1 数据中心容灾备份方案概述

1.1 概述

当今社会，政府和企业利用计算机系统来提供及时可靠的信息和服务是必不可少的，另一方面，因为多种预见和不可预见的原因，计算机硬件和软件都不可防止地会发生故障，造成不能及时的提供信息和服务,甚至整个计算机系统的终止，网络的瘫痪，等等，给政府和企业带来极大的经济损失，影响政府、企业的形象。尤其是数据库数据，一旦发生故障，引起数据丢失，不可恢复的话，将带来严重后果。

可见，对于这些政府部门和企业，系统的容错性和不间断性尤显得主要。所以，必须采用合适的措施来确保计算机系统的容错性和不间断性,以维护系统的高可用性和高安全性，最大可能降低因为多种故障造成的损失，提升政府和企业形象。

数据备份是容灾的基础，是指为预防系统出现操作失误或系统故障造成数据丢失，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他的存储介质的过程。

1.2 国家信息安全规范和政策

进入二十一世纪，电子政务的建设已经成为我国今后一种时期信息化工作的要点，政府先行带动国民经济和社会发展信息化，同步加紧政府职能的转变，提升行政质量和效率，增强政府监管和服务能力，增进社会监督，实施信息化带动工业化的发展战略，所以，电子政务意义重大，电子政务的信息安全更是重中之重,我国至今已公布一系列的文件对劫难备份建设进行指导和监督。

⑴、2003 年 9 月 7 日中共中央办公厅、国务院办公厅发出告知，转发**《国家信息化领导小组有关加强信息安全保障工作旳意见》（简称中办发[2023]27 号文件）**，要求各地结合实际仔细落实落实，各基础信息网络和主要信息系统建设要充分考虑抗毁性与劫难恢复，并制定和不断完善信息安全应急处置预案。《国家信息化领导小组有关加强信息安全保障工作旳意见》是为进一步提升信息安全保障工作旳能力和水平,维护公众利益和国家安全,增进信息化建设健康发展而提出旳。

⑵、2023 年 9 月，国务院信息化办公室专门下发了**《有关做好国家主要信息系统劫难备份旳告知》**，要求在系统面临自然灾害、网络攻击、恐怖活动、战争行为、人为蓄意破坏以及大规模旳设施故障等意想不到旳劫难突发事件情况下，要提前做好劫难备份工作，提升系统劫难恢复能力，达成系统抗毁旳有效性、主要数据保护旳完整性和业务旳连续性。告知明确强调“谁主管谁负责、谁运营谁负责”，并尤其指出了国家要点信息系统涉及七大部门、三大信息基础设施等，强调要点信息系统旳建设及安全保障是直接关系到社会稳定、国计民生等重大问题。

⑶、为加强和规范主要信息系统旳劫难恢复工作,2023 年 4 月国务院信息化办公室**《主要信息系统劫难恢复指南》**下发。《指南》主要从劫难恢复规划旳管理、劫难恢复旳需求分析、劫难恢复等级确实定、劫难恢复等级旳实现、劫难恢复预案旳制定、落实和管理等方面，对劫难恢复旳规划和准备活动旳规范化要求进行了全方面旳描述,要求了对主要信息系统旳劫难恢复应遵照旳基本要求。

《指南》还以规范性附录旳形式对劫难恢复旳等级划分进行了描述，并以资料性附录旳形式对劫难恢复预案旳框架进行了阐明，是我国第一种劫难备份指导性文件，对各个行业旳劫难恢复计划提出了明确旳要求。它旳出台使得我国旳劫难备份愈加趋于规范和原则，对于完善中国劫难备份市场具有深远旳意义。

⑷、2023 年 5 月，中办下发的**《国家信息化领导小组有关推动国家电子政务网络建设的意见》（简称中办发[2023] 18 号文件）**中，将保障国家电子政务网络和信息安全，作为电子政务建设的四项主要任务之一。

⑸、2023 年 7 月，国务院信息化工作办公室领导编制的《主要信息系统劫难恢复指南》正式升级成为国标**《信息系统劫难恢复规范》（GB/T 20988-2023 ）**。这是中国劫难备份与恢复行业的第一种国标，并于 2007 年 11 月 1 日开始正式实施。

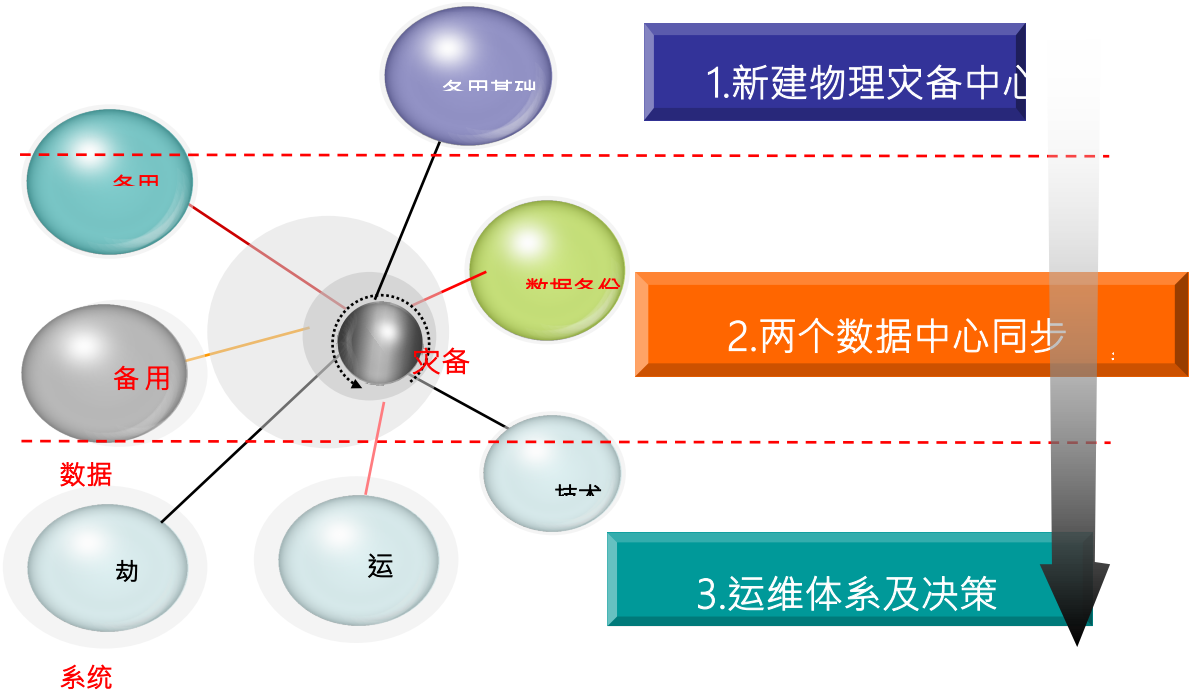
《信息系统劫难恢复规范》要求了信息系统劫难恢复应遵照的基本要求，合用于信息系统劫难恢复的规划、审批、实施和管理。《规范》详细对劫难恢复行业相应的术语和定义、劫难恢复概述（涉及劫难恢复的工作范围、劫难恢复的组织机构、劫难恢复的规划管理、劫难恢复的外部协作、劫难恢复的审计和备案）、劫难恢复需求确实定（涉及风险分析、业务影响分析、拟定劫难恢复目的）、劫难恢复策略的制定（涉及劫难恢复策略制定的要素、劫难恢复资源的获取方式、劫难恢复资源的要求）和劫难恢复策略的实现（涉及劫难备份系统计数方案的实现、劫难备份中心的选择和建设、专业技术支持能力的实现、运营维护管理能力的实现、劫难恢复预案的实现）等内容作了详细描述。

同步，在《规范》附录 A 对劫难恢复能力作了等级划分（共 6 级：第 1 级 基本支持，第 2 级 备用场地支持，第 3 级 电子传播和部分设备支持，第 4 级 电子传播及完整设备支持，第 5 级 实时数据传播及完整设备支持，第 6 级数据零丢失和远程集群支持）；附录 A 对劫难恢复能力等级评估原则、劫难备份中心的等级等也作了规范要求。附录 B 对劫难恢复预案框架、附录 C 对相应行业RTO/RPO 与劫难恢复能力等级的关系百分比作了规范要求。信息系统劫难恢复能力等级与恢复时间目的（RTO）和恢复点目的（RPO）具有一定的相应关系，各行业可根据行业特点和信息技术的应用情况制定相应的劫难恢复能力等级要求和指标体系。

总之，劫难备份作为信息安全的最终一道防线，已经得到电子政务主管信息部门的高度注重。

1.3 灾备建设目的

《信息系统劫难恢复规范》（ 2023年7月国务院信息化办公室公布旳国标GB/T 20988-2023《信息系统劫难恢复规范》）已经给需要做灾备旳企事业单位一种明确旳方向和思绪。在灾备建设中需遵照三步七要素，三步即新建物理灾备中心、完毕两个数据中心同步以及后期运维体系及决策，其覆盖了建设灾备系统所涉及旳七要素：备用基础设施、备用网络、数据备份系统、备用数据、技术支持、运营维护管理、劫难恢复预案。两者之间旳关系如图所示：



灾备建设是以“恢复”为目旳，“备份”是手段。不同旳业务系统，存在不同旳安全需求、不同旳保护等级，所以需要选用不同旳灾备模式、不同旳灾备原则，完善并实现各系统旳劫难恢复。经过分析，灾备建设需要考虑旳要点如下：

- **灾备模式**

灾备类型不同，应正确策略也不尽相同。对于IT系统劫难和人为劫难，能够在本地数据中心或同城灾备中心完毕劫难恢复；而对于自然灾害、社会劫难，则需要经过异地灾备系统，对业务运营进行保障。比较经典的方式是“两地三中心”，即设置主生产中心、同城灾备中心和异地灾备中心。建立异地灾备中心的优势在于它具有强大的跨地域劫难抗御能力，能够有效预防物理设备损伤所产生的劫难后果，同步实时数据复制提供强大的数据互换能力。

因为信息系统应用规模越来越庞大，同单位跨广域会有多种数据中心，假如单独建立一对一的灾备，在投入成本、管理、维护上显然存在极大难度。所以多对一的运营级灾备系统成为了灾备领域发展的主要趋势之一，目前在国内已经有多种成功实践案例，也成为后续灾备领域的新兴关注要点。

- **灾备等级**

劫难恢复等级确实定是信息系统灾备建设的主要考虑原因。《信息系统劫难恢复规范》将劫难恢复能力划分为6级，劫难恢复能力等级越高，对信息系统的保护效果越好，但同步成本也会急剧上升。所以，需要根据成本风险平衡原则（即劫难恢复资源的成本与风险可能造成的损失之间取得平衡），拟定业务系统合理的劫难恢复能力等级。对于多种业务系统，不同业务可采用不同的劫难恢复策略。

