

调度中心存储备份及容灾的应用模式探讨

董 宁，韦凌霄，张君毅

(北京电力公司调度通信中心，北京市 100031)

摘要：随着调度中心应用系统的不断发展，数据的安全性显得尤为重要。原有的硬盘、磁带备份方式越来越不适应当今大容量、高速、集中管理的数据存储备份要求。文中在调度中心实时控制和非控制生产系统在线运行的前提下，采用 SAN（存储区域网络）架构，LANfree 的备份与恢复技术，多级备份的机制，灵活的备份策略，实现了数据的安全备份、快速恢复和异地容灾，既大大提高了调度中心实时控制和非控制生产系统的安全性和稳定性，又有效地降低了备份系统的投资成本。

关键词：能量管理系统（EMS）；电力系统实时动态监测系统（WAMS）；SAN；LANfree

0 引言

随着电网规模的不断扩大，调度中心在电力生产中发挥着越来越重要的作用。为了向调度和其他生产部门提供准确、及时的生产信息，调度中心一般建有能量管理系统 EMS、电能量计量/计费系统（TMR）、电力系统实时动态监测系统（WAMS）、继电保护和故障录波系统等，不同调度等级的调度中心具有的系统有所不同。这些系统均属于实时监控或非控制生产系统，每天都采集和积累着大量的电网历史数据。这些数据是进行电网运行、管理、分析和领导决策的极为宝贵的生产信息资料。如历年来的负荷数据就是高级应用软件负荷预报的基础。历史数据越多越详尽，预报的准确率就可能越高。如何安全、可靠地存储备份这些数据，避免数据的丢失，就成为目前我们特别关注的问题。

在国家电网公司发布的《国家电网公司信息系统数据备份与管理规定》中指出：数据是信息系统的基础，是电力企业的重要财富，数据备份是保证数据安全的关键技术措施，是信息安全体系的主要组成部分。规定中还明确了数据备份的内容不仅仅是应用数据，还应包括操作系统、应用软件和系统数据。对于实时或准实时系统，系统的快速恢复、业务的持续性显得尤为重要。

1 存储备份技术的发展

九十年代以前，存储产品大多作为服务器的组成部分之一，这种形式的存储被称为或 DAS（Direct attached storage，直接附属存储）。随着技术发展，进入九十年代以后，人们逐渐意识到 IT 系统的数据集中和共享成为一个亟待解决的问题。于是，网络化存储的概念被提出并得到了迅速发展。从架构上来分，今天的网络化存储系统主要包括 SAN（Storage area network，存储域网）和 NAS（Network attached storage，网络附属存储）两大类。

网络附加存储设备（NAS）是一种专业的网络文件存储及文件备份设备，一个 NAS 里面包括核心处理器，

文件服务管理工具,一个或者多个的硬盘驱动器用于数据的存储。NAS 可以应用在任何的网络环境当中。主服务器和客户端可以非常方便地在 NAS 上存取任意格式的文件,包括 SMB 格式(Windows)NFS 格式(Unix, Linux)和 CIFS 格式等等。NAS 系统可以根据服务器或者客户端计算机发出的指令完成对内在文件的管理。

SAN(存储区域网)是指独立于服务器网络系统之外的高速光纤存储网络,这种网络采用高速光纤通道作为传输体,以 SCSI 的应用协议作为存储访问协议.将存储子系统网络化,实现真正的高速共享存储。SAN 通常由 RAID 阵列、磁带库、光盘库和光纤交换机组成。SAN 和服务器的数据通信通过 SCSI 命令而非 TCP/IP,数据是以数据块的形式访问。

DAS 和 NAS 的存储方式,由于受容量、数据传输率、网络带宽等问题的影响,而且性能和可扩展性方面存在不足,从发展的趋势看,未来的存储会向着 SAN 的存储方式靠拢。

