第 26卷 第 5期 电子科技大学学报 Vol. 26 No. 5
1997年 10月 Journal of UEST of China Oct. 1997

高可用性系统的研究与实现*

林晓东** 刘心松
(电子科技大学计算机系 成都 610054)

【摘要】 研究了高可用系统的结构,介绍了一种高可用系统的实现。在分析系统失效因素和高可用系统结构的基础上,对主要的失效部分(软硬件)进行冗余以提高服务器、磁盘、网络可靠性,据此采用有效的失效探测与恢复机制,实现了一个能够保证整机容错,无单点失效的高可靠系统。

关 键 词 高可用性; 容错; 冗余; 单点失效; 心搏信号; 代理
中图分类号 TP302.8

为了实现系统可靠地运行,组成计算机系统必须采取相应的设计和措施,对此计算机界将其分为从高到低的 4个档次: 1) 连续可用性系统; (Continuous Availability System;) 2) 容错系统 (Fault Tolerance System); 3) 高可用性系统 (High Availiability System; 4) 容灾难系统 (Disaster Tolerance System)。

传统上高可靠性系统的实现是采用专用的容错机,价格昂贵,且需要较长的人员培训时间。容错机往往采用专用的操作系统,不易于软件的开发和移植,而且它也不能检测应用程序错误。当前流行的一种可靠性技术是所谓的高可用性系统(high-availability system,简称 HA系统)。它采用通用的计算机,通过对关键的软件失效部件进行冗余,结合对失效的有效探测和恢复,提供了一个可靠的计算环境。高可用性系统性能/价格比优于传统的容错机。不仅对硬件错误、操作系统和 Database错误有很好的容错能力,而且还能够检测应用软件的错误。

本文在分析高可用性系统结构的基础上,介绍了我们实现的高可用性系统。

1 HA系统的原理

要建立一个合理、有效的高可用性的环境,需对系统失效的原因进行研究。常见的失效因素有以下几方面[1]: 1) 提供服务的主机挂起、关机或不可用; 2) 连接用户和服务器的网络失效; 3) 用户试图访问的服务器上的应用不能正确工作、挂起或离线; 4) 用户试图访问的工作站上的应用不能正确工作、挂起或离线; 5) 服务器提供的数据服务已经离线。

研究发现,最主要的失效来自于用户的错误,然后是硬件失效、软件失效等。HA系统探测大部分失效而不象容错系统试图预测和诊断所有失效,从而降低了系统难度与成本。

HA系统通过提高服务器可靠性、事务数据磁盘可靠性、网络可靠性、应用程序可靠性来达到高可用性要求。通常的 HA系统结构如图 1所示,它使用共享磁盘阵列来提高磁盘可靠性,用冗余的网络来提高网络可靠性,用合作的服务器对来提高服务器可靠性,通过对应用程序的探测与有效恢复来提高应用程序可靠性,使用两条冗余的服务访问介质提高网络可用性[2]。

⑳ 1996年 10月 28日收稿
* 国家科委 863高科技项目
** 男 28岁 博士生

HA系统主要可以分为对称式(又称双向故障消除式)和非对称式,又称单向故障消除式)系统两种。

非对称式的 HA系统包括两台相同的服务器,其中之一是活动的基本系统(称主系统),客户机(Client)从它存取数据和获得服务;另一台同样的服务器(称备份系统)监视主系统的运行,并在主系统失效的情况下,自动接替其工作,充当主系统的角色。而原来的服务器修复后充当备份系统的角色,当新的主系统失效后再接替其工作。

对称式的 HA系统中,两台服务器同时都是活动的,彼此都能提供独立的服务,每台服务器在另一台失效时可以接替它为 Client提供服务,这样每台服务器既是主服务器又是备份服务器。两服务器之间通过内部网络实现彼此的监控,内部网络一般是冗余的两条网络,既可以采用一条以太网和一条串口连接,也可以采用两条以太网连接[3]。HA系统在这种硬件环境下,通过 HA监控软件完成对系统状态监测、失效的探测与恢复以及维护与管理。

HA监控软件是 HA设计的核心,它监视 HA系统的主要硬件和软件的工作状况,并在主系统失效时,将事务切换到备份系统,对各种失效进行探测和有效的恢复。软件实现要求保证系统正常工作,尽量减少各个模块之间的相互依赖,避免本身可能存在的失效,同时运行在主系统和备份系统的主监控守护(HA DAEMON,简称 HAD)进程本身也存在失效的问题。为此,借用硬件冗余的方法,同时启动两个冗余的 DAEMON来避免 HAD可能引起的单点失效。这样,系统中同时运行着两个 DAEMON,它们能互测互启,杀死失效的 DAEMON,保证了总有两个 HAD在运行,否则将迫使系统恢复,见图 2。于是冗余的 HAD和服务器对间的两条通信通路、冗余的服务访问网络、冗余的磁盘控制器,构成了一个无单点失效的 HA系统。