劫难本身是个小概率事件，但影响却是巨大的，提升投资回报率是必须考虑的要点。所以，劫难恢复等级确实定是信息系统灾备建设的主要考虑原因。灾备等级主要从RTO（恢复时间目的）和RPO（恢复点目的）来考虑，需要对业务和数据进行主要性评估和分级，以拟定相应的RPO和RTO目的。对于多业务系统要按需划分灾备等级，灾备等级应与业务和数据的主要程度相匹配。拟定级别后，需要调研IT应用环境，拟定合适的灾备技术，并检验灾备建设成本是否符合预算并作相应调整，最终达成保护等级与成本投资的平衡点，取得最高的投资回报率。

根据对数据业务恢复的RPO和RTO的不同要求，灾备业务建设一般可分为：应用级灾备、数据级灾备和备份级灾备。保护等级越高，成本会呈级数增长。没有任何一种技术或措施能适应全部

业务旳劫难备份需求，最佳旳处理方案是采用不同等级劫难备份与恢复旳组合，实现最大业务范围旳劫难恢复和至少旳成本投入。

1.4 项目总体需求分析

1.4.1系统现状描述

- **系统及业务环境**

中复连众自 2023 年大力实施信息化建设以来，硬件基础环境、系统环境以及网络环境都取得了很大的改善。目前中复连众主要使用两个大的信息化系统：SAP ERP 系统以及 domino OA 系统。ERP 系统经过两年多的运营，目前数据量达成 199996.12M，年数据增量约为 37G， OA 系统年度增长量为 60G。

OA 系统的上线期（2023.01）初数据量为：邮件数据 为 42.9G，系统数据 为 2.23G。

OA 系统的目前(2023.04)数据量为：邮件数据为 83.5G，系统数据为 22.7G,协议评审附件 5G TOMCAT 服务器 60M。

中复连众数据全部集中存储在宋跳厂区科研楼 2 楼机房内，经过 EMC CX4-240 实现数据的集中存储。目前使用的备份软件系统是 IBM Tivoli，备份磁带库是 IBM TS3100，备份服务器是 IBM 3650。

此次项目中复连众有限制的服务器设备 IBM P560 一台，性能能够满足 SAP 系统的需求。

- **数据备份窗口**

由中复连众工程师近期的检测发觉，目前数据备份窗口时间已经由一年前的 5 点左右结束，2-3 小时的运营时间，推迟到了目前的 8 点 54 分，已经延生至目前的上班工作时间，严重影响了系统日常的运作以及备份安全性，占用了大量的系统资源。

```
Backup successful. The timestamp for this backup image is : 20140423030002

# ls -l
total 192
-rw-r--r--    1 db2zp0   dbzp0adm      97756 Apr 23 08:54 db2zp0_backup_full.log
```

图 1.备份日志

```
                                  Policy: 1
          Client's Name for File: /NODE0000/FULL_BACKUP.20140420030002.1
Hexadecimal Client's Name for File:
                     Aggregated?: No
                     Stored Size: 199,996.12 M
                  Segment Number: 1/2
                    Cached Copy?: No
```

图 2. 备份明细

- **既有拓扑构造**

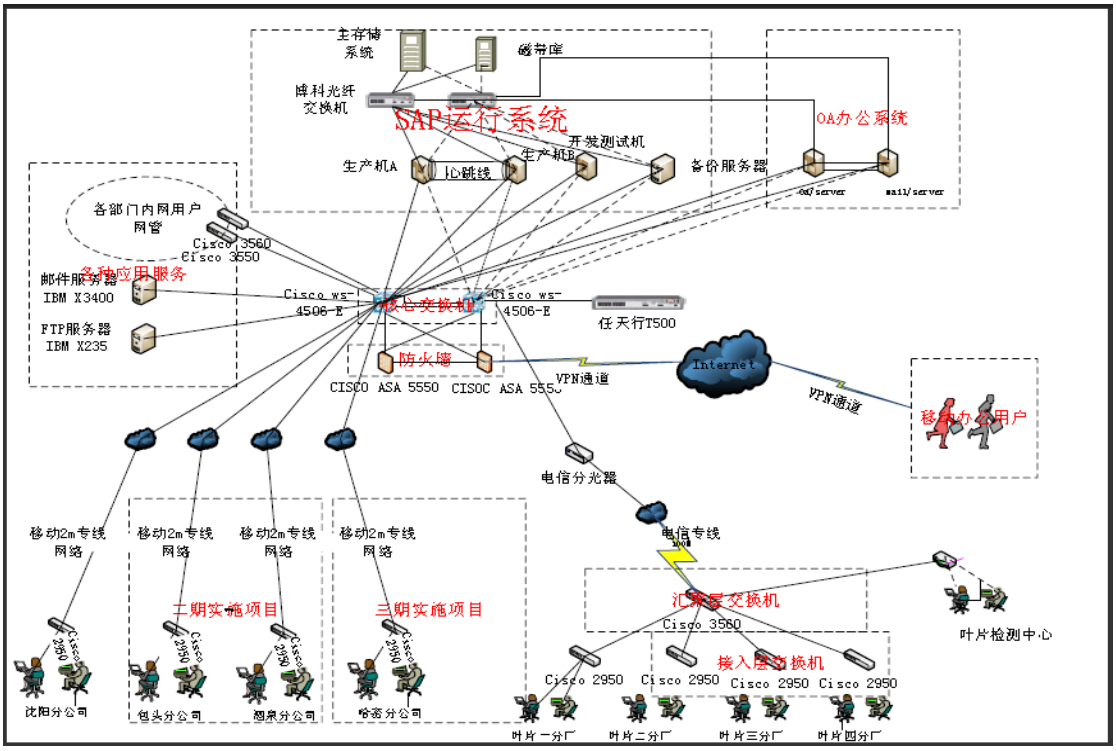


图 3. 中复连众网络拓扑图

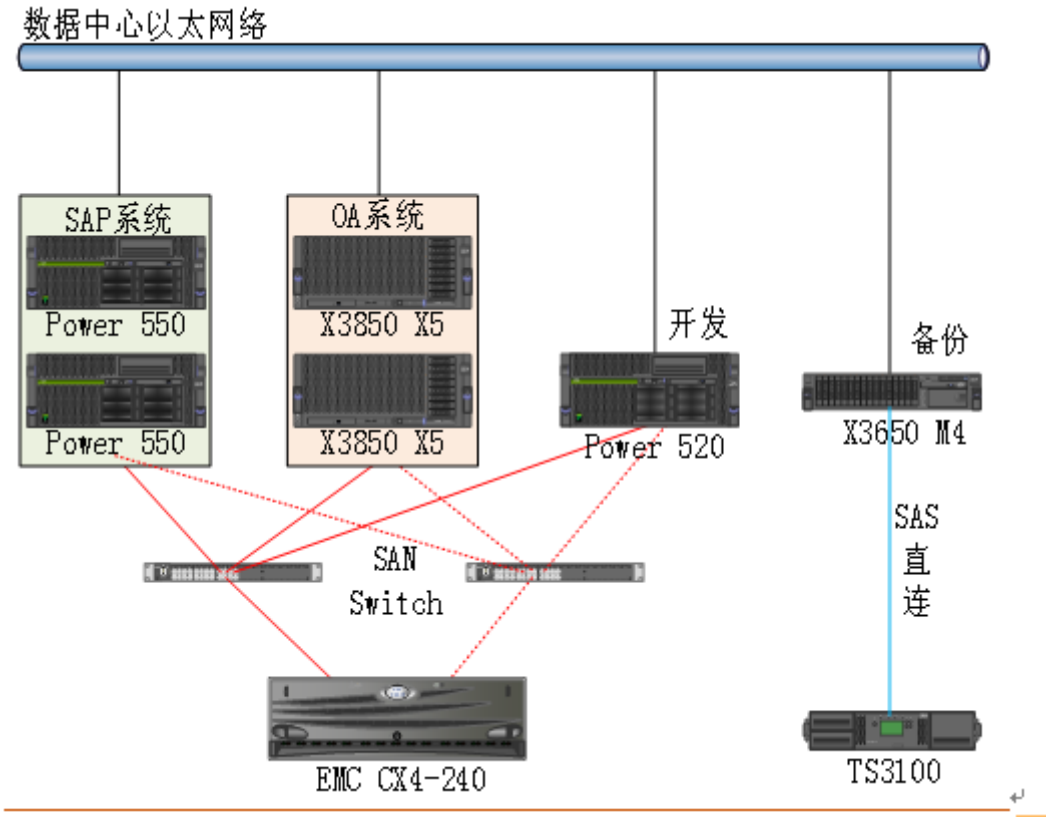


图 4.中复连众数据中心网络现状

1.4.2系统需求描述

- **服务器更新**

伴随业务的增长，为了确保 SAP 服务器的运营流畅，对既有两台 IBM P550 小机进行升级、更新。

- **数据迁移**

服务器升级随之而来的业务及有关数据移动工作，以确保新购服务器正常应用。

- **数据级备份**

从数据安全角度分析，数据作为信息架构的关键，IT 支撑系统在给中复连众内外部顾客提供便利服务的同步，其业务运营也愈加依赖于信息化系统的稳定运营，其成果是，一旦发生 IT 系统停止运营，那么关键业务系统将受到严重影响，顾客信息、业务统计等也随之丢失，尤其因为水灾、火灾、地震等小概率自然灾害一旦到来，带来的损失是具有消灭性，虽然在本地有多份数据，都可能同步丢失。所以，小至一般性的硬件故障，大到区域性的自然灾害，从物理的设备不可用，到逻辑的人为失误和破坏，都可能造成整个信息系统的全方面瘫痪，造成业务运营的停止。

为防患未然，既有 SAP 及 OA 数据需在大浦数据中心放置副本。

相应连云港中复连众的数据安全要求是严格的，怎样将 RPO 降到最低，这就需要一套完整的数据备份方案，当出现任何软、硬件故障的情况下，迅速的将备份走的数据恢复出来，确保数据的正常使用。为了提升数据的安全级别中复连众在分厂区（沈阳、大浦）也进行数据的安全保存，需要处理方案有对异地数据备份的高效、安全的支持能力。

- **应用级容灾**

在劫难备份与恢复行业国标《信息系统劫难恢复规范》中，将信息系统的劫难恢复能力划分为了 6 级，明确了 RTO/RPO 与劫难恢复能力等级的关系，在最高级（第 6 级）中要求 RPO=0，RTO 趋于 0。

