

文章编号:1671-251X(2013)05-0019-05

DOI:10.7526/j.issn.1671-251X.2013.05.006

李明建,刁勇,张轶.基于双机热备的瓦斯灾害预警系统设计[J].工矿自动化,2013,39(5):19-23.

基于双机热备的瓦斯灾害预警系统设计

李明建^{1,2}, 刁勇^{1,2}, 张轶^{1,2}

(1. 瓦斯灾害监控与应急技术国家重点实验室, 重庆 400037;

2. 中煤科工集团重庆研究院, 重庆 400039)

摘要:针对煤矿瓦斯灾害预警系统软硬件运行环境的单点失效问题,设计了一种基于双机热备的瓦斯灾害预警系统,介绍了该系统的双机热备方案、软硬件结构设计及实现方法。该系统选用互备运行模式的双机备份高可用性集群及基于 RoseHA 和共享磁盘阵列的双机热备方案,提高了系统的可靠性。应用结果表明,与单服务器的预警系统相比,基于双机热备的瓦斯灾害预警系统的平均无故障间隔时间大幅增加,平均故障修复时间大大缩短,系统可靠性有了较大提高。

关键词:瓦斯预警; 灾害预警; 双机热备; 服务器集群; 共享磁盘阵列

中图分类号:TD712.7

文献标志码:A

网络出版时间:

网络出版地址:

Design and implementation of gas disaster early-warning system based on hot-standby

LI Ming-jian^{1,2}, DIAO Yong^{1,2}, ZHANG Yi^{1,2}

(1. State Key Laboratory of Gas Disaster Detecting, Preventing and Emergency Controlling, Chongqing 400037, China; 2. Chongqing Research Institute of CCTEG, Chongqing 400039, China)

Abstract: In view of problem of single-point failure in hardware and software running environment of gas disaster early-warning system of coal mine, a gas disaster early-warning system based on hot-standby was proposed, and its hot-standby solution, hardware and software design and implementation were introduced. The system employs high-reliability hot-standby cluster for mutual backup and hot-standby solution based on RoseHA and shared disc array, greatly improves its reliability. The application result shows that reliability of the gas disaster early-warning system based on hot-standby is greatly improved with longer mean time between failures and shorter mean time for fixing failure, compared with the early-warning system based on single server.

Key words: gas early-warning; disaster early-warning; hot-standby; server cluster; shared disc array

0 引言

煤矿瓦斯灾害预警系统(以下简称预警系统)是基于地理信息系统技术,综合地质测量、瓦斯地质、采掘生产、通风防突、监测监控等业务管理信息,对各类瓦斯灾害发生的可能性进行实时智能判断、超前提醒的大型专家系统^[1]。预警系统需要使用采掘

进度、防突措施施工与日常突出预测、瓦斯体积分数等关系数据,更需要煤层瓦斯赋存、井巷工程、地质构造等空间数据^[1-2]。预警系统的可靠性在很大程度上依赖于预警模型的有效性,此外,预警系统软硬件运行环境的可靠性也是影响系统可靠性的重要因素。研究设计高可靠性预警系统,除了根据矿井实际情况研究适用的预警模型外,还要设计高可靠性

收稿日期:2013-02-06。

基金项目:“十二·五”国家科技支撑计划项目(2012BAK04B01);国家重点基础研究发展规划(973 计划)资助项目(2012CB724300)。

作者简介:李明建(1977—),男,重庆人,工程师,主要从事煤矿安全管理相关软件系统研究、需求分析、设计开发等工作,E-mail:cqlmj@foxmail.com。

的预警系统软硬件运行环境。国家安全生产监督管理局制订的相关行业标准要求:煤矿安全监控系统及井下作业人员管理系统必须具备双机或多机备份,且故障切换时间应小于 $5\text{ min}^{[3-4]}$ 。为解决预警系统软硬件运行环境的单点失效问题,本文提出一种基于双机热备的瓦斯灾害预警系统。