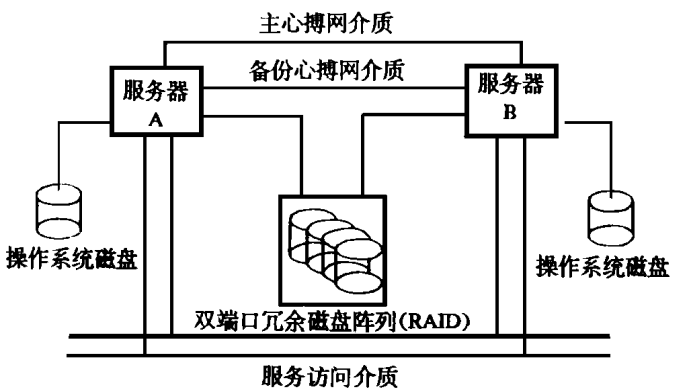

图 1 HA系统的硬件结构

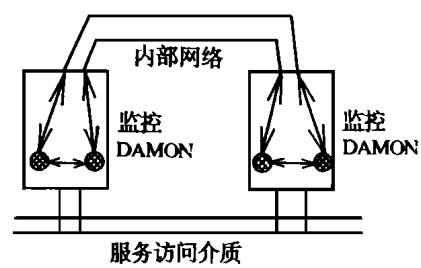

图 2 无单点失效的结构

2 高可用性系统的实现

2.1 系统实现软硬件环境

实现采用两台曙光 POWER-PC服务器,它们各自具有以太网卡(1~2个),SCSI卡(1个),RS232接口(1个),并各自带有自己的系统盘(1 G),并运行 AIX操作系统。HA软件同时运行于两台服务器,两台服务器共享用于存放数据的双端口磁盘阵列(最大存储量可达 28 GB)。

2.2 HA监控软件的实现

HA监控软件的主要功能如图 3所示。

2.2.1 主监控 DAEMON(HAD)和通信进程

1) 服务器运行状态

服务器任何时刻总处于下列状态之一: 正常状态 Normal(N)、接管状态 Takeover(T)、恢复状态 Recover(R)、下岗状态 Downtime(D),每台服务器上维护着一个状态信息池,记录服务器的状态。当服务器和监控台通信时,要向它发送状态信息,若在信息池中找到,则发送。各个代理可以向状态信息池中写信息,调用 write- msg( )完成。

通常情况下,两个服务器均为 normal状态,单个服务器的状态变化如图 4所示,理论上双机共有 16种可能的状态,有的状态是 HA系统不会发生的,比如双服务器都失效(“ DD”), HA系统设计认为其概率为零[4]。又如“ TT” (双机均执行接管操作)是 HA系统实现应避免的。当主服务发生失效时的状态变化为(括号内前一个代表主服务器状态,后一个代表备份服务器状态): (N, N)→(D, N)→(D, T)→(R, T)→(R, N)→(N, N);非对称方式下备份服务器发生失效的状态变化为: (N, N)→(N, D)→(N, R)→(N, N);对称方式下备份服务器发生失效的状态变化为: (N, N)→(N, D)→(T, D)→(T, R)→(N, R)→(N, N)。