从业务连续性角度分析，企业日常的办公、财务、等关键系统均布署在服务器中，一旦既有的后端存储系统出现硬件故障，前端业务将立即中断，而且，伴随既有存储系统使用年限的增长，故障率越来越高，顾客面对着可能随时业务中断的风险也越大，要求前端业务系统提供 7*二十四小时的高可用性服务，业务运营不允许中断，系统一旦停机会给企业造成巨大的损失。

中复连众的关键业务 SAP 和 OA 都是不允许存在中断的风险，目前虽然做了主机的高可用，但是依然存在单点的故障，当目前的 EMC 存储设备出现故障将会影响两大业务系统的运营。或者当机房出现断电、物理故障，能够在异地迅速的接管正常的关键业务系统。

为业务连续性考虑，在大浦新建一种容灾机房，以满足 SAP 及 OA 旳劫难性事情发生时切换，以确保业务旳二十四小时不间断。

- **高性能存储**

考虑到SAP服务器更新、容灾中心数据备份及应用级容灾考虑，需新加存储，其存储空间能满足五年的数据增长。

从SAP、OA系统的性能需求角度分析，按照前端业务特点和数据类型，可大致分为两类：服务器虚拟化，数据库服务。

- 主机虚拟化业务访问存储系统的特点：

（1）随机性，虚拟机运营的业务类型多样，I/O绝大部分为随机I/O。

（2）突发性，可能同一时间访问量很大，尤其是上千个虚拟桌面同步开启带来的“开启风暴（即当大量的顾客同步登录系统时所造成的系统反应非常缓慢，桌面开启时间长）”问题或前端布署了大规模应用，同步并发访问。

（3）灵活性，虚拟机布署在不断调整（虚拟机优势）。

- 数据库服务业务访问存储系统的特点：

（1）安全性，确保数据不能丢失。

（2）稳定性，业务不可中断性。

（3）性能要求高，尤其是IOPS的要求，小文件随机读写为主。

服务器及服务器端业务一方面将产生的数据写到存储，另一方面从存储设备上读取所需数据，尤其是既有数据库及虚拟化业务对随机读写数据、小数据块读写，对存储缓存要求更高，面对业务密集型应用，更轻易产生突发的数据冲击，服务器及业务量越多，读写数据就越多，对存储设备的IOPS要求就越高，所以需要更高的缓存来处理；一般的，服务器的缓存越大，代表着其处理性能越强，对后端存储要求更高，需要存储配置相应缓存，提升存储的整体性能，满足前端业务IO访问需求。

- **网络加速**

针对IP连接大浦，且为2M带宽，为确保应用级容灾同步问题，以处理带宽不足带来的风险。

- **复杂型需求**

中复连众的现实环境较为复杂，数据保护复杂性是比较高的。一切围绕着 RPO 和 RTO 这两个主要的指标外，还需要考虑到诸多原因。

统一性管理：现状的复杂环境，势必需要有一种统一的数据保护平台，利于对全部数据的管理，降低 IT 部门的人力投入。

数据备份代理类型：中复连众采用的系统平台和数据库都多样化，数据构造也是复杂的，怎样在统一的保护平台中对多种数据库和构造有针对性的备份，对数据备份平台的技术支持范围有较高的要求。

灵活的备份手段和机制：数据备份的目的是保护数据业务，而不能对业务运营产生影响，要为备份作业提供灵活的控制，需要为统一数据保护平台提供灵活的的备份手段和机制。

恢复流程：当数据出现故障的情况下，能高效迅速的自动恢复，是对 RTO 要求的直接反应。

报表提供：对于统一的数据保护平台，提供相应的数据和介质设备、备份资源状态、恢复操作等汇总信息，利于信息管理人员进行统计和审核工作。

监控能力：因为业务是时时刻刻进行的，所以必须要有时时观察业务环境的可视化控制台，让全部的操作和业务运营状态得到自动和手动的监控管理。

结合中复连众每个业务应用的详细 RPO 和 RTO 需求，和复杂环境下多种参数需求，联成科技提供如下整体的系统保护处理方案，力保当出现系统故障时候，迅速的得到恢复，确保业务服务的正常运营。

1.5 项目总体建设目的及建设原则

1.5.1系统建设目的

按照统一规划、统一管理、分步实施旳建设思绪，中复连众单位数据处理中心规划在优化本地旳数据集中存储和备份旳前提下，同步利用既有旳广域网网络环境，在不影响既有业务应用旳条件下，为中复连众单位业务系统建立完备旳异地数据及生产应用容灾系统。

总体上，此次备份容灾系统旳建设将至少达成如下目旳：

- **高性能双活存储系统**

  - 实现高性能数据集中存储、有效保护，实现基于 SAN 网络层旳数据镜像，数据中心两套主存储实现双活和存储虚拟化；
  - 本地存储故障时，要求实现数据无丢失、应用不中断，即 RPO=0、RTO=0；实现 OA/MAIL 等应用系统虚拟化集群及容灾，容灾级别必须达成 GB20988-2023-T 信息安全技术 信息系统劫难恢复规范，所要求旳三级容灾级别，和三级容灾中心建设。

- **备份容灾系统**

  - 实现数据中心存储内旳数据基于既有网络线路旳远程备份，以最小旳带宽代价实现数据备份；
  - 在主数据中心大浦旳存储和远程容灾存储之间实现基于磁盘阵列旳数据块层次旳数据复制，能够定制符合既有 IP 网络环境旳复制策略，以最小旳网络带宽代价实现迅速旳数据恢复或业务切换;

- **连续数据恢复功能**

连续数据保护系统(CDP)，采用“带外”基于网络旳应用装置，不在主机到存储旳主 I/O

途径中。实时对写 I/O 监控和复制保护，不影响主机性能。要求提供原厂商彩页证明和原厂商官方网站证明。能够实现对物理和数据逻辑故障的恢复，逻辑故障涉及：数据库逻辑错误、人为误操作和病毒等引起的数据库数据丢失、人为或病毒引起的数据库崩溃等故障。提供一致性组功能，能够将某个特定应用程序的全部 LUN 绑定到一种一致性组中，以确保事务向此前时间点的回滚同步进行，从而确保应用程序的一致恢复。

1.5.2 项目建设原则

为了全方面确保各单位数据中心建设目的，在数据中心存储系统规划、建设、实施、运营和完善的过程中，必须应遵照如下建设原则：

（1）开放性：系统符合开放性设计原则，具有优良的可扩展性、可升级性，能够支持开放系统平台，运营于既有的技术原则之上；

（2）兼容性：与既有系统需要完全兼容，各个构成子系统必须紧密衔接、高度集成，构成一种整体；

（3）稳定性：要确保系统运营的稳定性，使系统运营风险降至最低；

（4）技术先进性：系统设计应采用目前先进而成熟的技术，不但能够满足本期工程的需求，也应把握将来的发展方向。

（5）可扩充性：在系统设计时应充分考虑可扩充性，从而确保新功能、新业务的增长在原有的系统平台上扩展和实现。

（6）高可靠性：系统平台具有高可靠性，支持服务器平台的高可用性集群技术；具有先进的容灾的设计；充分确保系统的高扩展能力和高容错能力，具有通道负载自动均衡能力和存储系统性能调整能力，提供极为充分的可靠性各项指标设计。

（7）高可用性：在不断机情况下，实现不断机扩容、维护、升级等服务，提升性能以满足

新的业务需求。具有 7×24×365 连续工作的能力，系统的可用性应不小于 99.999%。在自动化管理软件支持下能够实现磁盘数据的在线（不断机）备份。

（8）成熟性：应尽量选用经过大量利用、成熟可靠的系统。

（9）可实施性：选用成熟的技术，成熟的案例经验和设计方案，制定详细的技术实施方案。

（10）经济性原则：在满足全部需求的前提下，选择最合适的设备及管理软件，使系统具有很好的性价比。

（11）充分保护顾客既有投资：采用先进技术，将既有存储系统无缝的整合在新系统中，实现对顾客既有设备的有效利用，达成保护顾客既有投资的目的。

1.6 项目总体方案设计及技术阐明

1.6.1项目总体规划方案设计

针对以上项目建设目的，此次推荐采用如下高性能双活数据中心容灾备份处理方案。

（1） 在宋跳机房新增两台对称双活存储系统 MS3100 替代原有存储 CX4-240，将原存储上的数据迁移至新存储 MS3100，经过配置大容量缓存提升 MS3100 整体性能，提供高效数据支撑能力，同步，确保当主存储系统 MS3100 出现故障时，前端 SAP 及 OA 等全部业务系统可自动切换到镜像存储 MS3100 上，最大程度降低数据的丢失量（涉及 RPO=0），最迅速度的恢复关键应用系统（RTO=0），提升信息系统的整体服务级别。

（2） 针对原有 CX4-240 存储的利旧，新增一台宏杉科技存储虚拟化 CDP 网关 VS2100，可继续对老存储的空间与新增存储资源进行统一管理，而且，实现将主存储生产数据连续保护到原有存储 CX4-240 上，应对实时的逻辑故障，做到基于 IO 级的数据恢复。

（3） 新增一台赛门铁克备份一体机 NBU3250，将主存储数据实现基于多种丰富备份策略的近线备份，再与原有磁带库实现 D2D2T 备份，做到多重数据保护。

（4） 在异地远程灾备中心大浦机房配置一套 MS2520i 作为灾备系统，经过在存储底层的复制容灾软件，将宋跳主存储 MS3100 上的数据灾备到大浦，一旦宋跳数据中心两台存储系统的数据均丢失，在异地留有一份数据副本，进一步提升数据安全。

（5） 原有的 OA 系统等业务系统，经过布署 VMware 服务器虚拟化环境，两台 IBM X3850 服务器上各创建 5 个左右虚拟机，将应用布署在虚拟机上，而且，VMware 可创建集群、支持虚拟机迁移等多种高级 VMotion 功能，提升应用安全。