2 系统数据存储备份的现状存在的问题

2.1 系统数据存储备份的现状

目前的实时监控系统或非控制生产系统为了提高系统可靠性,大多采用双网双机热备用方式,对于主要服务器均采用双机容错技术、集群(Cluster)技术,避免因系统单点故障(如硬盘损伤)导致整个计算机系统无法运行,实现计算机系统高可用性。数据通过磁带机备份。

2.2 存在的问题

(1) 热备份方式并不能解决像操作人员误删除造成数据丢失这样的问题,因为热备份系统为保证数据的一致性,会定时同步双机的数据。一旦误删数据,则不能恢复。

(2) 备份介质磁带的可靠性较差,难以保存,容易失效。所用磁带机存取速度太慢,备份一次数据所需时间太长。

(3) 数据存储备份方式接近手工,难以满足数据的高效在线备份的需求。

(4) 主机操作系统、应用系统的备份、恢复采用手工方式,这种现状的严重后果是:一旦由于硬盘故障造成操作系统或者应用系统不能正常运行,恢复需要很长的时间。恢复期间,势必影响作业的连续性,甚至造成整个系统停止运行。

(5) 系统缺乏异地容灾功能,不能防范来自非计算机系统因素的隐患,如火灾、地震等灾难。

从以上的问题分析中,我们可以认识到调度中心各应用系统的设计方案中如果没有相应的数据存储备份解决方案,就不算是完整的系统方案。计算机系统不是永远可靠的。双机热备份、磁盘阵列、磁盘镜像、数据库软件的自动复制等功能均不能称为完整的数据存储备份系统,它们解决的只是系统可用性的问题,而计算机系统的可靠性问题需要完整的数据存储管理系统来解决。因此,对原系统增加数据存储备份管理系统和在新建网络方案中列入数据存储备份管理系统就显得相当重要了。

3 存储备份容灾系统的设计原则

(1) 由于调度中心的生产系统多为实时或准实时在线运行系统,数据的备份不能影响系统的运行。这意味着数据的传输不能通过原有的以太网,以免造成实时网络的瘫痪。

(2) 有效、集中地管理众多系统分散的数据。对于一个调度中心,建设一套规模较大的存储备份容灾系统实现多个系统的数据备份问题是比较好的选择。那么,这套备份系统必须能够接入不同的平台和不同

的主机，实现数据的有效、集中管理。

(3) 数据的安全性。数据在装入、访问、卸载、存储等过程中要最大限度地保证其安全性，不能因为主机，网络或存储设备的偶发故障造成灾难性的丢失。

(4) 灵活方便的系统扩展能力。随着电网规模的不断扩大，调度中心所采集的数据量也将不断膨胀，为了适应存储容量的爆炸性增长，整个系统要有灵活方便的扩展能力，以适应整个系统的变化。

所以我们建设的备份系统不但要完成数据的存储，管理，共享，以及备份等应用要求，还应对数据的安全性，系统的完整性，先进性，扩充性，可靠性，以及可用性等加以考虑。

4 解决方案和备份系统具有的功能

4.1 解决方案（见图 1）

采用 SAN 存储区域网技术来构建调度中心的存储备份容灾系统，SAN 以其独有的高速、稳定、兼容性高等特点极好地满足了实时系统的相应需求。SAN 核心技术是 SCSI-3 协议和 Fibre Channel 光纤通道，目前 SAN 数据传输速度已经达到了 100Mbit/s。SAN 技术具有以下特点：①大容量存储设备数据共享；②高速存储设备通道；③灵活的存储设备配置；④兼容以前的存储设备；⑤数据的高可靠性和安全性。

