浅论灾备系统在现代企业 IT 管理中的应用

张操
（国家电投集团贵州金元股份有限公司，贵州　贵阳　551800）

摘要：IT 信息系统成为企业经营发展重要支撑，发生灾难时数据快速恢复及灾备端服务安全可用是系统的重要任务，系统化规范地实施、管理灾备系统才能有效保障数据安全及服务连续性，即通过同步复制＋快照＋快照管理保证数据一致性，通过梳理业务依赖关系、灾备系统演练和切换、使用半自动化容灾管理辅助工具，保证容灾应急预案执行的安全性、高效性，以持续提高 IT 系统的服务质量。

关键词：数据保护；灾难备份；规范化实施；实施突发事件；容灾管理
中图分类号：F49;TP309　　**文献标识码：**A　　**文章编号：**1671-0711（2018）04（上）-0032-03

1　引言

现代企业基本都以集中部署分级应用的方式展开信息化应用，当 ERP 系统成为企业生产经营管理重要支撑时，信息系统和数据就成为企业核心资产，对数据实施连续性安全保护是必要的、迫切的，它是企业连续运作、规避风险、健康发展的要求，是企业进行全球化战略布局、成为世界级企业的要求，也是行业、法规遵从性的要求。通过一系列灾备系统的建设和计划行为，实现当关键系统发生灾难时能够快速恢复，实现无数据丢失的灾难保护，实现业务连续性目标。灾备系统涉及众多计算机技术及众多厂商的各类解决方案，所以容灾是一种科技含量较高的特殊 IT 运维管理，项目实施的关键，在于建立灾备系统有关的常态管理流程，建立配套应急管理预案，建立科学的人员、资源组织管理流程。

2　关键业务信息系统现状

企业 ERP 系统的应用、数据服务集中部署，建大集中应用承载数据中心，建基础网络，包括办公局域网、数据中心局域网、企业广域网，ERP 系统部署于企业数据中心，公司本部、所属单位广域网互联互通，本部通过办公网使用 ERP，所属单位通过广域网使用 ERP。ERP 系统应用现状参见图 1。

ERP 硬件系统主要是后端存储、前端服务器及用户网络，包括存储阵列、8Gbps FC 存储网络、10Gbit/s 以太网络，具体配置如下。

（1）数据库服务器由 2 台高配小机组成，2 台分别作为 Oracle RAC 的 2 个运算节点，运行 Oracle 10g RAC，通过 8Gbps FC 存储网访问共享存储阵列。（2）WEB 应用服务器由 2 台高配 x86 PC 服务器组成。（3）采用 Oracle 脚本逻辑导出的方式，每天备份 ERP 系统数据，同时存储在备份磁盘阵列及备份磁带库。

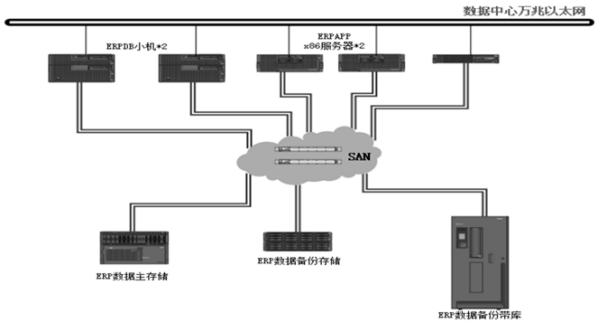

图 1　企业核心业务 ERP 信息系统拓扑

3　关键系统数据安全风险

（1）通过 Oracle 脚本进行数据备份，人工操作效率低，备份文件管理效率低，易发生备份文件错乱，无法保证数据恢复的准确性和高效率。（2）ERP 系统承载了企业生产经营财务等核心业务，灾难发生时 Oracle 脚本恢复数据需数小时，不能满足业务连续性要求。（3）由于脚本备份仅实现了数据备份，缺少裸系统和数据平台备份，灾难发生时需重建系统和数据平台，不能实现快速恢复。（4）存储存在单点故障，主存储发生故障会导致系统崩溃、数据丢失、服务停止，对企业生产经营造成极大的损失。没有灾难备用资源，不能短时间恢复系统运行。

4　关键系统数据灾难备份解决思路

针对以上关键系统存在的安全隐患和风险，分阶段体系化建设灾备系统，逐步提高并不断强化对关键系统的数据保护。

第一阶段：关键系统应用初期，业务量、数据量、访问量都不大，结合企业 IT 资源现状，确定一期灾备系统指标 RPO ≤ 2 小时，RTO ≤ 8 小时。

第二阶段：随着应用深度和范围不断扩大，业务量、数据量、访问量持续增加，信息系统逐渐成为企业生产经营的重要支撑，灾备系统的重要性凸显，在一期的基础上，二期灾备系统指标RPO=0，数据任意点时间恢复。