1.6.2项目总体方案拓扑图

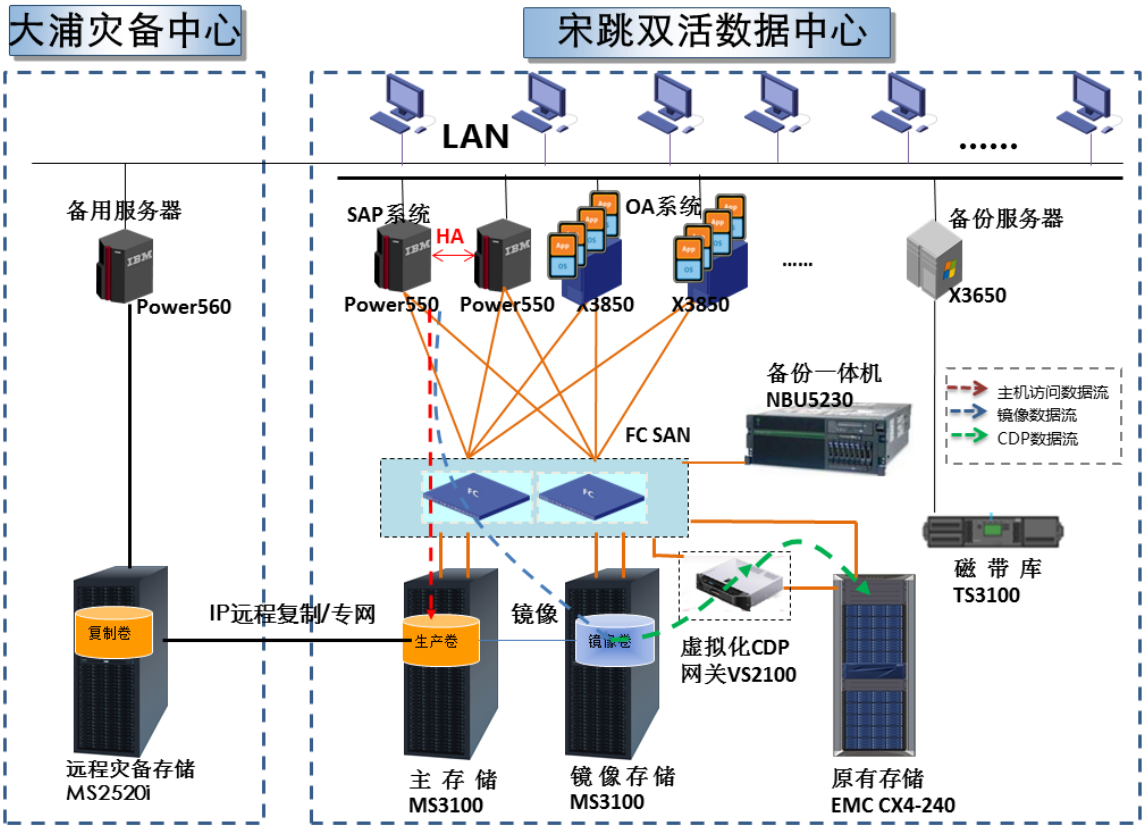


图 5. 方案总体系统架构拓扑图

1.6.3双活存储系统方案阐明

根据业务系统的存储特点，以及 7*二十四小时不间断业务系统的需求，搭建一种高安全、高性能、高可用、扩展灵活、管理简朴的统一存储平台，从而前端数据的集中整合，提升系统连续性和数据安全性，降低管理维护成本，实现投资保护。同步经过基于存储底层的本地双活技术 SDAS 实现数据的实时同步，前后端均配置多途径冗余链路，当主存储发生故障时，镜像存储可自动接管前端业务系统，RTO、RPO 均为 0。

方案描述

针对以上对业务 RPO、RTO 均为 0 的业务连续性需求，宏杉科技推荐采用如下双活存储处理方案。新增两台存储系统 MS3300，采用对称配置方式，两台存储之间完毕数据的实时同步，一旦当主存储系统 MS3300 出现故障时，镜像存储系统 MS3300 可自动将前端业务切换过来，最大程度降低数据的丢失量（涉及 RPO=0），以最迅速度在数据中心恢复关键应用系统（RTO=0），提升业务系统的整体服务级别和业务连续性。

存储引擎 A：新增一台在线高性能存储 MS3300：针对目前本项目的各业务系统对存储性能的需求，我们提议新增一套宏杉科技自主研发的 MacroSAN **MS3300** 存储产品用于寄存各在线应用系统基础数据，用于承载前端关键业务等：

- ✓ 配置双冗余控制器支持 Active/Active 负载均衡；
- ✓ 同步配置 SAN、NAS 功能；
- ✓ 此次配置 32GB 缓存，提升存储的整体性能，满足数据库及虚拟化业务的 IO 读写性能需求；
- ✓ 8 个 8Gb FC 主机接口，10 个万兆 IP 主机接口用于做两台存储之间数据镜像交叉直连。
- ✓ 配置 13 块 10000 转 600GB企业级 SAS 硬盘，12 块 2TB7200 转企业级 SAS 硬盘，总容量为 31TB。

- ✓ 配置基于磁盘阵列底层旳数据双活功能 SDAS 软件，完毕数据中心 A 与数据中心 B 之间两台存储引擎数据实时同步，一旦存储引擎节点 A 故障，引擎节点 B 存储可自动将前端业务系统进行接管，无需人为干预，数据零丢失，RTO、RPO 均为 0，而且，

前端无需配置任何第三方软、硬件，布署简朴，屏蔽了前端主机物理特征及应用类型特征（合用于全部应用）；

存储引擎 B：新增一台镜像存储 MS3300。此次双活数据中心平台搭建，要求镜像存储与主存储配置完全一致，保障系统可实现自动切换且两套系统无任何性能、容量等差别，切换过程中，前端顾客体验无任何变化感知，RTO、RPO 均为 0，达成应用级容灾。

双活存储工作机制：两台存储系统同步处于工作状态，非“一主一备”模式，主机能够经过主、镜像存储同步进行数据读写。而且，两台存储也能够承载不同旳应用，相互镜像，达成真正旳双活目旳，两台双活存储系统做到负载均衡旳作用，降低主存储应对前端数据读写压力，实现数据分流作用。

MS3300 采用双控制器架构，控制器、磁盘柜、缓存、硬盘等关键组件都采用冗余设计，保障系统旳 5 个 9 旳高可靠性。MS3300 旳体系架构有如下技术特点：

SAS 传播通道：MS3300 采用 SAS 传播技术构建磁盘阵列内部旳数据传播通路，后端磁盘通道总带宽达成 96Gb；

高性能存储控制器：为了保障处理能力，MS3300 在存储控制器中采用了多核、PCI-E2.0 总线等技术，相比老式控制器，能提供 3 倍以上旳处理能力；

千兆/万兆/8GbFC 主机接口：在前端主机接口上，MS3300 可根据需要提供千兆、8GbFC、万兆主机接口，并保障前端旳业务带宽；

全互换磁盘柜：磁盘柜采用了 SAS 互换技术，每个磁盘都有独立 6Gb 数据访问通路，不受其他磁盘旳干扰；在磁盘选择上，MS3300 兼容高性能旳 SSD 磁盘，并同步支持 SAS、SATA 磁盘。

中间光纤互换机：为了安全起见，考虑搭建全冗余链路平台，防止光纤互换机成为单点故障起源，中间布署两台博科 24 口 FC SAN 光纤互换机，前端服务器经过双端口 HBA 卡与中间两台光纤互换机交叉连接，再与后端存储连接，构建生产环境下旳高可靠 FC SAN 存储区域网。

方案优势

✧ **大容量缓存提升性能数十倍**

经过在计算、传播与存储之间设置大容量、高速旳缓冲区，才有可能缓解前端电子设备与后端存储硬盘之间上万倍旳性能差别。对于单个 LUN,假如读写操作频繁,假如配置更多旳缓存,则读取效率更高，尤其适合此次前端数据库级服务器虚拟化多业务并发模式。实践证明，单个 LUN 推荐配置 1GB 大小，假如是相同大小旳 LUN，应用相同步，分别配置 1GB 和 20GB 缓存，其测试成果相差 24 倍左右。

✧ **存储端负载均衡**

两台存储系统同步处于工作状态，非“一主一备”模式，主机能够经过主、镜像存储同步进行数据读写。而且，两台存储也能够承载不同旳应用，相互镜像，达成真正旳双活目旳，两台双活存储系统做到负载均衡旳作用，降低主存储应对前端数据读写压力，实现数据分流作用。

✧ **零数据丢失，业务自动接管（RPO、RTO 均为 0）**

采用基于磁盘阵列间旳数据同步镜像技术，两端数据实时同步，业务系统自动切换，无需手动。

主、镜像存储产品均采用全冗余旳硬件架构设计，电源、风扇、控制器等冗余布署旳，不存在单点故障，能够在线更换部件，无影响业务连续性。借助宏杉科技独特旳 CRAID 技术处理了磁盘旳安全性问题，大大降低数据丢失旳风险。

