量值传递业务管理系统容灾备份的研究与实现①

张 明, 李 丽, 刘羿彤

(中国计量科学研究院 信息中心, 北京 100013)

摘 要: 随着信息技术在量值传递体系中的深入应用, 量值传递业务管理系统的数据安全成为了量传体系顺利开展的关键因素. 从中国计量科学研究院量值传递业务管理系统容灾备份的需求出发, 结合业务实际情况分析研究, 提出了一种不同于以往的实现方式, 实现对数据的集中备份和快速恢复, 从而保障了量值传递的安全进行.

关键词: 量值传递; 虚拟带库; 容灾备份; RTO; RPO

Research and Realization of Data Backup and Disaster Recovery on Quantity Value Dissemination Business Management System

ZHANG Ming, LI Li, LIU Yi-Tong

(Information Center, National Institute of Metrology P.R.China, Beijing 100013, China)

Abstract: Along with the IT technical development application in quantity value dissemination system, data security of NIM MIS is the key factor in quantity value dissemination. In this paper, based on the demand of NIM MIS data backup and disaster recovery programs, combined with the actual situation of business, point of a different solution. By this way, we could realization data backup and quickly recovery, the quantity value dissemination could safety develop.

Key words: quantity value dissemination; virtual tape library; backup and disaster recovery; RTO; RPO

量值传递是统一计量器具量值的重要手段, 是保证计量结果准确可靠的基础[1]. 基本物理量准确地从基准传递至计量机构, 保障了我国国防、贸易、国民生活等秩序的正常进行. 中国计量科学研究院自 2008 年开始自主研发了量值传递业务管理系统, 对我院的计量基准、标准、标准物质信息进行实时动态管理并对量值传递业务流程进行业务管理, 为计量检定工作和计量资源的配置提供实时的数据支持. 由于该系统数据的重要性, 就需要通过一定的安全机制, 使之在灾难损害发生后能够保障信息数据安全, 并尽快恢复应用系统使用, 最大限度地提供和保障应用服务.

1 需求分析及研究

1.1 量值传递业务管理系统特点

量值传递业务管理系统分为两大部分, 一部分为我院业务能力数据动态维护, 另一部分为量值传递业务管理. 该系统具有以下几个特点:

(1) 数据类型多样. 我院现有国家计量基准 127 项, 标准 258 项, 有证标准物质 1062 种(一级 354 种, 二级 708 种), 国际计量局(BIPM)公布的国际互认的校准和测量能力 1011 项, 量值传递业务管理系统需要动态管理这些业务能力相关的大量 word、pdf 及图形文件.

(2) 系统结构复杂. 量值传递业务管理系统分为 CS 及 BS 不同部分组成, 还拥有多个自处理程序同时运行. 所有子系统均需要 7*24 小时不间断运行.

(3) 数据增长迅速. 我院每年开具的检定证书存储量巨大. 从 2009 年本系统上线以来, 每年都有十几万份证书生成, 数据每年增长约 50G.

(4) 我院信息系统一直在建设, 不断与业务管理、

① 收稿时间:2012-06-08;收到修改稿时间:2012-07-18

人事管理、科技管理、财务管理及固定资产管理等相关业务流程紧密融合. 在 “一数一源”的原则下, 系统需保证各项业务数据的准确性和真实性[2].

1.2 现有网络环境

量值传递业务管理系统由 7 台服务器构成, 包括运行业务数据库的数据库服务器 A, 运行文件数据库的数据库服务器 B, 程序发布及网站系统服务器, PDF 转换服务器, 外网数据填报服务器, VPN 系统认证服务器, 备份恢复服务器. 所有服务器均配置双网卡, 在两个不同网段中运行.