1 系统设计原则

首先,双机备份方案必须满足空间数据访问要求。预警综合数据库采用“空间+关系”混合设计方式,且空间数据使用版本化存储,使用多张表存储 1 个要素类,因此,采用简单的同步机制实现双机数据同步在技术上不可行。其次,双机备份方案必须满足预警服务运行要求。预警服务基于有状态设计,不接受客户端程序的直接连接,仅读取预警综合数据库,执行预警操作,然后将预警结果更新到预警综合数据库,客户端定时读取预警结果。最后,双机备份方案必须满足 C/S 客户端访问预警综合数据库及智能客户端将本地数据库同步到预警综合数据库的要求。

2 双机热备方案设计

2.1 适用于预警系统的集群

服务器集群是一种新技术,通过服务器集群可以在付出较低软硬件成本的情况下在性能、可靠性、灵活性方面获得相对较高的收益,其任务调度则是集群系统中的核心技术^[1]。根据不同用途,集群系统可以分为 3 类:

(1) 高可用集群:在运行服务器发生故障时将其作业交接到待机服务器的集群。高可用集群以高可用性为目的,包括共享磁盘型和镜像磁盘型。

(2) 负载均衡集群:将客户端的请求按既定的负荷均衡原则分配给各节点的集群,以高扩展性为目的,一般无法进行数据交接。负载均衡集群包括 load balance 集群、并列数据库集群。

(3) 高性能集群:一般用于计算量很大的系统,使用超级计算机执行单一业务。使用所有节点的 CPU 来执行单一业务的网格计算技术近年来已成为热点,其本质就是高性能集群。

设计高可靠性预警系统的目的并非要让服务器接受大量的客户端访问,即无负载均衡要求;也不是要服务器承受大量的单一业务,即无高性能计算要

求。其目的在于提高系统可用性,减少宕机恢复时间,因此,选择高可用集群方案完全能够满足预警系统运行环境要求。

2.2 双机热备运行模式

根据受控应用、数据存储及其他资源的分布特点,双机热备有 3 种运行模式:主备机模式、互备模式、双机双工模式。

(1) 主备机模式即 2 台型号相同或不同的服务器,其中一台处于工作状态,另一台处于待命模式,2 台设备间用特定的方式通信,以告知彼此的状态。当备份机在一定时间范围内接收不到来自工作机的通信信息时,立即切换到工作模式,达到备份的目的。主备机方案有 2 种选择:① 共享硬盘型,即使用共享硬盘阵列存储数据、程序、配置信息,在切换时仅需要切换共享磁盘阵列的控制权;② 镜像硬盘型,即数据、程序、配置信息分别在 2 台机器上存储,在适当的时候进行同步,该方案以数据复制的时间为代价,但消除了共享磁盘阵列失效的风险,当然,共享硬盘阵列失效机率远比单一磁盘低。

(2) 互备模式即 2 台设备之间互相备份,彼此独立工作,完成不同的数据类型传输(设备甲处理或传输 A 类业务数据,设备乙处理或传输 B 类业务数据),当其中一台设备发生故障时,另一台设备在完成自己处理或传输工作的同时,接替另一台设备的处理或传输工作,达到备份的目的。典型方案:一台服务器作为数据库服务器,另一台服务器作为应用服务器,当其中一台服务器出现故障时,另外一台服务器承担所有任务。对于预警系统,正常情况下数据库系统运行于一台服务器;预警服务及预警网站运行于另外一台服务器;数据库文件存储于共享磁盘柜中,客户端通过虚拟 IP 访问预警综合数据库。

(3) 双机双工模式即 2 台服务器均处于活动状态,分别运行相同的应用,这样既保证了整个系统的性能和承载能力,也实现了负载均衡和互为备份,一般需要利用磁盘柜存储技术实现共享存储功能。对于预警系统而言,由于智能客户端本地数据库与预警综合数据库成对的数据复制内部机制较复杂,很难保证 2 个数据库的状态完全一致,而且必须保证复制本两端一对一关系,因此,该模式不适用于预警系统。