4.1 一期灾备系统建设

（1）建立自动化集中备份管理机制，采用专业备份管理软件，对关键系统的数据和环境，实现自动化、专业化备份，并同时保存在备份阵列和磁带库，还实现了对非关键系统的备份。（2）建立裸系统快速恢复环境，当ERP服务器发生系统错误崩溃不能启动时，可快速恢复系统备份映像。（3）建立灾难备用环境和恢复测试环境，当关键系统发生故障而短时间无法修复，备用环境可临时替代生产环境，恢复关键系统应用，备用环境也可作为备份恢复数据验证和灾难恢复演练使用。（4）选择美国赛门铁克（Symantec）公司的NetBackup作为一期关键产品，新增一台小机作为灾难备用硬件，同时作为AIX、Linux等异构系统的裸机恢复环境，一期拓扑见图2。

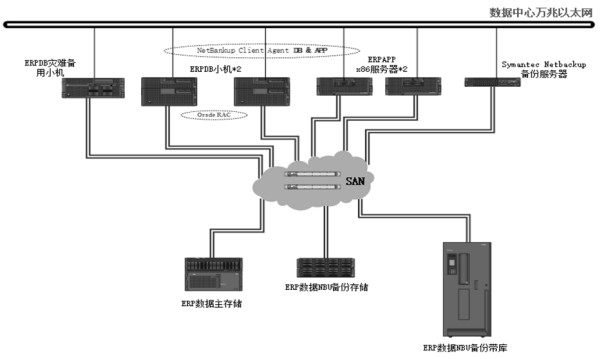

图2 企业核心业务ERP系统一期容灾项目建成

4.2 二期灾备系统建设

在一期灾备系统基础上，为达到更高级别的数据保护，更高的业务连续性，引入业界CDP技术的产品和系统实现，具有连续数据保护CDP功能的解决方案有：（1）磁盘阵列复制技术。（2）主机层复制技术。（3）数据库复制技术。（4）应用层复制技术。（5）第三方存储复制，系统通过同构或异构磁盘阵列来实现数据复制，同时提供数据复制管理功能。

采用解决方案4选型EMC RecoverPoint作为二期关键产品，并对一期系统进行运行调优，保持关键系统裸机恢复环境，保持非关键系统数据和操作系统灾备环境，并通过新系统同步复制+快照+快照管理功能保证生产端和灾备端的数据一致性。

（1）部署两套EMC VNX磁盘阵列，一对EMC RecoverPoint设备，新建EMC 8Gbps FC存储网，设备系统实现互联互通，实现关键数据的任意时间点无丢失，实现快速保存及可靠恢复。（2）ERP系统小机和应用服务器，一期备份服务器，一期数据备份存储和一期备份磁带库，接入新建存储网。（3）通过虚拟平台新建关键系统的临时生产环境，小机系统和OracaleRAC平台升级调优，EMC-ERP、EMC-CDP阵列和EMC RecoverPoint CDP统一接入EMC 8Gbps FC-SAN，一期项目中备份小机、备份服务器、备份阵列和备份磁带库统一迁移至新建存储网，新磁盘阵列导入历史数据，进行二期灾备系统的关键数据备份与恢复测试，二期拓扑见图3。

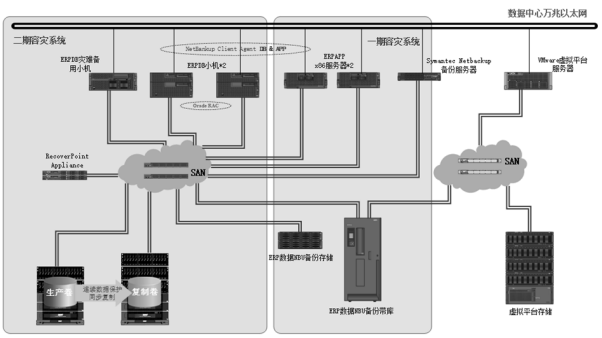

图3 企业关键业务ERP一期二期容灾系统建成

5 灾备系统实施

5.1 项目启动阶段

项目启动前充分做好组织和人员安排，同时充分做好项目涉及的技术准备工作，分解工作任务责任到人，并做到职责明确。一期和二期容灾系统建设都按以下原则进行项目实施的组织管理。

5.1.1 成立项目实施小组

负责项目实施风险和质量控制、方案审批决策和项目人员及资源组织管理。

5.1.2 项目实施方案审定

项目总体实施方案是整个项目实施的指导性、规范性、操作性文件，主要包括以下几点。

（1）实施总体任务目标（项目验收标准）。（2）实施进度计划（阶段验收标准）。（3）实施准备（软硬件环境）。（4）实施详细计划（项目进度计划细化）。①解决项目实施中存在的风险，如何防范和降低对业务系统产生的影响；②主要的实施操作步骤，细化到每一步的技术要求和操作说明；模块化测试和总体测试，明确方法和标准。