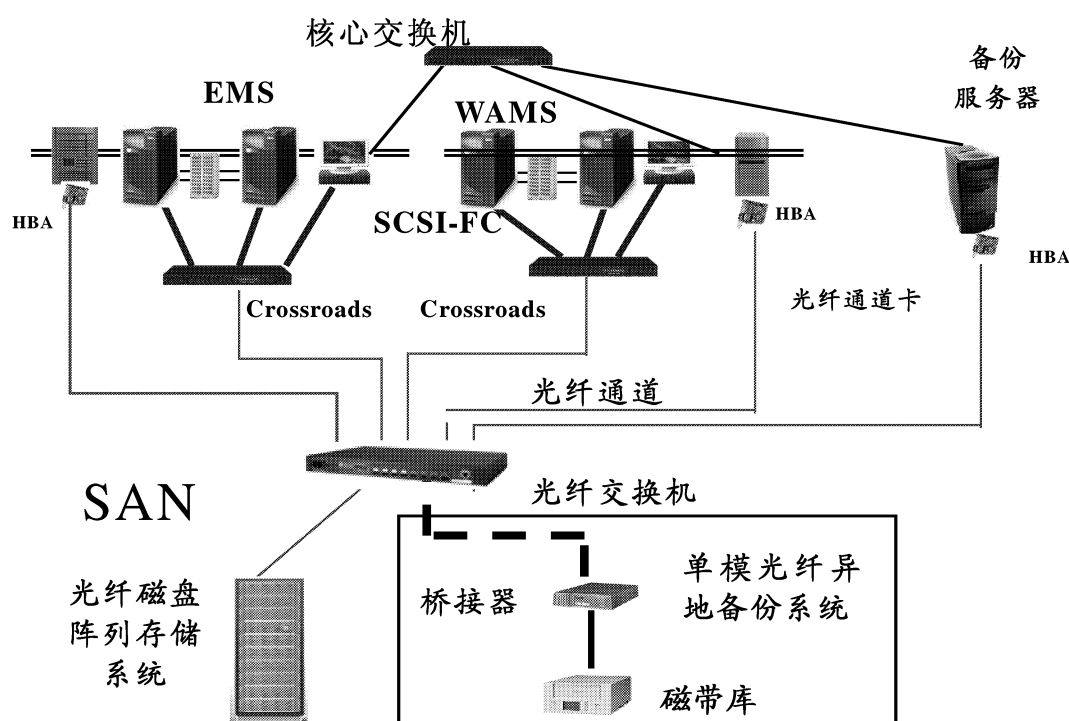


图 1 数据存储备份容灾系统拓扑示意图

基于 SAN 的 LAN-Free 数据备份。LAN-Free 备份模式其核心是利用存储局域网中所有的服务器都与自动带库建立了硬件连接的特点，共享磁带库，在备份时就好像是服务器直接通过光纤通道将数据传送到自动带库，而无需像传统的网络备份，先将数据通过局域网送到备份服务器，再由备份服务器传送到自动磁带库，从而在充分利用存储局域网高带宽的同时释放了实时网络宝贵的带宽。这对于保证实时系统的稳定

运行有非常重要的意义。

建议的软硬件配置:

(1) HBA。光纤通道适配器安装在主机上, 类似于网卡, 主机通过它来同 FC-AL 连接起来光纤通道适配器支持不同的操作系统: Windows、HP TRU64、SUN Solaris 和其它的一些操作系统。

(2) 光纤交换机。应提供多个独立的全线速转换千兆位交换端口, 转换带宽高, 支持 Fabric 功能。提供光纤交换机管理软件。采用第三代专用环交换技术-Stealth 3。提供即插即用的标准接口, 具有突出的可靠性和灵活性。是 SAN (存储区域网) 系统中重要的连接设备。

(3) 全光纤通道磁盘阵列。内外部均为光纤结构, 支持 RAID0, 1, 5 校验并由用户选择。支持在线热插拔, 可在线替换故障部件。支持 100Mbit/s 标准光纤接口, 支持热插拔光纤 Bypass 功能, 对主机及操作系统 Plug & Play, 无须任何驱动程序, 具备完善的磁盘阵列管理软件包, 并可由系统操作员进行监控、设置、维护及电源、风扇等部件设计为冗余并可热插拔。