考虑可靠性、成本、资源有效性及预警系统体系结构设计约束,本文选择互备模式作为预警系统的

双机热备运行方案。

3 系统结构设计

3.1 硬件结构

表 1 常见的商用双机备份软件比较

比较项目	MSCS	RoseHA	ExpressCluster
支持双机热备模式	主备机、互备、双机双工	主备机、互备、双机双工	主备机、互备、双机双工
支持网络模式	域模式	域模式、工作组模式	域模式、工作组模式
支持共享资源	磁盘卷标、IP 地址、共享文件、服务器名称	磁盘卷标、IP 地址、共享文件、服务器名称、应用程序、组策略	磁盘卷标、IP 地址、共享文件、服务器名称、应用程序、定义的用户
支持心跳线类型及心跳冗余	Socket/RS232,不支持心跳冗余	Socket/RS232,支持心跳冗余	Socket/RS232
需要共享磁盘阵列	是	是	是
软硬件成本	对于 Windows Server 企业版和数据库版,不需要其他软件,但需要有单独的域控制器	购置 RoseHA 二节点(1.4 万元),需要共享硬盘阵列	购置 ExpressCluster X3.0 for Windows 二节点阵列版(4.8 万元),需要共享磁盘阵列
满足预警系统要求程度	一般工作于工作组模型网络中,无法完全满足要求	完全满足要求,以自定义服务方式对预警服务进行管理	与基于 RoseHA 的方案相比,软件成本较高

根据表 1,预警系统最终选择基于 RoseHA 和共享磁盘阵列的双机热备方案,其硬件结构如图 1 所示。

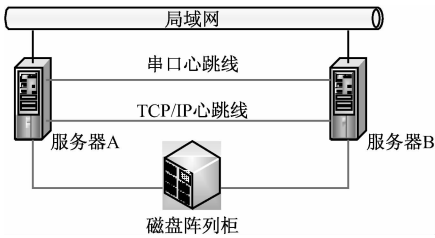


图 1 预警系统硬件结构

根据预警系统服务器要求,2 个服务器功能分配如下:服务器 A 采用 SQL Server 2005,包括预警综合数据库、监控预警数据库、防突信息数据库、短信数据库;服务器 B 包括突出综合预警服务、监控数据采集服务、监控预警服务、预警网站(IIS)、Web 矿图查询系统。

3.2 软件结构

预警系统所涉及的业务部门具有空间上的分散性,涉及信息具有时间上的间歇性,因此,基于分布式数据库理论设计预警系统的数据存储方案。分布式数据库系统中的每个站点都保存中央数据库的一个副本。在正常运行期间直接访问本地数据库,定时或不定时集中将更新数据同步到中央数据库^[8-10]。根据预警系统数据存储分布特点,可将预警综合数据库作为分布式数据库的主控副本,而各

国内外常见的商用双机备份软件有 Microsoft 公司的 Cluster Service (简称 MSCS)、Rose Datasystems 公司的 RoseHA、NEC 公司的 ExpressCluster 等^[5-7]。这 3 种软件的比较见表 1。

子系统本地数据库作为辅助副本,所有更新都先同步到中央数据库,再适时传送到其他各子系统本地数据库^[11]。地质测量管理、瓦斯地质分析、采掘进度管理等子系统独立性较强,需要长时间编辑操作才能提交完整的数据更新,因此,采用本地数据库存储空间数据与属性数据作为分布式数据库的辅副本;而突出预警管理平台、突出预警服务等子系统,为了提高预警及防突流程控制的时效性,必须及时获取空间数据更新,因此,采用版本技术连接到预警综合数据库,执行空间数据的读写操作。

