备工作需要肩负的责任重大。

云安全方面，需要不断提升对云计算核心软硬件的自主研发能力，加快虚拟化安全、数据安全隔离和加密、安全中间件、数据备份与恢复等云计算安全关键技术研发及产业化。

提高企业自身信息安全防护意识，建议有条件的企业可考虑将信息安全服务纳入企业的信息化建设预算，并将网络完全应急处理、信息系统安全运维、数据与系统灾备等信息安全服务能力建设纳入重点支持范围。灾难恢复是信息安全保障的最后一道防线。当数据丧失可用性和可控性时，仍可通过灾难恢复技术挽救回来。

6.4 演练在灾备系统变得日益重要

灾备供应商不仅需要提供完善的灾备演练系统，还需要保证灾备演练系统的正常可用。

对于已经进行灾备建设的企业，需要充分了解业务系统更新、调整后，原有的灾难恢复预案是否仍然有效；灾备系统是否已经有效更新；真正发生灾难需要启用灾备系统时，灾备系统的切换时间是否可以满足业务的恢复要求；系统切换流程、步骤是否有遗漏和错误；如何在不影响业务的情况下完成系统回切，并保证系统和数据的完整性等一系列问题；灾备演练对于检验灾难恢复预案的适用性、有效性，提升灾备系统的实际恢复能力具有重要意义。

6.5 灾备人才队伍建设正在加快

灾备属于小概率事件，但是潜在的威胁一旦发生，用户所遭受的损失是惊人的。未雨绸缪，有备无患是灾备服务商给用户保护数据安全与业务连续的方案。近年来，随着各个行业的业务信息化的快速发展，我们发现作为企业IT部门团队越来越多。目前，金融、证券等有明确监管需求的行业一般会有专门的部门负责灾备的规划建设，其他行业的企业IT部门虽然没有专门负责灾备的组织，但也会有个别IT人员兼职灾备规格建设的工作。与此同时，对相关灾备人员的资格认证也越来越多，像DRI每年都在中国举行CBCP的认证工作，培养一大批BCM领域的专业人才。

众所周知，导致数据丢失及业务故障的主要因素：一是难以控制的天灾（火山爆发、地震、海啸、战争等）；二是无法预料的“人祸”（黑客攻击、误操作等）；其三是信息系统本身的脆弱性（BUG、漏洞等）。

从近几年的实际案例中，我们不难发现，虽然造成数据丢失的原因很多，但最大的因素依然是人为的误操作及恶意删除而导致的，这一比例大约占75%。因此，企业不仅需要从硬件的灾备体系上防微杜渐，更需要从人员

思想和习惯上培养灾备意识，做好相应的管理权限分级等工作，逐步完善企业灾备人才队伍和机制体系的建设。

另外，值得注意的趋势是随着跨区域技术的融合发展，促使新的容灾备份产品的功能日新月异，这需要相关的人员熟练掌握软件的使用功能、熟悉行业发展动向等，同时对快速的技术更新和产品迭代有开阔的视野，及时跟进，并做好经验的积累和沉淀。

上海英方软件股份有限公司
SHANGHAI INFORMATION2 SOFTWARE INC.

电话：400-6178-601
邮件：info@info2soft.com
地址：上海市浦锦路2049弄万科VMO花园广场38栋6楼