(4) 带库。主要由库体、磁带驱动器、磁带槽位、磁带交换口、控制面板、机械手和电子控制单元组成。库体内的大部分空间用于放置磁带, 一台或多台驱动器安装在库体内专门的位置, 用于读写磁带。带库工作时, 机械手在管理软件和电子控制单元的控制下移动, 通过安装在机械臂上的条码读取器寻找相应的磁带, 然后将其抓取到驱动器内; 读或写操作完成后, 再由机械手将磁带取出, 放回磁带槽位。

(5) 桥接器。桥接器分为正向和反向。反向桥接器又称为反向路由器, 实现 SCSI-FC 的转换功能, 可将不能安装 HBA 卡的主机, 以 SCSI 接口的方式连入 SAN 的光纤存储设备。推荐产品是 Crossroads 公司的 SA 40。正向桥接器实现 FC-SCSI 的转换功能, 可将 SCSI 的磁带库接入光纤交换机。

(6) 备份软件。随着数据的重要性日益体现, 备份技术也发展很快。各种备份软件也可以说是种类繁多, 但总的来讲现在市场上形成主流的主要有 Legato Network、Veritas Netbackup, CA ARCserve, BackBone Netvault, IBM TSM、HP Omniback 等产品。当前的各种备份软件可以说各有利弊。我们可根据需求分析以及集成商的经验选择适合的备份软件作为方案的核心软件备份平台。

4.2 备份系统的主要功能

4.2.1 快速备份和恢复

数据备份的最终目的是为了恢复。新的备份系统中最重要的是在运行系统出现故障的情况下可以快速恢复系统。这就要求备份系统本身应该有一份实时可用的系统可以供生产系统使用。由于备份采用了系统备份方式, 系统中所有的数据都在备用磁盘阵列上统一存放, 一旦操作系统、数据库、应用系统和应用数据出现故障可直接从备用系统引导, 恢复作业运转的操作方式十分简单, 只须下一个引导命令, 从而恢复故障系统。

4.2.2 多级备份机制

对于调度中心的实时或准实时在线运行系统, 如果数据对象 (操作系统、数据库、应用系统和应用数据) 丢失, 后果非常严重。因此建立多级备份机制非常必要。我们设计的备份系统采取二级备份机制。即一级备份到专用磁盘阵列, 一旦主机内的硬盘系统发生了故障, 该磁盘阵列应能立刻代替主机内的硬盘, 在比较短的时间内重新启动业务。与此同时该系统还有二级磁带库备份, 在主机硬盘与磁盘阵列同时出现故障时, 保证能够完整的从二级磁带系统恢复, 从而确保系统数据的完整。

4.2.3 LANfree 的备份与恢复数据

因为要建立多级的备份，实际在网络传送的数据量是现有数据量的几倍。这就对网络的带宽和网络协议的效率提出了要求。调度中心各系统使用的是专用网络，网络上的数据都是电力实时采集数据，在这种情况下网络的数据带宽显得十分重要，而要实现数据的集中备份与管理，必然要在机器之间（Client-Server 架构）传递大量的备份数据，特别是多级别的数据备份。我们构建的 SAN 备份系统是专用的存储网络，LANfree 的数据传输，不占用应用网络带宽。

4.2.4 异地的磁带备份

在实现多级备份的同时，为了提高数据的安全级别，该存储备份系统的二级备份子系统放置在异地，避免因火灾等灾难发生时造成损失。

4.2.5 数据库的 Online 备份

商用数据库系统是调度中心的各个系统中极为重要的组成部分，大量的历史数据、系统参数等均保存在商用数据库中，以供查询、检索和分析之用。主流商用数据库一般有 Oracle、Sybase、SQL server 等，下面以 Oracle 为例介绍数据库的备份。由于 Oracle 数据库的数据一致性由 Oracle 维护，而不是操作系统，所以针对数据库的在线备份，其备份方式一般都要采用数据库自己的接口进行备份与恢复。

