# 论灾难备份与恢复策略

**摘要**

2007 年我有幸参加了 XX 人民银行电子同城实时清算系统的开发，担任项目经理一职，负责项目的系统分析和数据库设计等工作。该系统的建设目标是实现我市人民银行间资金清算业务电子化、实时化处理，解决手工清算交换速度慢、劳动工作强度大、资金使用效率低的问题。项目于 2006 年 10 月通过招标后投入开发，2007 年 9 月试运行，2008 年 5 月通过总行专家验收。

本文结合工作经历，简要叙述了项目概况，概述了数据库备份和恢复的重要性以及项目的数据库的备份与恢复策略。详细阐述了“冷备热备相结合、全量增量相结合、自动手工相结合”策略的具体实现方法和实施步骤，以及只有通过制定和严格执行相关制度，才能保证数据库安全性和完整性的体会。最后提出项目中数据库备份与恢复存在的问题及改进措施。

**正文：**

2007 年我有幸参加了 XX 人民银行电子同城清算系统的开发，担任项目经理一职，负责项目的系统分析和数据库设计等工作。项目于 2006 年 10 月通过招标后投入开发，2007 年 9 月试运行，2008 年 5 月通过总行科技部门领导和专家评审验收。电子同城实时清算系统由中心处理系统、网点处理子系统、前置机处理子系统、对接站处理子系统四个子系统组成，借助于金融数据通信网等计算机网络，连接同城交换中心和各同城票据网点，提供网内票据交换、电子联行往来账等业务的实时收发及资金清算服务，实现同城票据各交换网点之间的所有借记和贷记结算业务，包括支票的代收、代付，本票、汇票的代收，信汇、电汇、委托收款和托收承付的划回等，系统的建设对于防范和化解金融风险，促进地方经济发展，起到了重要作用。

在系统管理中，数据库的备份和恢复是一个日常性的工作，是维护数据库安全性和完整性的重要操作。备份和恢复是数据库管理员备份是恢复数据库最容易和最能防止意外的保证方法。没有备份，所有的数据都可能会丢失。备份可以防止表和数据库遭受破坏、介质失效

或用户错误而造成数据灾难带来的损失。恢复是在意外发生后，利用备份来恢复数据库的操作，尽快恢复系统正常运行。根据备份的时机不同，数据库备份可以分为热备份和冷备份两种策略。根据备份的数据不同，可以分为全量备份和增量备份。同时数据库的恢复可以采用日志记录等技术。

电子同城清算系统，由于项目所处的行业特殊性，数据库的安全性和完整性尤为重要，一旦发生意外，必须尽快恢复系统运行并保证数据库完整性，否则将会造成全市资金无法及时清算，带来巨大的经济损失，甚至导致地方性金融风险的发生。针对这种情况，我们采取了“冷备热备相结合、全量增量相结合、自动手工相结合”的备份策略，从而最大程度保证数据库的安全性和完整性。

一、冷备热备相结合

考虑到人们普遍对 UNIX 操作系统不熟悉，不易遭受病毒攻击和无须安装大量的系统补丁的安全性考虑，按用户要求，对数据库服务器我们采取了使用 INFORMIX 数据库，基于 IBMP630 服务器、AIX 平台的设计，运行 HACMP 技术对系统提供监测，并实现主备机的自动切换。在数据库存储方面，我们使用了磁盘阵列设计，对 4*72G SICI 硬盘做 RAID 1 实现数据库的热备份，当其中任意一块硬盘损坏都能够保证数据库的正常运行，虽然这样会降低数据写入速度，但同时提高了数据读取速度，重要的是数据安全性更高。

在日常工作中，使用磁带备份和异地备份方式实现数据库的冷备份。

二、全量增量相结合

全量备份是指对数据库的完整备份，包括所有的数据以及数据库对象。实际上备份数据库过程就是首先将事务日志写到磁盘上，然后根据事务创建相同的数据库和数据库对象以及拷贝数据的过程。由于是对数据库的完全备份，所以这种备份类型速度较慢，而且占用大量磁盘空间。根据系统数据的重要性，采取以月度为周期的全量强制双备份，其中包括数据库和事务日志，未完成全量双备份，则系统无法进入下个月度的状态。从而保证数据库遭到严重破坏时，可以通过使用数据库备份和事务日志备份将数据库恢复到发生失败的时刻，几乎不造成任何数据丢失，这是对付因存储介质损坏而数据丢失的最佳方法。

增量备份是指将最近一次数据库备份以来发生的数据变化备份起来，与完整数据库备份

相比，差异备份由于备份的数据量较小，所以备份所用的时间较短，采取以日为周期的增量备份。当数据库发生意外时，利用增量备份可以实现数据库的快速恢复，但是它却无法像事务日志备份那样提供到失败点的无数据损失备份。

全量和增量的备份与恢复相结合可以在有效保证数据库安全性和完整性的前提下，尽量减少工作量。

三、自动手工相结合

日常工作中经常碰到备份介质损坏而导致数据无法恢复的情况，通常是由于只对数据库做了单份备份，为了防止这种情况的发生，我们应该尽量采取双备份的方式，但双备份会加大工作人员的工作量，工作人员也因为存在侥幸心理而忽略了双备份的重要性，为此，我们专门设立了一台 PC 机，通过 FTP 计划任务的方式，每天凌晨 1 点，自动完成数据库服务器和 PC 机的数据库备份同步工作，减少备份工作量的同时，通过异地备份的方式实现了数据库的双备份。这一备份方法得到用户方项目负责人的高度赞赏和肯定。

“冷备热备相结合、全量增量相结合、自动手工相结合”的备份策略，从而最大程度保证数据库的安全性和完整性，但是这仅仅是策略和技术手段，只有有效实施才能真正避免数据灾难带来的损失。我们为用户制定了详细的应急方案，更重要的是用户方要根据备份策略制定严格的数据库备份和恢复方面的管理制度，并要严格执行，比如要定期进行存储介质的有效性检查和应急方案的演练等等。

定期数据备份可以在数据发生意外损失的情况下，进行灾难恢复，最大限度避免损失。通过我们一系列的数据库安全设计和备份、恢复策略，加上用户方严格的制度和执行，系统数据的安全性和完整性得到了有效的保障，对提高资金使用效率，防范和化解金融风险，促进地方经济发展发挥了重要作用，得到上级行、市政府和地方各金融机构的一致好评。该项目获得 2008 年 XX 银行系统创新创效成果一等奖。

回顾项目开发过程，我们在数据库备份和恢复方面也存在一些不足之处，如系统虽然实现了数据库服务器的热备份和磁盘阵列的 RAID1 设计，但主备机共享同一磁盘阵列，并没有实现磁盘阵列的备份，当磁盘阵列发生严重故障时，将为系统数据恢复造成一定的困难，并且会造成当日数据的丢失，在二期工程中，我们将搭建一台服务器，构造一个相对简单的数据库环境，利用 INFORMIX-ONLINE 实现数据库的异机实时备份，达到数据库的无损恢复。