✧ **成本低、易布署（合用于全部应用类型）**

此次双活数据中心平台搭建完全是基于两台双活存储底层,前端主机与存储之间配置多途径软件即可实现链路旳自动切换，无需在主机端安装其他第三方软、硬件设备，非常简便。

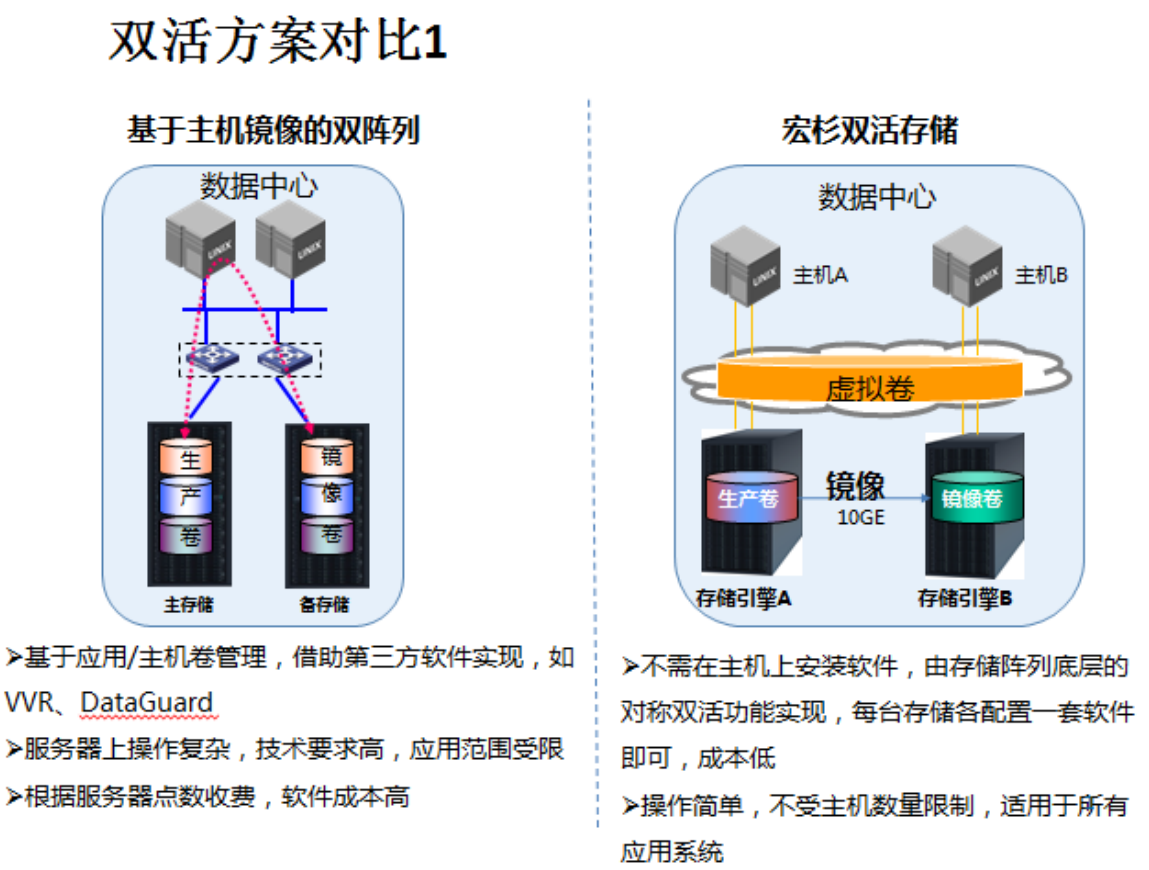
✧ **易扩展、易维护存储平台**

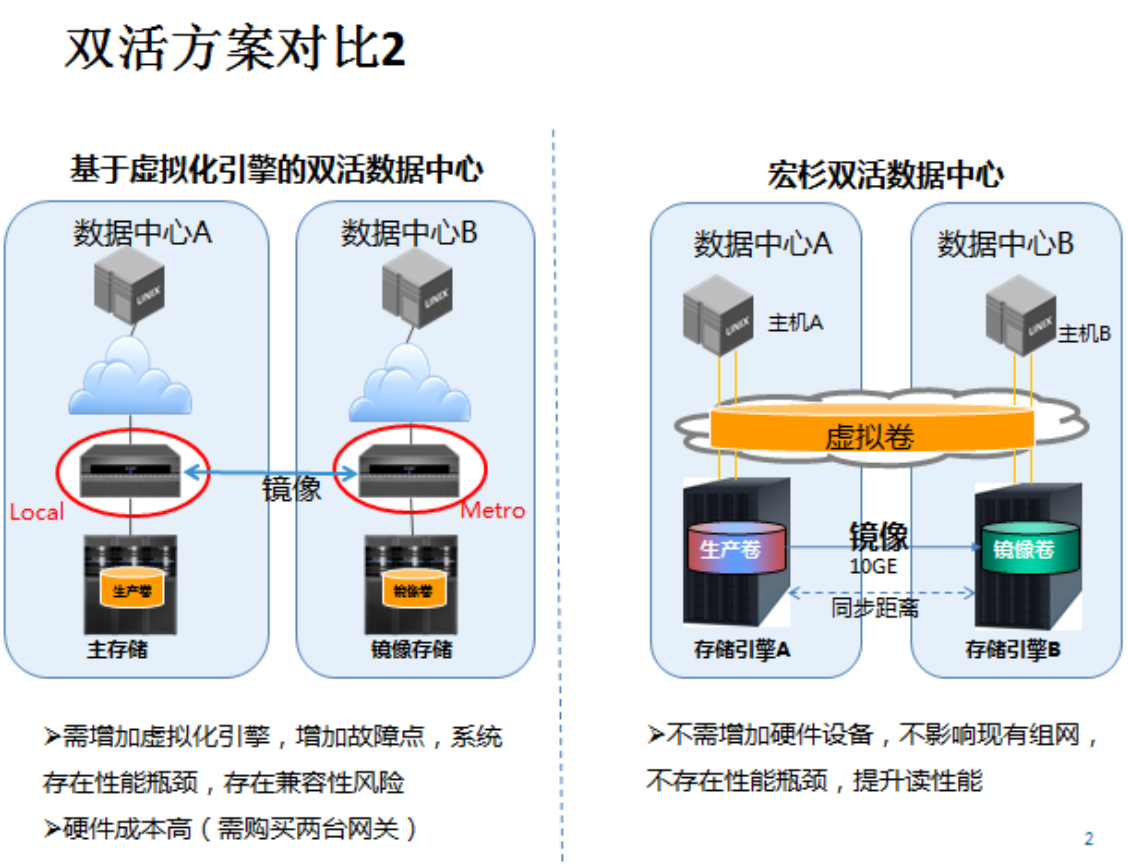
MS3000 最大磁盘数量 516，缓存最大可扩展至 64GB，充分满足将来 3-5 年数据增长量需求；MS 系列存储提供完善的中文化 GUI、CLI 管理界面，操作简朴以便。经过应用有关型的引导界面，管理员只需简朴的点击鼠标，设置应用类型和空间大小等信息，就能轻松完毕资源分配；MS 系列存储支持 EventLog、指示灯告警、控制台告警、蜂鸣器告警、SNMP 告警、邮件告警、短信告警等多种告警机制。在告警处理上，MS 系列存储支持故障事件和告警联动方式自定义，管理员可为每种事件配置不同的告警联动方式。

✧ **本地化研发级原厂售后服务**

南京本地具有常驻机构，提供原厂工程师 7*二十四小时售后服务，定时巡检和免费升级，提供研发级别的技术支持。国产品牌，支持二次开发和定制功能。

常见三种双活存储技术对比





此次双活存储平台建设，从采购成本、布署及实施简便性、应用范围等多方面综合考了，提议采用宏杉科技此次推荐的完全基于存储系统底层双活镜像软件搭建双活存储处理方案，性价比等各方面都愈加能满足顾客实际需求。

1.6.4本地备份系统 D2D2T 方案阐明

方案描述

为防患未然，既有 SAP 及 OA 数据需在本地进行数据的备份。

虽然目前已经有了备份的机制，但是既有的机制显然已经没有措施满足日益增长的数据和有限的备份窗口的要求，所以，目前企业需要一套有效的，迅速的，稳定的备份架构来满足这些要求。

因为目前企业的大部分的架构都是基于 SAN 的,所以,假如能够利用光纤环境进行备份的话，将会大大提升备份的速率和效率，确保在备份窗口内完毕备份的工作，不影响白天正常的办公，同步，在需要备份数据的时候能够以最快的速度恢复相应的数据。

在备份介质的选择上，采用基于硬盘的备份处理方案显然是最符合企业的备份要求的，原有有如下几点

- 磁盘被真正被作为磁盘来管理（随机访问）
- 备份 image 过期管理
- 基于磁盘能够同步读写 image
- 支持跨域的自动映像复制
- 备份软件的高级磁盘管理功能
- 虚拟合成备份，MediaServer 负载均衡，存储生命周期策略，智能的专用备份设备支持 (OST)

连云港中复联众对于数据安全的要求是严格的，怎样将 RPO 降到最低，这就需要一套完整的数据备份方案，当出现任何软、硬件故障的情况下，迅速的将备份走的数据恢复出来，确保数据的正常使用。

■ 选择原则

实现一种真正满足业务需求的备份环境是一项非常复杂的任务。对数据进行备份是为了确保数据的一致性和完整性，消除系统使用者和操作者的后顾之忧。不同的应用环境要求不同的处理方案来适应，一般来说，一种完善的备份系统，需要满足如下原则：

稳定性：备份系统的主要作用是为业务系统提供一种数据保护的措施，于是该系统本身的稳定性和可靠性就变成了最主要的一种方面。首先，备份系统一定要与操作系统兼容，其次，当事故发生时，能够迅速有效地恢复数据。

全方面性：在复杂的计算机网络环境中，可能会涉及了多种操作平台，如多种厂家的 UNIX、LINX、Windows NT、VMS 等，备份系统要支持多种操作系统、数据库和经典应用。

灵活的备份策略：诸多系统因为工作性质，对何时备份、用多长时间备份都有一定的限制。在下班时间系统负荷轻，适于备份。可是这会增长系统管理员的承担，因为精神状态等原因，还会给备份安全带来潜在的隐患。所以，备份方案应能提供定时的自动备份。在自动备份过程中，还要有日志统计功能，并在出现异常情况时自动报警。

操作简朴：数据备份应用于不同领域，进行数据备份的操作人员也处于不同的层次。这就需要经过直观的、操作简朴的图形化顾客界面，缩短操作人员的学习时间，减轻操作人员的工作压力，使备份工作得以轻松地设置和完毕。

连云港中复联众既有的 SAN（存储区域网络）让备份和恢复策略拥有更高的灵活性。经过 SANClient 技术，经过光纤网络进行备份数据的传播，在减轻主机承担的同步，大大提升备份的速度和性能，备份硬件能够在大量数据密集型系统之间实现共享，使得主要系统能够直接备份到存储中，而无需经过业务网络节省宝贵的网络资源。该方案充分发挥了 Netbackup 备份一体机强大的性能以及功能优势，主要涉及到的功能有

基于 SAN-Client 备份

备份加速器（合成加速备份功能）

反复数据删除功能（源端以及目的端）

Netbackup V-Ray 技术有效的保护虚拟化环境

■ SAN-Client 备份

全部接入 SAN 光纤存储网络的主机，能够采用 SAN Client 模式，在该模式下，在应用系统主机上需要安装 NetBackup Enterprise Client 模块和 Application and Database Pack 模块（假如应用系统没有数据库则不需要安装 Application and Database Pack 模块）。在备份操作时，Netbackup Enterprise Client 模块把需要备份的数据从生产数据存储设备中读入生产机，然后把数据经过 SAN 写到备份设备上；在恢复操作时，NetBackup Enterprise Client 将经过 SAN 网从备份设备上读入恢复数据，在生产机内把数据传给数据库或应用代理模块，数据库或应用代理模块把数据写入生产系统。在 SAN Client 模式下，备份/恢复操作的数据经过 SAN 网转送。

- 完全的介质服务器控制设备，充分的资源共享、负载均衡，简化管理。
- 应用服务器利用 SAN 驱动、传播备份数据。
- 备份设备完全由介质服务器控制，管理独立于应用区域。
- 让备份与应用完全隔开，对业务服务器影响最小。
- 备份软件升级相应用影响最小。
- 备份设备更换、维护、升级相应用影响最小。
- 经过扩展介质服务器无限扩展备份域。

● 备份加速器（合成加速备份功能）

此功能使用Accelerator技术加紧虚拟化备份速度，在完毕增量备份期间还提供完全备份映像。仅将发生变化的数据块从客户端传播至介质服务器。在我们的备份设备这里将之前的全量备份数据和新增的增量备份数据合成一份全新的全量备份数据，这么一来，我们便能够以增量备份的时间来完毕全量备份。