此次的备份方案中针对数据库系统共有两种备份方案可供选择，一是采用经典的备份软件挂接数据库备份插件的方式运行，采用这种软件备份的优点是造价低，接口统一，可以与系统数据以及其它数据一起纳入备份作业。缺点是备份速度相对较慢，所备份出来的 Oracle 数据无法直接打开，必须要恢复数据后才能演验证数据备份的正确性。

另一种采用了更为先进的 DSG 公司一体化数据存储管理平台中的 SnapAssure 磁盘备份技术，可以实现 Oracle 数据库在无归档方式下进行在线备份。采用 Snapissure 软件对 Oracle 数据库备份优点是可以对数据库采取更加灵活的备份策略，备份的数据可以随时打开，随时验证数据备份的重要性，而且还可以用来作为查询使用，同时备份与恢复速度都相对较快，可以在更短的时间内恢复数据库系统。但是系统相对于经典的备份软件造价相对较高。

5 备份策略

5.1 备份流程

首先磁盘阵列为每台服务器提供一个分区做逻辑盘。将服务器系统盘自动定时备份到相应分区，该操作作为一级备份。当本地硬盘故障时，可以使用光纤磁盘阵列中该工作站的逻辑盘立刻重新引导系统，恢复前台应用作业的正常运行。

5.1.1 一级备份过程

- (1) 接服务器在光纤磁盘阵列相应的逻辑盘；
- (2) 本地硬盘的所有信息备份到光纤阵列的相应分区。

5.1.2 二级备份过程

- (1) 务器将光纤磁盘阵列中的文件系统卸载；
- (2) 份服务器安装光纤阵列上的文件系统；

(3) 过备份服务器上备份软件, 按照事先配置好的备份策略将服务器在光纤磁盘阵列中逻辑盘数据备份到二级磁带库系统, 备份模式为 LANfree。完成二级备份后, 备份服务器放弃对光纤磁盘阵列上相应逻辑盘的管理权。