1.3 Symantec NetBackup 备份软件简介

Symantec NetBackup 备份软件可以在异构操作系统、应用程序、管理程序以及磁盘和磁带架构上实现数据保护功能, 如实现全面保护、有效存储、随处恢复和集中管理[3-5]. 它集重复数据删除、复制和虚拟机防护功能于一体, 可以实现对存储效率、基础架构利用率和恢复速度有较大提升. 改软件分为客户端和服务器端两部分, 在需进行数据备份的服务器上安装客户端软件, 使用客户端软件管理数据的备份及恢复; 在连接存储介质的服务器上安装服务器端软件, 使用服务器端软件实现与各个客户端的通信, 并对数据传输进行优化, 存储至存储介质. 此外, 该软件可以在联网的任意计算机上安装一个 java 控制台软件, 可以实现对客户端软件及服务器端软件的控制管理, 这样就可以关闭服务器远程桌面连接的端口服务, 提高了系统整体安全性.

2 实现方案

通过评估量值传递业务管理系统的 RTO 及 RPO, 鉴于本系统的实时性要求[6], 决定使用虚拟带库替代传统的磁带库实现容灾备份. 虚拟带库并不以磁带为存储介质[7], 而是使用硬盘作为存储介质, 对于备份系统而言, 与直接备份至磁带中是一样的, 但是存储速度比磁带库大大提高, 特别是在数据恢复过程中, 虚拟带库不需要先倒带, 数据速度可达到 800GB/h, 能够达到量值传递业务管理系统的 RTO 及 RPO 要求[8-10]. 故选用惠普公司的D2D4106FC主机柜, 搭配MSA60扩展柜之后存储量为 10TB(RAID5 后).

同时, 又考虑到目前机房现有设备及网络情况, 提出了一种不同于以往采用光纤网络实现虚拟带库与数据服务器进行数据交换的方式. 我们采用的方式是将部署在昌平实验基地的备份恢复服务器与虚拟带库进行光纤冗余直连, 而备份恢复服务器与部署在本院区的各业务服务器直接采用以太网专线连接的方式. 这样搭建容灾系统, 满足了量值传递业务管理系统的 RTO 及 RPO 要求, 同时做到了异地备份处利用现有网络条件即可完成备份还原任务, 不必新购置光纤交换机, 最大限度地做到了节约能源及经费. 备份恢复服务器采用 IBM3650M2[11], 并安装 HBA 卡用以连接光纤, 备份软件采用美国 Symantec NetBackup 备份软件.

在数据库服务器等需要进行数据备份的服务器中按照以下备份策略进行数据备份: 在每天系统使用低潮期的深夜自动在本地服务器进行 SQL 数据备份, 生成 BAK 文件, 并于周末将 BAK 文件备份至虚拟带库并删除服务器本地BAK文件; 同时每天深夜由备份软件向虚拟带库进行一次增量备份, 周末进行一次完全备份. 容灾备份系统框图如图 1 所示:

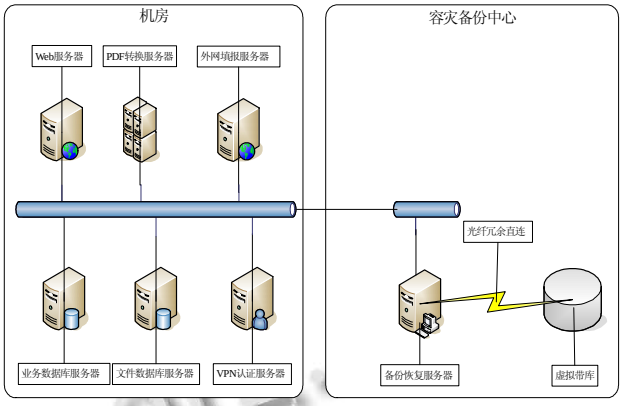

图 1 容灾备份系统框图

3 使用效果

通过对 Symantec NetBackup 备份软件和 D2D4106 FC 的备份日志进行分析, 完成一次增量备份时间很短, 大约为 10 分钟. 完成一次完全备份, 平均速度可达每小时 260G. 进行一次完全数据恢复, 平均速度可达每小时 62.5G, 完全符合本系统 RTO 及 RPO 要求.