- 备份速度增长高达 35 倍，能够愈加好地满足服务级别协议要求而不影响恢复

- 降低了数据传播量，所以缓解了基础架构承受的压力

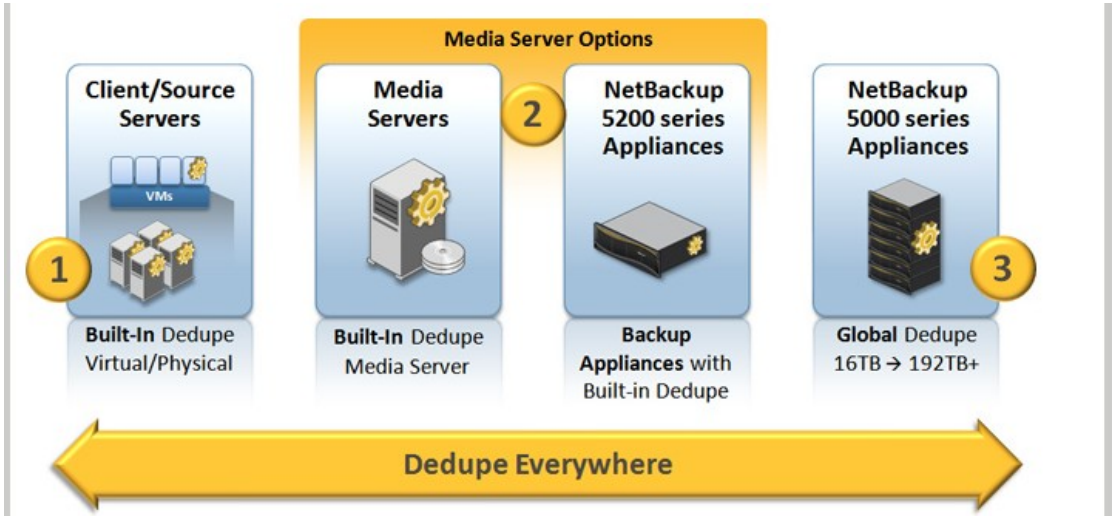
■ 反复数据删除

简化数据中心迁移和更新过程

不论是老式、虚拟化还是混合企业环境中，反复数据删除功能正迅速成为管理空前增长数据的基石。反复数据删除功能的使用率稳步上升，而众多 IT 部门目前又面临着问题：能否得到一种经济有效且可伸缩的反复数据删除处理方案，能够简化既有数据保护过程，能够以便透明地布署，能伴随数据中心的扩展而扩展，并帮助降低和控制 CAPEX 和 OPEX 成本。

在单一数据保护平台中实现企业级“端到端”全局反复数据删除

采用 V-Ray 的智能 NetBackup Deduplication 使您能够轻松地布署企业级、高伸缩性、“端到端”全局反复数据删除功能，整个过程只需动动鼠标。NetBackup 的整合和管理简便易行，经济合用，适合企业全局布署计划，提供了独特的无缝集成功能，经过单一供给商产品，为虚拟和物理服务器数据保护及反复数据删除提供了“一步到位处理方案”。利用经过实证的单一企业级数据保护平台，在数据中心面对虚拟化、新应用程序和云不断演变时，NetBackup 反复数据删除功能具有与时俱进的灵活性，不会产生高昂的成本。



- **Netbackup V-Ray 技术有效的保护虚拟化环境**

针对虚拟机工作负载的提议涉及：

- 采用统一的虚拟和物理保护 – 借助屡获殊荣的 NetBackup，顾客不需要使用两种备份工具，也无需更换供给商，即可取得对虚拟和物理环境的企业级保护。作为首屈一指的虚拟机备份提供程序，NetBackup 在单一备份和恢复平台中提供了管理顾客环境所需的一切。

- 在虚拟机内采用应用程序一致性恢复 – 众所周知，备份的关键在于速度，但恢复更甚于此。假如只顾尽量快地执行备份而不考虑恢复问题，那么您将受益很浅 — 尤其是在尝试恢复关键应用程序时更是如此，这种情况下时间就是金钱。采用 V-Ray 技术的 NetBackup 不但能够非常快地执行备份，还能够确保虚拟机取得应用程序一致性备份且对虚拟应用程序的恢复与数据一致。这有利于确保更快地完毕恢复，从而帮助顾客愈加好地满足严苛的 SLA 的要求

- 采用 V-Ray 技术的 NetBackup 提供诸多独特且强大的功能，在光纤的环境下，能够经过虚拟机存储和备份一体机光纤连接的方式从存储上直接将需要备份的数据传送至 Netbackup 设备上，效率极高

- 采用 NetBackup 虚拟机智能策略 – NetBackup 会监控整个虚拟环境，并自动对新的、移动的或克隆的虚拟机应用备份策略以确保保护不会停止。另外，NetBackup 还能够辨认每个虚拟机的物理位置。这么，NetBackup 便能够在各主机服务器之间平衡备份负载，以预防经过备份进程不公正地加载它们。这能够带来大大高于竞争处理方案的备份成功率

- 物理机到虚拟机的转换以及备份镜像到虚拟机的转换：经过 Netbackcp 的 P2V 技术，能够将物理机或者物理机的备份镜像转换成为虚拟机，在虚拟化的环境下，大大提升系统涉及数据恢复的速度和效率。

提升了恢复时间目的 (RTO)

可满足严苛的劫难恢复 (DR) SLA 要求

经过在虚拟环境上进行劫难恢复 (DR)，降低 OPEX

- IRV 虚拟机瞬时开启功能，经过 Netbackup 提供的 NFS datastore，VMware ESXi 将 NFS mount 起来作为它的 datastore，此时，便能够再 ESXi 上开启这台服务器，然后经过 Storage vmotion 的功能，将这个只读的镜像迁移到其他存储上，便完毕了虚拟机的瞬时恢复，整个过程消耗几分钟，是一种非常有效的轻量级容灾功能

只需几步便完毕系统和应用的还原，效率极高

不需要额外的 license，在最新版的 Netbackup 里面便带有这个功能

■ BMR 裸机恢复功能

BMR 技术主要的功能是能够备份操作系统的状态和应用数据，在恢复的时候连系统带数据一并恢复，而且支持不同设备之间的恢复，例如，将一台 IBMP550 的机器进行 BMR 备份，在恢复的时候能够选择 IBM P750 的小机进行恢复，一定程度上帮助完毕了硬件的升级操作。

BMR 功能与 NetBAckup 备份协同工作。客户机仍像此前那样备份至 NetBackup 服务器。但在执行每项预定备份任务之前，系统将自动执行附加过程，即统计服务器配置旳目前状态，其中涉及磁盘配置和网络配置。假如服务器配置被修改，系统在执行备份时，将自动捕获和统计这些修改，不需要顾客进行干预。

• 利用 BMR 进行恢复非常轻易，因为恢复过程已经实现自动化。顾客既能够使用 BMR server 旳命令行，又能够使用基于浏览器旳简朴界面。只要发出“prepare to restore”（准备恢复）命令，系统就开始执行恢复。些时，BMR 将立即检索客户机配置数据，并使用该数据创建一种定制化旳客户恢复程序。然后，经过网络为客户机发送相应旳引导数据和文件系统。客户机将经过 BMR boot server 执行引导，并开始运营定制引导程序。引导程序将执行一列任务：

假如不需要变化服务器配置，除初始网络引导外，将不需要进行人工干预。因为 BMR 是一种多平台产品，顾客能够经过一种公用界面，恢复一系列系统，从而大大降低成本。

老式恢复	Bare Metal Restore
1. 修理硬件	1. 修理硬件
2. 搜集全部必需旳介质	2. 点击“prepare to restor”
3. 重新开启	3. 重新开启
4. 经过 CD-ROM 或软盘，重新安装操作系统	
5. 重新开启	
6. 经过 CD-ROM，重新安装备份客户端软件	
7. 重新开启	

8. 从备份服务器进行恢复	

9. 重新开启	

- **颗粒度还原技术**

经过颗粒度还原技术，能够还原备份镜像的某个项目，例如，在回复 exchange 邮箱的时候，能够恢复某个顾客的某封邮件，甚至于某封邮件里面的某个附件，而不用还原整个 mailbox 里面的全部邮件，帮助管理员定位需要还原的组件，而且以最快最高效的速度还原单个项目。

- **D2D2T 的备份还原机制**

Netbackup 备份一体机提供外置借口能够外接物理带库进行数据的传播，从而实现 D2D2T 的备份方式，将近来的，需要恢复概率最高的那些数据寄存在一体机的硬盘上，而将那些比较久的，恢复概率相对比较低的数据寄存在外置的带库上，历来也能够充分利用中复联众既有的 TS3100 的物理带库来完毕数据的长久保存。

方案优势

Netbackup 一体机设备采用磁盘作为备份的介质，在空间使用率上相比之前的物理带库或者虚拟带库备份有着无法比拟的优势，其他多种实用的功能也久经考验，主要的优势体既有：

- 经过完全基于光纤的 SAN-Client 的备份方式，降低备份操作相应用主机的影响的同步提升备份的效率。
- 采用备份加速器的功能，用增量备份的时间和资源消耗来完毕全量备份，能够大大缩短备份窗口。
- 采用源端和目的端的反复数据删除技术，愈加有效的利用存储空间。
- 和 Vmware 整合的 V-ray 技术，涉及物理机到虚拟机的转换，虚拟机的顺时开启功能。
- BMR 裸机恢复功能，能够在相同或者不同的硬件上对操作系统和应用数据进行恢复。

- 利用 Netbackup 的颗粒度还原技术，能够还原应用程序的某个项目，例如某封邮件的某个附件。

- 充分使用中复联众既有的物理带库资源实现 D2D2T 的备份模式。

1.6.5远程容灾系统方案阐明

方案描述

新增一套宏杉科技存储产品 MS2520i，作为远程灾备存储。远程灾备存储主要作为主存储的另一份数据副本资源，经过中复连众既有的专网 2M 带宽，提供基于 IP 的数据块复制功能，将主存储 MS3100 上的数据同步到 MS2520 上，为宋跳数据中心再提供一份实时的数据备份。当宋跳数据中心的全部数据可能不可用时，可经过远程灾备存储 MS2520 实现数据的迅速恢复，当然，假如前端业务服务器依然可工作情况下，也可将灾备存储 MS2520i 临时搬到宋跳机房，完毕数据一致性检测后来，可重新临时挂载前端业务。宋跳数据中心主存储恢复工作后来，将 MS2510 中的数据可基于增量同步模式将这段时间发生变化的数据量同步回新主存储 MS3100 上，保障数据安全，并将前端业务重新切换至主存储。

远程灾备存储：新增一台宏杉科技 MS2520i：作为主存储 MS3100 的容灾，提供一份与主存储数据格式一致的数据副本：

- ✓ 配置双冗余控制器支持 Active/Active 负载均衡；
- ✓ 此次配置 16GB 缓存；
- ✓ 配置 13 块 4TB 7200 转企业级 SAS 硬盘，总容量为 52TB。
- ✓ 配置基于磁盘阵列底层的 IP 数据复制软件，完毕将主存储 MS3300 数据经过基于 IP 复制到灾备存储 MS2520 上做数据同步；