5.2 项目实施阶段

实施阶段按项目总体实施方案中的工作任务和工作计划执行，过程中履行工作日志、周工作总结制度，记录调试操作配置，监督项目进度，项目验收支撑材料积累。

项目总体实施方案对工作任务进行了系统、科学、合理的分解和安排，明确了工作职责，将工作任务分

解为关键任务和非关键任务，采取分模块独立实施，最后进行联合调试的策略，极大程度地减少和降低了实施安全风险和突发事件的发生几率。尽管项目总体实施方案中管理和技术内容具体详细，但实施过程中难免会与实际情况产生技术上的偏差或差异，比如集成商对实施产品的技术理解不够全面、准确甚至错误，或对 IT 实施环境调研不细，导致发生技术突发事件，如果影响方案中关键工作任务的执行，需立即终止项目实施，方案上会论证修订后再重启实施。如果仅影响非关键任务的执行，及时灵活进行调整变通即可。

表 1

序号	生产系统			现有数据保护措施			是否存在风险
	关键业务应用	系统平台	数据库 / 应用平台	裸系统	数据库 / 应用平台		
					应用程序	数据库文件	
1	ERP 数据库系统	IBM AIX	Oracle RAC	无	无	手工备份	高
2	ERP 应用系统	Windows		无	无		高

表 2

序号	生产系统			现有数据保护措施			是否存在风险
	关键业务应用	系统平台	数据库 / 应用平台	裸系统	数据库 / 应用平台		
					应用程序	数据库文件	
1	ERP 数据库系统	IBM AIX	Oracle RAC	BMR	NBU	NBU	中
2	ERP 应用系统	Windows		BMR	NBU		中

表 3

序号	生产系统			现有数据保护措施			是否存在风险
	关键业务应用	系统平台	数据库 / 应用平台	裸系统	数据库 / 应用平台		
					应用程序	数据库文件	
1	ERP 数据库系统	IBM AIX	Oracle RAC	BMR	NBU+CDP	NBU+CDP	低
2	ERP 应用系统	Windows		BMR	NBU+CDP		低

人为的突发事件情况比较复杂，主要分为人员变更、需求变更、IT 环境变更等，项目实施责任主体方人员变更，向项目组提交书面申请，审批后才能进行人员变更，须避免因人员变更时发生项目实施安全风险或突发事件；需求发生变更时立即对项目总体实施方案进行修改调整并上会审定；IT 环境变更导致不能按既定方案开展工作时，立即对项目总体实施方案进行调整，经实施小组上会审定后再重启实施工作。

我们在一期二期项目实施过程中，按上述管理和实施策略进行了具体实践，项目实施全过程规范化、标准化、制度化，保障了项目实施进度、质量，编制了总体测试方案并细化测试项目操作步骤，按项测试并详细记录，按标准流程进行了数据和系统裸机备份恢复测试，达到了项目预期。

二期项目实施中，在关键系统生产环境临时切换到虚拟平台时，数据库虚拟机产生性能瓶颈，虚拟机 CPU 负荷超 90% 并居高不下，无法正常支撑 ERP 系统应用，针对该突发事件，立即安排系统计划性停机，协调 4U ERP 应用物理服务器安装数据平台并导入业务数据，性能问题及时有效的解决，将突发情况对项目实施的影响降到了最小。

5.3 项目验收、竣工阶段

本阶段重点是项目培训，项目技术资料移交，协助编写项目运维管理制度。管理人员可进行原厂培训取证上岗。

通常需移交技术资料如下：（1）产品到货清单，安装调试清单。（2）项目实施方案。（3）项目过程资料，主要包括工作日志、工作周报。（4）项目验收报告。竣工资料还应包括项目合同，项目安装实施报告，项目测试方案，日常运维手册，产品手册相关资料，项目实施技术总结报告，及支持系统安全可靠运行的管理制度。

6 实施数据保护前后效果

（1）未实施数据保护存在风险（表 1）。

（2）实施数据保护后风险（表 2）。

（3）实施连续性数据保护后风险（表 3）。

7 企业灾备系统建设的展望

一期二期灾难恢复系统建设实施，结合长期管理运维实践，验证了我们所引入的技术、产品和系统，可靠性高、灵活性大，兼容性强、适应性好，在国内外中大型企业中都正在应用且具有成功经验。企业对灾难恢复系统是可管理的、可运维的。

参考文献：

[1]GB /T 20988 2007. 信息安全技术 信息系统灾难恢复规范 [S]. 北京 : 中国标准出版社 , 2007.

[2] 张冬 . 次世代数据存储思维与技术 [M]. 北京: 清华大学出版社，2017 ISBN 978-7-302-46492-1.

[3] 杨义先，姚文斌等 . 信息系统灾备技术综论 [J]. 北京邮电大学学报，2010(2).

[4] 施跃跃，徐景良 . 金融行业灾备架构高指标 RTO 的实现方式 [J]. 计算机应用与软件，2012(2).