

Design of Disaster Recovery Project about Tracking Telemetry and Command System based on Cluster

Hui Yan, Weijie Han, Yu Wang, Xiaodan Gu

Department of Information Equipment, The Academy of Equipment Command & Technology, Beijing, China, 101416

Email: yanhui_99@163.com, visc_hwj@126.com

Abstract: The TT&C (tracking Telemetry and Command) system plays an important role on the space-flight task directly. A disaster recovery project is designed for the aerospace TT&C system based on high availability clusters. The project realizes disaster recovery of the key TT&C data and assets by remote disk mirror technology and important application transfer by IP redirecting. The project satisfies the disaster recovery needs of the aerospace TT&C system efficiently.

Keywords: the TT&C system; disaster recovery; high availability clusters; remote disk mirror; IP redirect

基于集群技术的测控系统容灾方案设计

阎 慧, 韩伟杰, 王 宇, 顾晓丹

装备指挥技术学院 信息装备系, 北京, 101416

Email: yanhui_99@163.com, visc_hwj@126.com

摘 要: 测控系统的安全可靠直接影响着航天任务的完成。基于高可用性集群技术设计了测控系统容灾方案, 方案采用远程磁盘镜像技术实现测控关键资产数据的容灾备份, 并采用 IP 重定向技术实现关键业务的容灾迁移。方案有效满足了测控系统的容灾需求。

关键词: 测控系统; 容灾; 高可用性集群; 远程磁盘镜像; IP 重定向

1 引言

如果把飞船以及发射到空间的各种卫星及飞行器比作风筝, 那么航天测控系统就像是牵引风筝的线, 它是航天通信、测控和指挥的纽带, 它的安全性和可靠性关系到整个航天事业。因灾难造成数据丢失或业务中断, 严重的甚至会影响航天任务, 造成不可估量的损失。引起航天测控系统灾难的因素很多, 可以是系统中的软硬件故障, 还可以是因火灾、地震、战争而引起的数据处理设备的损坏, 以及误操作和人为破坏而造成的数据丢失、数据库崩溃等。只要造成了航天测控系统业务的中断和关键数据的丢失, 都是灾难。容灾的目的是防止信息系统在遭受灾难时造成系统服务停止和数据丢失, 其实现主要通过异地建立和维护一个备份系统(容灾中心), 利用地理上的分散性来保证对灾难性事件的抵御能力^[1]。所以建立航天测控容灾系统, 保证测控数据的完整性和业务的连续性, 对完成航天任务就显得极为重要。

资助信息: 本课题得到部委级基金项目支持。

2 容灾需求分析

航天测控系统在航天任务中主要承担通信保障、下行数据实时处理、上行控制、指挥决策及事后数据处理等核心测控业务, 这些核心业务的安全性和可靠性在很大程度上将决定航天任务的成败, 因自然灾害或人为事故造成的业务中断和数据丢失, 将会对航天任务造成不可估量的损失和影响。

建立航天测控容灾系统, 主要考虑其承担的航天任务, 为任务过程中的关键数据和业务提供安全保障。容灾系统主要的灾备需求包括:

(1) 关键资产备份

历次的航天任务会形成大量的任务实施流程、关键技术问题解决方案, 并存储积累大量的任务原始数据和事后分析结果。这些数据是航天测控系统的核心关键资产, 对后续航天任务的准备和执行具有重要的参考价值。建设容灾系统需要提供这些关键资产的备份存储能力。

(2) 灾难恢复能力

通过构建容灾系统,提高航天测控系统应对自然灾害(火灾、水灾、地震等)、社会灾难(电力故障、恐怖袭击、战争损害等)和人为灾难(人员误操作、网络攻击、计算机病毒损害等)的能力,使得在灾难发生时,可以尽快地恢复或重建其软硬件系统,恢复系统对航天任务的支持能力。

(3) 保持应用业务

在飞船发射、运行管理和返回阶段,飞船和空间站交会对接阶段,以及空间站长期管理阶段等任务关键实施阶段,容灾系统需要提供实时在线备份支持能力,当出现灾难事故时,容灾系统可以实时接管原系统所承担的航天任务业务,保持测控业务工作的连续性。

3 高可用性集群技术

集群^[2]是由相互独立的一些计算机系统构成,这些相互独立的系统构成的是一个相互协调的群组,这些计算机系统作为一个整体对外提供服务。对于用户来说,这些计算机的行为就像一个计算机一样,但其处理能力、可靠性和 I/O 能力都有大幅度提升。基于这种特性,可以构建高可用的集群方案,实现高可用的航天测控容灾系统。

高可用性集群是共同为客户端提供网络资源的一组计算机系统,其中每一台提供服务的计算机称为节点。当一个节点不可用或者不能处理客户的请求时,集群系统会采用基于 IP 重定向的应用迁移技术将该请求及时转到其它可用节点来处理。