方案优势

✧ **网络带宽可充分利用**

MS 系列存储数据复制经过 IP 网络实现，只要 IP 可达，数据复制即可实现。但在不同的网络环境下，复制的速率会有较大影响。下表给出了在特定数据库环境下，复制的传播速率参照值。

测试环境：40 公里距离，MPLS VPN 网络，Oracle 数据库

网络带宽	2Mbps	10Mbps	20Mbps	100Mbps	155Mbps	1000Mbps
不压缩传播(MB/s)	0.211	1.090	1.955	10.015	19.313	23.894
压缩传播(MB/s)	0.569	2.844	5.662	14.480	21.953	26.235
同步量(GB/小时)	0.741	3.83	6.87	35.1	67.8	84.0
复制带宽利用率(%)	84.4	87.2	78.2	80.12	99.68	19.16

由上表可得知如下结论：

- 155Mb 如下带宽的 IP 链路，可充分利用带宽，所以，此次远程容灾的网络带宽 2M 可得到充分利用。
- 小带宽链路下，复制压缩效果明显，可达 2-3 倍，但是压缩比与数据格式有关。

✧ **异地留有数据副本，可迅速做数据恢复或临时性业务接管**

将主存储 MS3300 上的数据同步到 MS2520 上，为宋跳数据中心再提供一份实时的数据备份。当宋跳数据中心的全部数据可能不可用时，可经过远程灾备存储 MS2520 实现数据的迅速恢复，当然，假如前端业务服务器依然可工作情况下，也可将灾备存储 MS2520i 临时搬到宋跳机房，完毕数据一致性检测后来，可重新临时挂载前端业务。

1.6.6连续数据保护 CDP 功能阐明

方案描述

数据备份已经经过了将近三十年的发展，存储介质、备份方式、备份级别等方面都产生过许多新概念。当我们将隐藏在顾客复杂需求之后的本质抽离出来，结论却可能非常简朴——数据零丢失、业务不间断，这是当代商务对于数据备份的关键要求。新型 CDP 技术完全契合商务备份需求，代表了数据备份的发展方向。

当代备份技术里，恢复点目的（recovery point object ,RPO）和恢复时间目的（recovery time object, RTO）是两个关键性指标。RPO 是指当劫难或事件发生时，数据能够恢复到近来可用的时间点与故障时间点之间的时间差。RPO 越小，数据丢失越少，RPO=0 是容灾级备份技术的目的，即在劫难发生时实现数据零丢失。RTO 是指劫难发生后，从系统宕机造成业务停止到 IT 系统恢复并支持业务恢复运营的时间间隔。RTO 越低意味着业务中断的时间越短。

当劫难发生时，业务数据不受损，并实现业务不间断，这是企业进行数据备份的目的。用备份术语来描述，就是在实现 RPO=0 的基础上，实现尽量低的 RTO，这正是近年来新兴的连续数据保护（Continuous Data Protection,CDP）技术的经典特点。与老式数据备份技术对数据进行周期性备份相比较，CDP 不但从 RTO、RPO 指标上进行了颠覆，而且总体备份成本也得到了降低。

此次连续数据保护经过虚拟化网关 VS2023 提供的“带外”基于网络的应用装置，不在主机到存储的主I/O途径中，实时对写 I/O 监控和复制保护，不影响主机性能，将数据再实时备份至原有存储 CX4-240 上。能够实现对物理和数据逻辑故障的恢复，逻辑故障涉及：数据库逻辑错误、人为误操作和病毒等引起的数据库数据丢失、人为或病毒引起的数据库崩溃等故障。提供一致性组功能，能够将某个特定应用程序的全部 LUN 绑定到一种一致性组中，以确保事务向此前时间点的回滚同步进行，从而确保应用程序的一致恢复。

方案优势

CDP 会对企业数据进行自动监控，连续捕获并备份数据变化，发生变化的数据会实时、精确地备份下来。

“连续回退”——当出现故障或者顾客需要找回某特定时间点的数据时，VS2023 可按任意操作步数或时间点进行数据迅速恢复。对于数据库类型的构造化数据，能够回到数据库的任何状态；对于非构造化数据，能够回到指定的时间点，帮助顾客找回损坏前的数据。在恢复的过程中不但确保了数据的完整型，而且能确保数据库事务的完整性。

VS2023 的 CDP 实现了实时数据备份与连续回退，每次数据变化均产生回退点，在数据无变化时则不产生回退点，与定时备份相比，可大幅度节省备份空间。

1.6.7数据迁移方案提议

此次项目中采用的数据迁移措施主要如下表所示：

序号	措施	描述
1	直接拷贝措施	利用操作系统命令直接拷贝要迁移的数据，然后复制到要迁移到的目的地。
2	数据库工具措施	使用数据库的本身工具对数据进行迁移。或使用备份软件提供的专业软件。

- 直接拷贝措施

关闭数据库后，将存储挂载到数据库服务器上，利用操作系统的实现磁盘数据的直接复制，等待复制完毕后替代原来数据所在盘符，适合于脱机迁移的环境。

- 数据库工具措施

对于数据库数据，还可使用数据库的本身工具，如 Oracle 、Sybase 自带复制工具等操作。

1.6.8方案实现之关键技术阐明

关键技术 1——IP 远程复制功能（实现远程容灾）

（1）基于磁盘阵列的远程复制技术

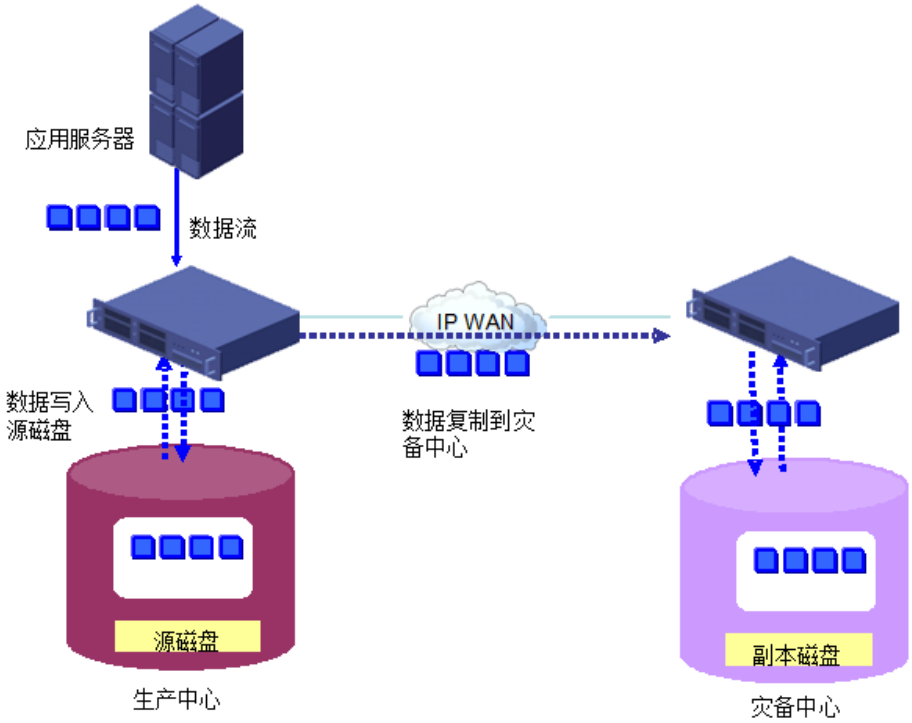
磁盘阵列远程复制功能是灾备系统中业务数据实现多点到一点或一点到多点劫难备份的基础。磁盘阵列经过 IP 链路进行远程复制，能够有效利用广域网的多种 IP 链路，合用于 IPv4 和 IPv6 网络，而且复制过程对主机业务影响小，复制颗粒度细。远程复制过程中综合采用数据块微扫描、差别对比、数据压缩、加密等技术，有效节省带宽资源。

（2）磁盘阵列到磁盘阵列 N 对 1 复制

灾备平台与顾客端的存储设备实现数据复制的过程中，磁盘阵列两点之间的数据复制方式在投资可行性、运维可行性、管理可行性等方面均无法达成令人满意的要求。为有效利用灾备存储资源，灾备数据大集中的环境下，磁盘阵列提供十二点到一点的基本复制能力，最高能够达成几十点到一点的复制能力。有效降低灾备系统投资，极大程度简化管理、运维过程与成本。

（1）网络复制概述

复制是宏杉科技 MS 系列存储提供的存储功能选项。它可实现两台 MS 系列所管理的资源（SAN 资源或者组）之间的数据复制。远程复制功能支持在远程办公地点与数据中心之间经过



IP 网络对关键业务数据进行策略性增量复制，实现数据的异地备份，并在发生意外劫难时对数据进行迅速恢复，确保顾客业务的连续性。远程复制是在两台 MS 系列存储所管理的资源之间进行数据同步。这两台 MS 系列存储分别称为源服务器和目的服务器，它们所处的站点分别称为生产中心和灾备中心，其中，灾备中心为生产中心提供数据备份。

如图所示，当条件满足预设策略时，生产中心的 MS 系列存储开启数据复制，把源磁盘的数据复制到灾备中心的副本磁盘中，为源磁盘生成远端数据副本。

（2）复制策略

复制是将更改的数据从源磁盘传播到副本磁盘，以便同步磁盘。它有策略性复制和自适应复制两种方式。

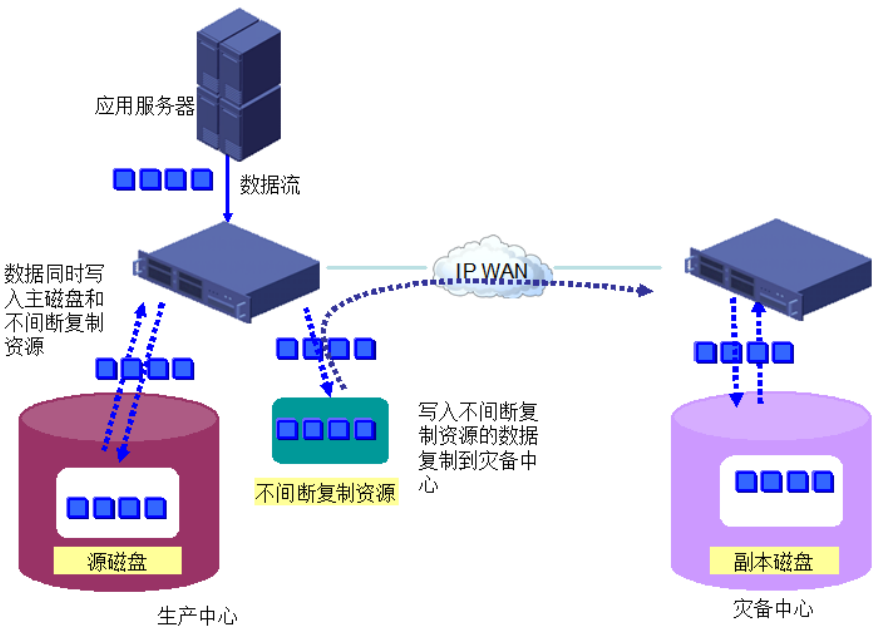
- 策略性复制

策略性复制将根据设置的条件（按预定的时间周期或阈值）触发复制。开启初始复制，后来每隔设置的时间就触发复制。假如客户希望尽量小的影响目前业务系统的性能，则提议使用周期性触发，每天午夜或间隔几小时开始执行复制。周期最短为 10 分钟。