数据库分布特性决定预警系统在体系结构上必须支持差异性。综合考虑数据分布性、网络有限可用性、数据存取效率及预警结果发布的实时性和便捷性等因素,预警系统将所有客户端分为智能客户端、传统 C/S 客户端和 B/S 客户端 3 类。对于地质测量管理、瓦斯地质分析等子系统,采用基于分布式数据库的智能客户端技术,在客户端上不仅部署子系统应用程序,而且部署子系统数据库,采用空间数据复本(Replica)技术进行离线编辑,完成以后执行数据同步任务;对于预警管理平台、突出预警服务等需要获取实时数据的子系统则采用传统 C/S 技术,在客户端上仅部署子系统程序,直接连到预警综合数据库进行数据查询和编辑;对于仅关注预警结果信息、矿图信息的用户,不在客户端上安装任何程序,仅通过浏览器访问 Web 服务器即可获得结果。

瓦斯灾害预警系统软件结构如图 2 所示。3 类客户端运行特点见表 2。

相对使用单一服务器的预警系统来说,基于双机热备方案的预警系统对系统结构有以下特殊要求:

(1) 对机器名的处理。不管是服务器端程序还是客户端程序,凡是代码中使用服务器名的地方,必须将其可配置化,并在配置文件中 使用虚拟 IP 代替,而不应使用双机中任何一个服务器的机器名。

表 2 3 类客户端运行特点

比较项目	智能客户端	传统 C/S 客户端	B/S 客户端
数据存储位置	本机/服务器	服务器	服务器
网络依赖性	很强,运行时不连接网络,同步时使用 TCP/IP 长连接	很强,使用 TCP/IP 长连接	较强,使用 HTTP 短连接
运行效率	高,所有数据均存储于本机	较低,直接读取服务器数据	较高,Web 服务器与数据库服务器在同一双机集群中
对服务器资源的依赖性	数据同步组件要求有确定的服务器 MAC 地址	无依赖,客户端通过虚拟 IP 访问数据库服务器	无依赖,Web 服务器通过虚拟 IP 访问数据库服务器
常用子系统	地质测量信息子系统;瓦斯地质分析子系统;采掘生产管理子系统	突出综合预警服务(运行于服务器上);突出预警管理平台;瓦斯涌出分析子系统;防突动态分析子系统	预警信息查询子系统;Web 矿图查询子系统

(2) 对 MAC 地址的处理。凡是服务器端程序代码中使用本机 MAC 地址的地方,都需要提取通过 RoseHA 设置的虚拟 MAC 地址。

4 系统实现

根据系统结构设计,在潞安矿业集团余吾煤矿预警系统实施过程中,2 台服务器均采用 IBM X3650 M3,共享磁盘阵列采用 IBM TotalStorage DS3200,服务器使用 SAS HBA 线连接到共享磁盘阵列;局域网中客户端采用虚拟 IP 连接到服务器,为防止客户端错误连接,虚拟 IP 与服务器私有 IP 一般不在同一个网段上。双机系统切换流程如图 3 所示。

为便于研究,选择基于 RoseMirrorHA 的双机镜像方案和基于 RoseHA 共享磁盘阵列的方案进行对比。在测试过程中,采用手动方式停止 SQL Server 服务,使服务器 A 切出,服务器 B 接管所有任务所使用的时间见表 3。

通过比较发现,2 种方案的最大差别在于基于 RoseMirrorHA 的方案需要较长时间执行数据镜像,且执行数据镜像所需的时间因服务器负载、数据更新量而有所差异,而基于 RoseHA+共享磁盘阵