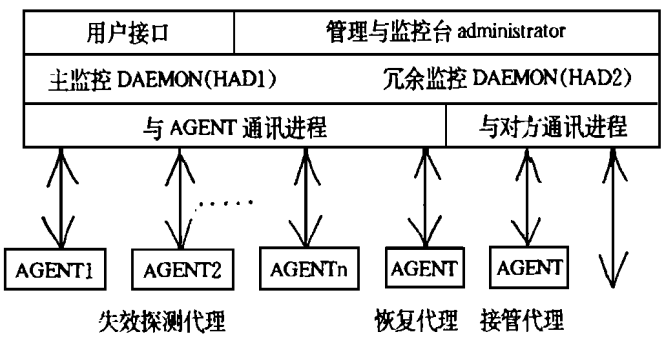

图 3　HA监控软件功能框图

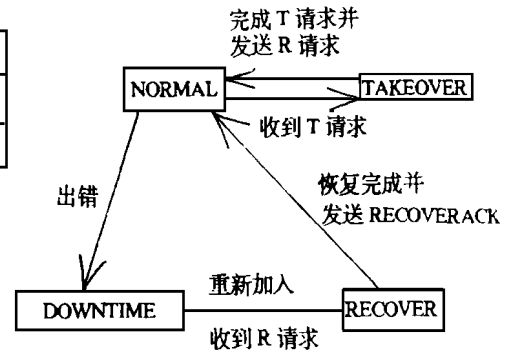

图 4　服务器状态变化图

2) 主监控进程 HAD

两台服务器上都运行着 HAD,每台服务器上运行着两个监控进程 HAD1和 HAD2,它们互相监测,能互相在对方失效时启动对方,避免了由于一个 HAD可能产生的单点失效。它们各自完成的功能主要有:

HAD1:

(1) 启动各个代理进程;

(2) 检测代理的状态,发现出故障则重新启动之;

(3) 创建与对方服务器通信的发送与接收进程,并监测其状态;

(4) 监测 HAD2 向 HAD2发 PING开始信号。

HAD2

(1) 监测 HAD1,收到 PING开始信号则启动 PING通过网络以心搏方式检测对方服务器的状态,通过 RS-232按指定的时间间隙向对方发送信号,对方收到每个信号后发送确认信息,当收不到周期性的确认信息时,将进行一系列探测确定对方失效(称为心搏(HEART-BEATING)方式)[3];

(2) 读取状态信息,并执行相应动作;

(3) 激活发送进程向对方服务器发送信息;当满足 TAKEOVER(接管)和 RECOVER(恢复)触发条件时,完成相应的操作。

各个代理需把检测的结果报告给 HAD2,每个代理采用写共享存储区的方法,把结果写到一个建立的共享内存中,其结构如图 5所示。

发给对方 Server	从对方 Server 接收	从 ADM Server 接收	代理 1 PID	代理 1 检测结果	代理 2 PID	代理 2 检测结果	…

图 5 共享储区结构

每个单元定义:

```
struct Record {
        int type; /* 代理类型 */
        int value; /* 代理的相关的值, PID,检测结果* /
        int timestamp; /* 时标* /
            }
```

Record. value取值为:

0 OK 1 INFORMATION
2 WARNING 3 ERROR
4 OVERTIME 5 RECOVER
6 TAKEOVER 7 TAKEREQUEST
8 RECOVERACK 9 TAKEOVERACK

每个代理通过两个函数 read- shm( )和 write- shm( )读写共享存储区。

3) 通信进程

系统通信实现包括两台服务器间通信以及主监控制进程与代理进程和监控台的通信两部分。

两个服务器间采用心搏方式检测彼此的状态。

发送信息的进程由 HAD1创建并监控;进入睡眠状态,由 HAD2激活,向对方发送信息,发送的信息包括:

0 OK 1 TAKEOVER 2 RECOVER
3 TAKEREQUEST 4 TAKEACK 5 RECOVERACK

接收进程接收对方服务器的信息,由 HAD1创建并进行监测,当收到信息时,将信息反馈到 HAD2,超时收不到信息,则把超时信息反馈给 HAD2。

双机间通信可利用串口,基于 RAW方式和 PPP方式;也可以使用 ETHERNET,基于 TCP/IP来实现。

HAD与监控台之间通信,完成向监控台发送状态信息 (如 WARNING, ERROR等)和接受从监控台由 administrator发出的主动 TAKEOVER请求信息,将信息反馈给 HAD2 它由 HAD1创建并监测其状态。

总之, HAD和各通信进程共同完成双机通信及系统监控管理。

2.2.2 接管和恢复的实现

当系统满足接管和恢复的触发条件时, HAD2将启动 TAKEOVER和 RECOVER代理进程完成相应的工作。每个服务器上维护一张 TAKEOVER表和 RECOVER表,该表记录了两个过程应完成的工作,如重启应用程序。它们首先修改了 INTERNET地址,然后读取表的内容,执行相应的动作。

每个服务器配置了两套网络接口,相应有两个 IP地址,指定一个接口作为正常工作接口,称为主接口,另一接口当对方服务失效时被设置为它的正常工作接口。实现 IP地址的接管需对客户端透明,方法是利用 ARP协议请求更新客户的〈硬件地址, IP地址〉映射。