基于 IP 重定向的应用迁移技术是一种重要的实现应用容灾的迁移技术,它主要使用 IP 重定向设备,使应用业务在集群节点之间自动切换,以实现容灾抗毁与业务连续性^[4]。其原理如图 1 所示。

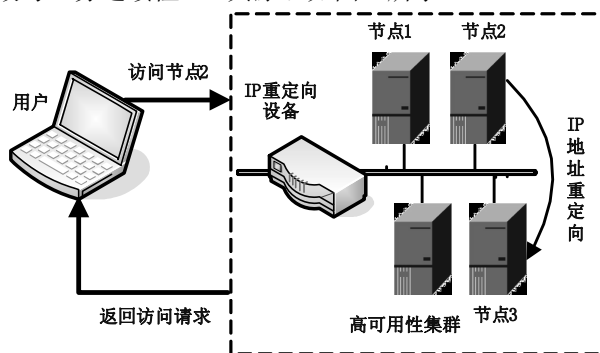


Figure 1. Application transfer based on IP redirecting

图 1. 基于 IP 重定向的应用迁移

按照高可用性集群的硬件拓扑结构,可以将其分为基于共享磁盘的高可用集群系统和基于磁盘镜像的高可用集群系统。基于共享磁盘的高可用集群系统通过共享磁盘实现集群中各节点的数据共享,包含主服务器、从服务器、存储阵列等主要设备,以及设备间的心跳连接线。基于磁盘镜像的高可用集群系统不包含存储阵列,集群中服务器的本地硬盘通过数据镜像技术,实现集群中各节点之间的数据同步,从而实现集群的功能^[5]。

4 基于集群技术的容灾方案设计

基于对航天测控系统的容灾需求分析,采用集群技术可设计如图 2 所示的航天测控系统容灾方案。方案针对航天测控系统的主要测量处理设备,以及这些设备处理的数据和完成的业务,在异地建设远程容灾中心(Remote Disaster Recovery System,简称 RDRS)。RDRS 通过采用远程磁盘镜像技术实现对航天测控系统关键资产数据的远程灾备,并通过部署高可用性集群实现对航天测控应用业务的容灾保障。

本方案部署了两条通信线路,一条基于公共的 TCP/IP 网,该网络负责传送各设备接收的上行数据,并将其实时镜像备份到容灾中心的异地数据存储系统。另一条通信线路为非 TCP/IP 网络,实现对原系统状态的监控,并在灾难发生时实现系统业务的迁移。

在业务容灾过程中,RDRS 的工作原理是利用非 TCP/IP 网络对 RDRS 环境中的各节点进行状态监控,它可以是用 RS232 串口线将各节点连接起来,也可以是将各节点的 SCSI 卡或 SSA 卡设置成 Target Mode 方式。RDRS 将监测并响应于三种类型的故障:网卡故障、网络故障及节点故障。其具体工作方式:

(1) 网卡故障

在 RDRS 环境中,非 TCP/IP 网络实际上是一根“心跳”专线,专门用来监测系统中发生了何种故障,如节点死机或者网络发生故障。在集群环境中,节点的网卡、非 TCP/IP 网络会不断地接收并发送 Keep-Alive (简称 KA) 信号,KA 的参数是可调的,KA 在连续发送一定数量的包都丢失后即可确认对方网卡,或网络,或节点发生故障。因此,基于 KA 信号 RDRS 可以很容易地发现网卡故障,因为一旦某块网卡发生故障,发往该块网卡的 KA 就会丢失。此时,该节点上的 cluster manager (集群控制终端)会产生

一个 swap-adapter 事件, 并执行该事件的 script (集群中提供了大部分通用环境下的事件 script, 它们是用标准 AIX 命令和 HACMP 工具编写的)。每个节点上都有至少两块网卡, 一块是 service adapter, 提供对外服务; 另一块是 standby adapter, 它的存在只有 cluster manager 知道, 应用和客户端并不知道。一旦发生

swap-adapter 事件后, cluster manager 将原来 service adapter 的 IP 地址转移到 standby adapter 上, 而 standby 地址转移到故障网卡上, 同时网络上其它节点进行 ARP 的刷新。网卡互换 (swap-adapter) 在几秒钟内即可完成, 以太网为 3 秒, 并且这种转换对应用和客户端是透明的, 只发生延迟但连接并不中断。