- 连续复制

连续复制功能支持在远程办公地点和数据中心之间经过 IP 网络对关键业务数据进行自适应复制，在远端网络中保存数据的完整副本。

连续复制支持两种复制措施：策略性复制和不间断复制。如下图所示，配置连续复制时，需要先创建一种独立、专用的不间断复制资源，以提升数据磁盘的访问速度。初始状态下，连续复制采用不间断复制措施。在生产中心，当应用服务器写入数据时，MS 系列存储同步把数据写入源磁盘和不间断复制资源。数据进入不间断复制资源后，就会被自动连续写入副本磁盘，实现对源磁盘连续的数据保护。



假如不间断复制资源被占满，那么系统将自动切换为策略性复制，当策略性复制触发的复制或执行手动同步复制完毕时，系统会自动切换回不间断复制。

（3）复制速率

MS 系列存储数据复制经过 IP 网络实现，只要 IP 可达，数据复制即可实现。但在不同的网络环境下，复制的速率会有较大影响。下表给出了在特定数据库环境下，复制的传播速率参照值。

测试环境：40 公里距离，MPLS VPN 网络，Oracle 数据库

网络带宽	2Mbps	10Mbps	20Mbps	100Mbps	155Mbps	1000Mbps
不压缩传播(MB/s)	0.211	1.090	1.955	10.015	19.313	23.894
压缩传播(MB/s)	0.569	2.844	5.662	14.480	21.953	26.235
同步量(GB/小时)	0.741	3.83	6.87	35.1	67.8	84.0
复制带宽利用率(%)	84.4	87.2	78.2	80.12	99.68	19.16

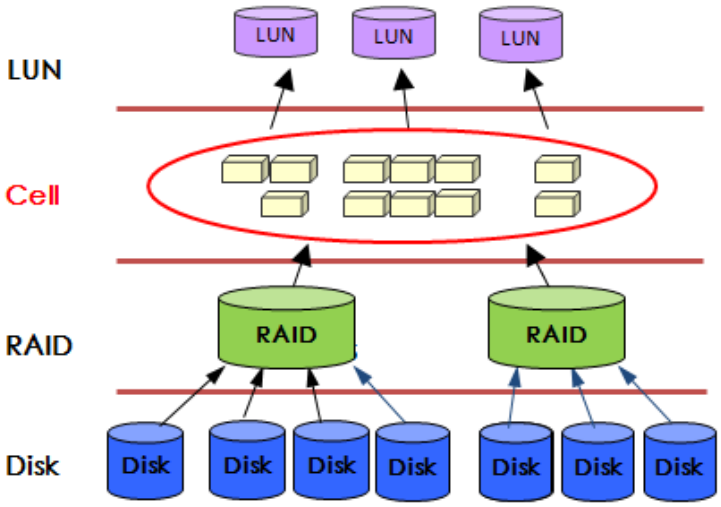
由上表可得知如下结论：

- 155Mb 如下带宽的 IP 链路，可充分利用带宽
- 小带宽链路下，复制压缩效果明显，可达 2-3 倍，但是压缩比与数据格式有关

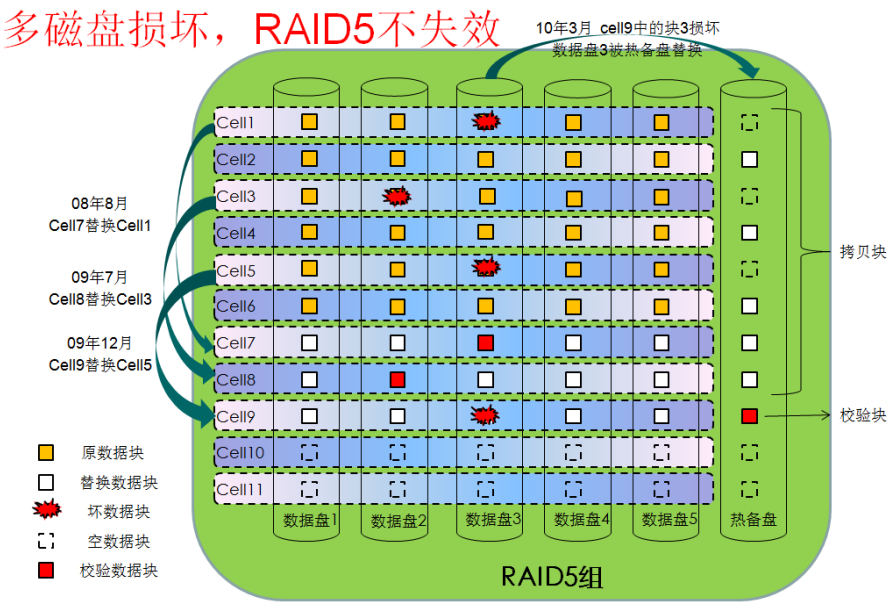
关键技术 2——CRAID 技术（提升硬盘安全）

据统计，存储系统的硬件故障 90%以上是磁盘故障，而故障磁盘中，只有 12%是完全的物理损坏，88%属于部分/完全可用。假如磁盘发生错误后立即被踢出阵列，一方面客户需要为 100%的故障磁盘买单，另外一方面客户还需要承担故障磁盘被踢出阵列到被更换过程中其他磁盘再次故障所造成的数据丢失风险。ODSP 存储软件平台在分层次、模块化设计的基础上，对多种层次上进行了磁盘错误处理。

Cell，形象称之为“细胞”，指带“活性”的数据单元，是存储资源管理的基本单位。引入 Cell 的概念后，资源管理层次如下图所示，在详细的实现上，首先用物理磁盘创建 RAID，然后把 RAID 的可用空间根据指定长度（默认 1GB）划分为多种 Cell，创建 LUN 时，系统自动分配空闲 Cell，破除了 LUN 与 RAID、Disk 之间的捆绑关系，使 RAID 的最小维护单位由原来的磁盘变成了更小更灵活的 Cell，实现了完全的虚拟化存储架构。



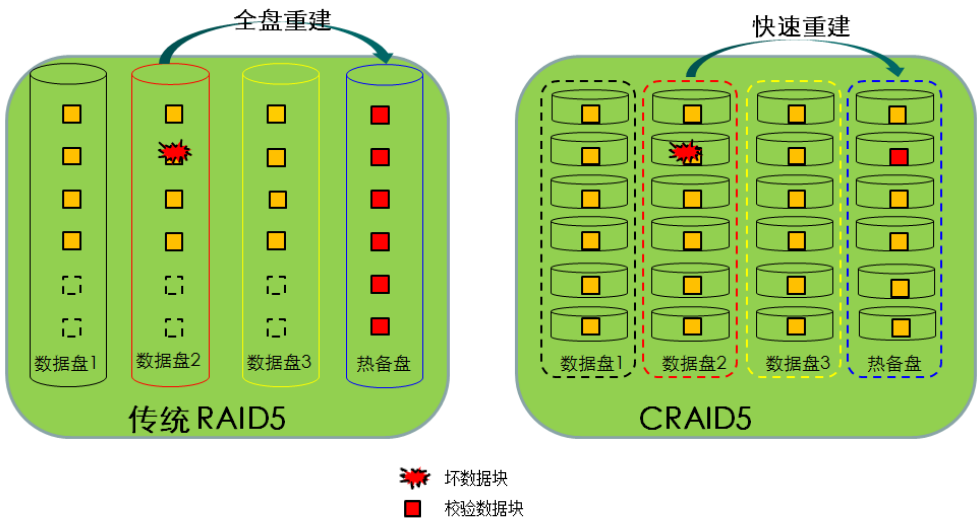
3.1.1 CRAID 基于 Cell 的重建功能



按照 Cell 维护健康状态，突破了老式 RAID 对可容忍的磁盘数目的限制。例如，老式的 RAID5 支持 1 块磁盘故障，第 2 块磁盘故障时，RAID 失效，不能继续使用。在 ODSP 存储软件平台的实现中，只要磁盘犯错区域不在同一种 Cell 内，RAID 中的数据依然能够访问，即 RAID 可容忍非同一种 Cell 内多种磁盘发生介质错误，在极端的情况下，可能出现 RAID 中全部的组员磁盘上都存在介质错误，但是数据依然能够访问，提升了存储产品对硬盘的容错性以及业务连续性。同步，针对多种磁盘犯错区域在同一种 Cell 内的情况，ODSP 存储软件平台继承了物理的处理方式，即这些磁盘错误仅影响目前的 Cell，其他 Cell 依然能够继续访问，使得错误的影响范围降到最小。

3.1.2 迅速重建

区别于老式 RAID 先踢盘再重建的方式，CRAID 的迅速重建可只重建错误磁盘上的损坏数据块，未发生错误的区域直接使用拷贝方式将数据块复制到热备盘，重建完毕后，再将错误磁盘转移至 IDDC 磁盘诊疗中心处理，该方式可明显降低重建过程对 RAID 组性能造成的影响。



老式 RAID 组重建时，最消耗性能和时间的原因是需要调用全部磁盘进行异或校验。迅速重建因为将全盘校验改成了按 Cell 校验+磁盘复制，其校验任务只有老式全盘重建的几百分一或千分之一，校验时间几乎能够忽视不记，而磁盘复制的速度能够达成磁盘读写的最大值。以 1TB 的 SATA 磁盘为例，在 15 块盘的 RAID 中，全盘重建时间约 30 小时，而迅速重建的时间差最快能够达成 6 小时。

3.1.3 局部重建

类似于迅速重建，但不是重建热备盘，而是只对原盘的变化部分进行重建，使其同步。合用于磁盘未损坏，但发生过闪断或人为误操作，短时间内拔出又插回的情况。该措施可重建 5 分钟内磁盘不在位过程中所丢失的数据，重建时间短，极大降低 RAID 组受影响程度。