恢复时, 服务器直接安装磁盘阵列相应分区的文件系统, 对本地盘复制即可。系统备份流程图如图 2 所示。

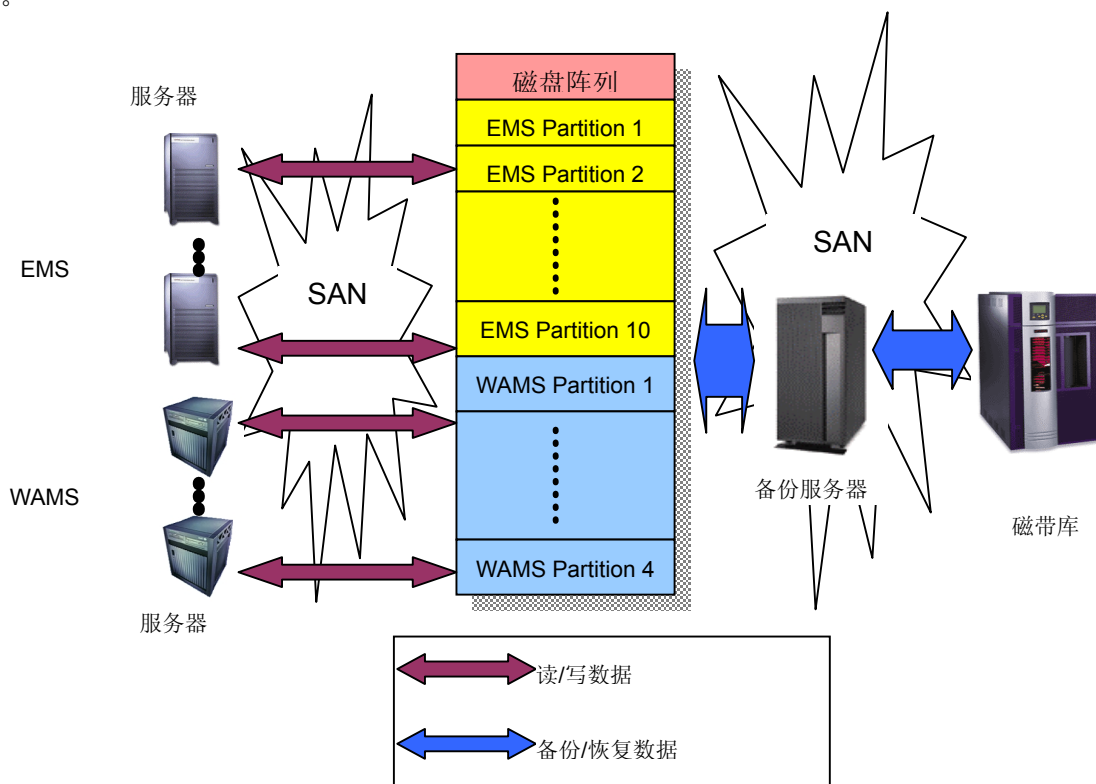


图 2 系统备份流程图

5.2 备份策略的选择

对于不同的系统、不同的业务和数据可采取不同的备份策略。如能量管理系统 EMS 中, 各服务器和工作站的操作系统和应用软件在安装运行后, 一般不再变动。可采用一次全备份的策略, 之后不再备份; 如有修改, 则再进行备份。对于历史数据, 可采用交替进行全备份和增量备份的策略, 实现数据的安全。

在备份时间的选择上, 由于备份任务会占用系统开销, 可考虑安排在夜里工作不忙时进行。不同的备份任务可安排在不同的时间, 以减少数据网络传输的负载。

6 几点说明

由于调度中心的各个应用系统所采用的软硬件平台都不相同, 如 EMS 大多采用 HP ALPHA 机型, 配有 HP TRU64 操作系统, 也有采用 SUN 公司的软硬件的。众多的平台如何平滑地接入同一套存储备份容灾系统, 是我们在作备份方案时应该着重考虑的。虽然厂商大都宣称自己的产品能够兼容其他平台, 我们也要事前搭建实验环境, 确切地验证可行性。

在本方案中, 由于备份服务器与所要备份的客户端之间需要有网络通信, 因此, 不同的系统之间有可

能因为光纤交换机和同一备份服务器而存在物理连接，这会带来一定的安全风险。根据《全国电力二次系统安全防护总体规定》的要求，调度中心的各个应用系统分为不同安全等级的 4 个安全区，安全区 I、II 和安全区 III、IV 之间实行严格的安全隔离，而安全区 I 与 II 之间为逻辑隔离。对于所采用的 SAN 光纤备份系统，数据备份是通过 SCSI-3 协议而非 TCP/IP，可认为不存在安全问题。备份控制命令是通过以太网传输，可考虑通过交换机的 ACL 控制或防火墙来保护实时监控系统的的功能。因此，建议安全区 I、II 的应用系统可共用一套存储备份容灾系统，通过相应的配置，既可保证数据的安全，又可避免产生新的网络安全问题。

7 结语

笔者提出的在调度中心的实时监控和非控制生产系统中共用一套 SAN 架构的存储备份容灾系统，既可以保证数据的安全性和可靠性，又可有效地降低备份系统的投资，其应用模式在具备条件的调度中心有一定的参考和推广价值。

参 考 文 献

- 1 Marc Farley. SAN 存储区域网络. 2nd ed. 北京机械工业出版社, 2001

董 宁(1970—)，男，硕士研究生，高级工程师，北京电力公司二级工程师称号，主要研究方向为调度自动化系统、计算机网络、网络安全和存储备份等。

韦凌霄(1974—)，男，硕士研究生，自动化处处长，主要从事调度自动化管理工作。

张君毅(1977—)，男，本科，助理工程师，主要从事调度自动化工作。