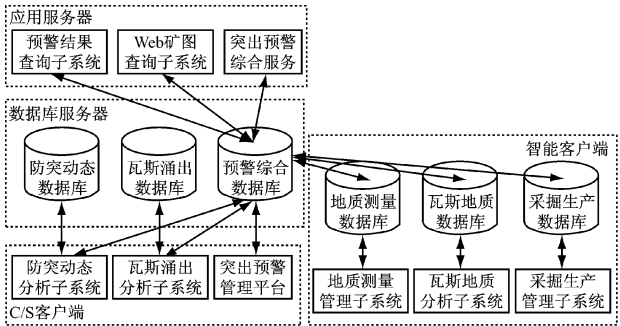


图 2 预警系统软件结构

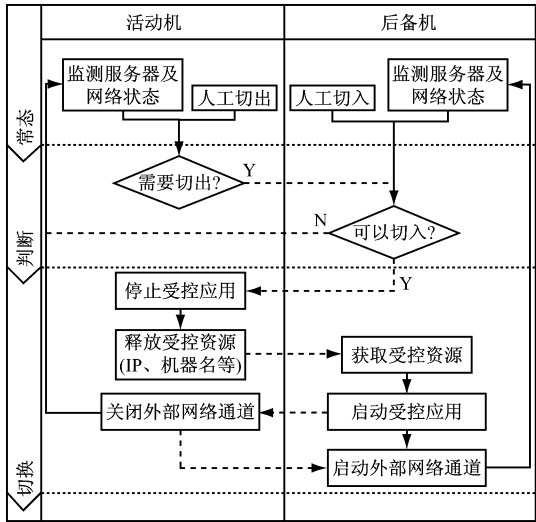


图 3 双机系统切换流程

列的方案则仅需要加载共享磁盘,后者是一种以增加硬件成本来减少切换时间的思路。

5 结语

基于双机热备的预警系统已经在潞安矿业集团余吾煤矿、晋煤集团赵庄矿等投入正式运行。与已投入运行的相同型号的单服务器系统相比,该预警系统的平均故障间隔时间(T_{MTBF})由 12 000 h(平均 1 年约 0.73 次故障)提高到 21 000 h(平均 1 年约

表 3 2 种双机热备方案执行过程比较

比较项目	RoseMirrorHA	RoseHA
检测服务器 A 上 SQL Server 已经停止	12	12
判断服务器 B 能否切入	5	5
执行数据镜像(数据库文件所在盘)	76	—
服务器 A 释放而服务器 B 加载共享磁盘	—	20
释放共享 IP 并关闭网络通道	4	4
启动 SQL Server 相关服务	25	25
接管虚拟 IP 并打开网络通道	5	5
合计	127	71

0.46 次故障),平均故障修复时间(T_{MTTR})也有较大的缩短,系统的可用性($\gamma = T_{\text{MTBF}} / (T_{\text{MTBF}} + T_{\text{MTTR}})^{[12]}$)有较大提高。当然构建双机备份系统的软硬件成本比单服务器系统有较大增加,且互备模式的双机热备系统的可靠性一般低于主从模式的双机热备系统^[13],因此,该预警系统的运行模式有待进一步研究。

参考文献:

[1] 王鹏,崔锋,郭锋.煤与瓦斯突出实时监测及预警系统研究[J].陕西煤炭,2011,30(1):13-15.

[2] 文光才,宁小亮,赵旭生.矿井煤与瓦斯突出预警技术

及其应用[J].煤炭科学技术,2011,39(2):55-58.

[3] AQ 1029—2007 煤矿安全监控系统及检测仪器使用管理规范[S].

[4] AQ 6210—2007 煤矿井下作业人员管理通用技术条件[S].

[5] 郭丽蓉,董凯.数据库服务器双机热备解决方案[J].电力学报,2003,18(2):143-144.

[6] 王秀娟.调度集中系统中双机热备机制的实现[J].北京交通大学学报,2009,33(2):30-33.

[7] 张金仙,郝英立,张利,等.工控组态软件双机热备的研究与实现[J].计算机测量与控制,2005,13(11):135-138.

[8] 邵佩英.分布式数据库系统及其应用[M].北京:科学出版社,2005:4-6.

[9] 钱郭锋,刘波,陈珺.分布式数据库系统的设计与实现[J].现代测绘,2010,33(3):26-28.

[10] 李晶晶.分布式数据库在管理信息系统中的应用[D].武汉:武汉理工大学,2004.

[11] 黄建红.主控副本方法在保持分布式数据库数据副本一致性中的应用[D].济南:山东大学,2004.

[12] 包建军,霍振龙,樊菁.可靠实现煤矿双机热备系统的方法[J].工矿自动化,2010,36(11):5-8.

[13] 武建锋,荆文芳.双机容错方案设计[J].电子产品可靠性与环境试验,2006,24(1):19-22.