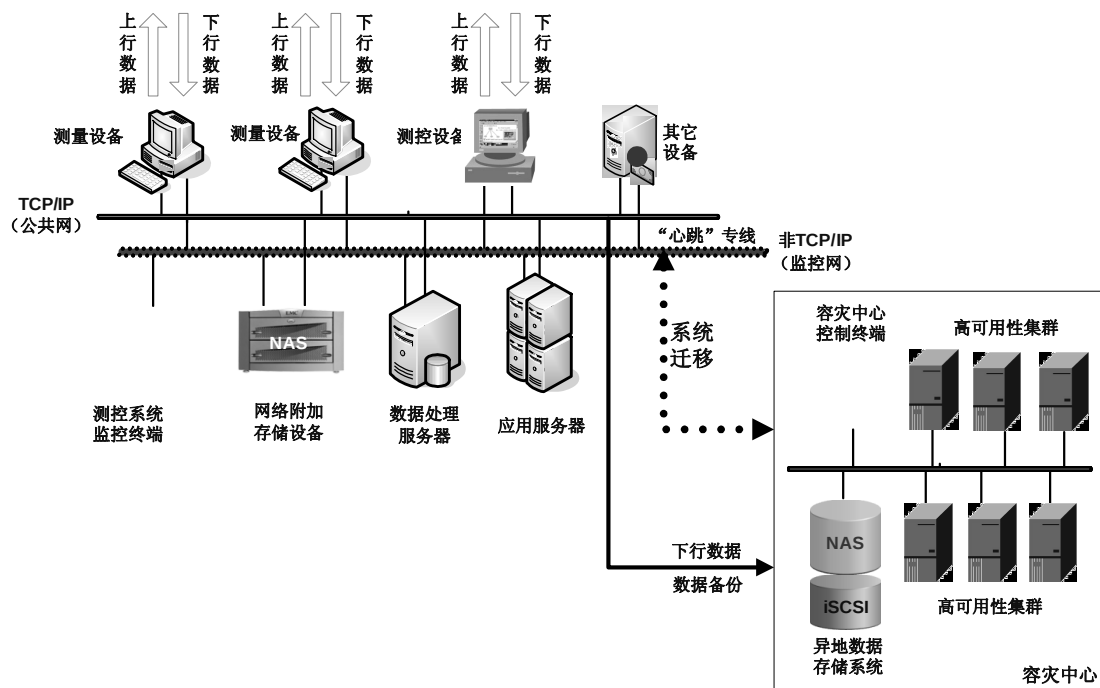


Figure 2. Disaster recovery project based on clusters
图 2. 基于集群技术的容灾方案

(2) 网络故障

如果发往某节点上的 service 和 standby 网卡上的 KA 包全都丢失, 而非 TCP/IP 网络上的 KA 仍然存在, 那么 HACMP 判断节点仍然正常, 而网络发生故障。

(3) 节点故障

如果不仅 TCP/IP 网络上的 KA 全部丢失, 而且非 TCP/IP 网络上的 KA 也丢失, 那么 HACMP 断定该节点发生故障, 并产生 node-down 事件。此时将有资源接管, 即放在共享磁盘陈列上的资源将由备份节点接管, 其中 IP 地址接管和重新启动应用由 HACMP 来实现, 而其他是由 AIX 来完成。当整个节点发生故障时, HACMP 将故障节点的 service IP address 转移到备份节点上, 使网络上的客户端仍然使用这个 IP 地址, 这个过程称为 IP 地址接管。

当一个节点发生故障失效之后, 如果设置了 IP 地址接管, 网络上的客户请求会自动连接到接管节点上; 同样, 如果设置了应用接管, 该应用会在接管节点上自动重启, 从而使系统能继续对外服务。对于要实现接管的应用, 只需在 HACMP 中把它们设置成 application server, 并告诉 HACMP 启动这个应用的 start script 的全路径名和停止该应用的 stop script 的全路径名。

5 总结

航天测控系统的安全可靠直接影响着航天任务的顺利完成。建设航天测控容灾系统的目的就是要保障测控数据的完整性, 以及测控业务的连续性。基于高可用性集群环境, 采用远程磁盘镜像技术实现测控关

键资产数据的容灾备份, 并采用 IP 重定向技术实现关键业务的容灾迁移。在下一步的工作中, 将继续探索集群技术在实现大型复杂系统及业务应用的容灾设计中的应用。

References (参考文献)

- [1] Yang P, Li T, Zhao K, et al. An internet based disaster recovery system. *Disaster Recovery Journal*, 2005, 18(1).
- [2] B.S.Everitt, S. Landau, M.Leese. *Cluster Analysis*. Arnold Publishers, London, fourth edition, 2001.
- [3] Cegiela R. Selecting technology for disaster recovery. In: *Proceeding of International Conference on Dependability of Computer Systems*, 2006:160-167.
- [4] Buford J, Jakobson G. Managing dynamic IP services: correlation-based scenarios and architecture. In: *Proceedings of Enterprise Networking, Applications and Services Conference*. 2001:75-81.
- [5] Jaime Blasco. *Clusters and Disaster Tolerant Solutions*. Storage Grid Seminar, 2005, 10.