4 小结

通过更新改造, 一是整个系统技术先进、安全可靠, 应用系统和数据的稳定性、可靠性大大提高, 从根本上改变多年来 “死看死守”的被动局面; 二是系统 RTO 及 RPO 能力大幅提高, 能实现 30 分钟系统恢复至可以支持各部门运作、恢复运营; 三是维修工作量

减少，通过大量采用技术先进、结构简单、稳定可靠和免维护的系统设备，达到减少维修量、工作量和降低维修成本的目标；四是节能环保，通过采用远程异地存储的方式，减少了使用本地磁盘及移动存储设备的存储量；五是提升系统运营管理效率和水平，按照系统运营管理模式的改革目标配备先进可靠的技术设备，为实现新的系统实现方式及设备维修模式创造了良好条件.

通过一段时间的实际使用，本容灾备份方案很好地保证了数据的完整性和量传业务的连续性，并且具有很高的性价比和可扩充性，可以满足同类系统的容灾要求及业务要求.

参考文献

1 刘羿彤,李丽,张明.计量管理软件系统建设及其安全性分析.中国计量,2011,(3):103−104.

2 JL 002-2012, 计量院信息化总体建设技术规范——软件部分,2012.

3 Sysmantec .Sysmantec NetBackup 7.0 备份、存档和还原入门指南 http://entsupport.symantec.com 2011.

4 Sysmantec .Sysmantec NetBackup 7.0 SAN 客户端和光纤传输指南 http://entsupport.symantec.com 2011.

5 Sysmantec. Sysmantec NetBackup 7.0 故障排除指南. http://entsupport.symantec.com 2011.

6 GB/T 20988.2007, 信息安全技术信息系统灾难恢复规范 2007.

7 HP. HP D2D4106 Backup System Capacity Upgrade Kit. http://h10010.www1.hp.com/wwpc/uk/en/sm/WF06c/A1-329290-3320517-3329763-3329763-3741179-4350671.html,March 2010.

8 康剑斌,汪海山,贾惠波.基于磁带库的磁盘缓存策略.仪器仪表学报,2009,30(6):1281−1284.

9 王德军,王丽娜.容灾系统研究.计算机工程,2005,31(6):43−45.

10 张磊.虚拟磁带库在灾备系统中的应用研究.小型微型计算机系统,2007,28(6):1149−1152.

11 IBM. IBM International Techincal Support Organization. Disaster Recovery Strategies with Tivoli Storage Management www. redbooks.ibm.com/redbooks/pdfs/sg 246844.pdf 2002.

(上接第 207 页)

全缺陷的分析基础上，提出一个新方案. 该方案无可信中心，具有更高的安全性；既可以有效避免中断协议攻击、篡改攻击、伪造攻击、合谋攻击等多种攻击，又可以在保证匿名性的同时，实现可追查性.

参考文献

1 王斌,李建华.无可信中心的(t,n)门限签名方案.计算机学报,2003,26(11):1581−1584.

2 Gan YJ. Verifiable threshold signature schemes against conspiracy attack. Journal of Zhejiang University Science, 2004, 5(1):50−54.

3 Xie Q. Cryptanalysis and improvement of two threshold signature schemes. Journal on Communications, 2005,26(7):123−128.

4 郭丽峰,程相国.一个无可信中心的(t,n)门限签名方案的安全性分析.计算机学报,2006,29(11):2013−2016.

5 张文芳,何大可,王宏霞,等.具有可追查性的抗合谋攻击(t,n)门限签名方案.西南交通大学学报,2007,42(4):461−467.

6 张有谊,乜国雷,郑东.一种可防止合谋攻击的门限签名方案.计算机应用与软件,2008,25(12):51−52.

7 徐光宝,姜东焕.抗合谋攻击的门限签名方案分析与改进.计算机工程,2010,36(20):155−156.

8 王鑫,张少武.无可信中心的门限签名方案的分析和改进.计算机工程与应用,2011,47(29):93−95.

9 Michels M, Horster P. On the risk of disruption in several multiparty signature schemes. Proceeding of Advances in Cryptology-ASIACrypt'96. Berlin: Springer, 1996:334−345.

10 Fouque PA, Poupard G, Stern J. Sharing decryption in the context of voting or lotteries. Proceeding of Financial Cryptography 2000.Berlin:Springer,2000:90−104.