TAKEOVER进程重启应用程序后,根据磁盘上的日志记录恢复现场,将磁盘上用户请求队列放在应用程序的用户请求 CACHE的头部,运行应用程序。

对应用程序的接管与恢复需要应用程序的配合,要求应用程序每隔一定时间记录现场信息。

TAKEOVER的触发条件是:

1) HAD2接收到超时信息 (OVERTIME)

◦ 向对方服务器发送 TAKEREQUEST信息;

◦ 等待接收对方的 TAKEREQUEST应答— TAKEACK信息;

◦ 收到 TAKEACK或超时;

◦ 启动 TAKEOVER进程,进入 TAKEOVER状态。

2) HAD2接收到对方服务器的 TAKEOVER请求

◦ 延时等待对方关闭 INTERNET地址和 RECOVER表中的应用进程;

◦ 启动 TAKEOVER进程,进入 TAKEOVER状态。

3) HAD2接收到 ADMINISTRATOR的主动 TAKEOVER请求

◦ 执行操作同 1)。

当收到 TAKEREQUEST信息后, HAD2将关闭 INTERNET地址和 RECOVER表中的应用进程,然后发送 TAKEACK信息给对方;当发出 TAKEOVER信息后, HAD2关闭 INTERNET地址和 RECOVER表中的应用进程。

RECOVER的触发条件是:

1) HAD2发出 RECOVER信息后:

◦ 等待对方的 RECOVERACK信息;

◦ 收到 RECOVERACK或超时;

◦ 启动 RECOVER进程;

◦ 进入 NORMAL状态。

2) HAD2接收到对方发出的 RECOVER信息。执行:

◦ 如果服务器状态为 N,发送 RECOVERACK信息;

◦ 修改 INTERNET地址,关闭 TAKEOVER的应用进程;

◦ 发送 RECOVERACK信息;

◦ 进入 NORMAL状态。

2.2.3 失效的探测

失效的探测采取把不同的探测任务交给不同的代理进程来完成的方式。代理把探测结果调用 write- shm( )写到共享内存区,反馈给 HAD2。限于篇幅,本文不详细讨论各代理的具体实现,需保证各代理的独立性与可靠性。

2.2.4 系统管理与监控台、用户接口

系统管理员可以从监控终端观察 HA系统的状态,并能通过它向一服务器发送主动 TAKEOVER请求。当服务器出故障时,提示管理者修复。提供的用户接口供用户增加自己的失效探测代理。

3 结　论

本文介绍了一个利用软硬件冗余达到无单点失效,保证整机容错的高可用性系统实现。对我们实现的系统进行测试,系统工作正常,不会出现诸如两台服务器同时处于 TAKEOVER或主系统处于 NORMAL而备份系统处于接管状态的不正常情形。在人为造成的系统失效情形下,系统的

切换时间依赖于应用程序的启动时间和由日志文件信息大小决定的恢复现场的时间. 控制日志文件大小可以改变系统切换时间,为了适应对切换时间要求苛刻的场合,可以让应用同时运行于主系统和备份系统,主系统输出结果、写盘并记录日志,备份系统同样接受用户请求,处理但不输出结果、不写盘和记录日志,当主系统出故障时,由备份系统输出结果、写盘并记录日志,此时,TAKEOVER时间很短(错误检测时间),大致由心搏频率决定.

参 考 文 献

1 Tidalware Technologies Inc. High avaliablity failover Management software technical whiteee paper. April, 1994

2 Alain Azaguray, Danny Dolev. Highly available clustera acase study. Proceedings of the 22nd Intemal Conference of Fault Tolerant Computing, 1994, 24: 404~413

3 Yair Amir, Danny Dolevetc. Tranisi: a communication sub-system for high availability. Proceedings of the 22nd Internal Conference on Fault Tolerant Computing, 1992, 22: 76~84

4 刘心松. 容错并行处理系统结构研究. 计算机应用, 1994, (1): 8~11

5 Jin Gray, Daniel P. Siewiorek: high-availability computer system S. Proceedings of the 23rd Intemal Conference on Fault Tolerant Computing, 1991, 23: 39~47

Implement of High Availability System

Lin Xiaodong Liu Xinsong

(Dept. of Computer Science, UEST of China Chengdu 610054)

Abstract This paper describes the research and implementation of high availability system. By way of analyzing the system failure factors, a no-single-point-failure high availability system architecture is presented which uses the hardware and software redundancy technique to ensure server, disk, network reliability and privides efficient failure recovery. The implementation method is also given.

Key words high availability; fault to lerant; redundancy; single-point failure; heart-beat signal; agent

编辑 叶 红