建设容灾系统的几点思考

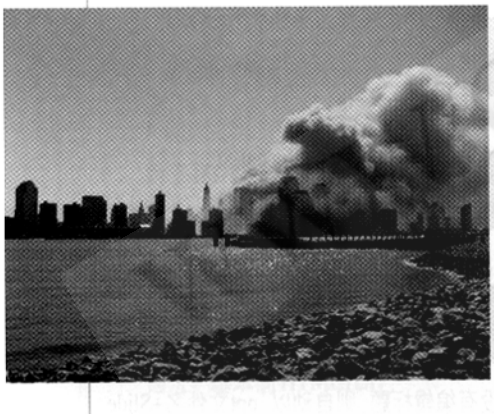
Reflections on Building Disaster-Tolerant Systems

摘要：本文结合目前容灾建设的实际情况，对各种容灾实现方案进行对比，分析不同方案的利弊和适用范围，以及保证容灾建设成功的关键条件等进行了论述，对容灾系统建设能起到一定的借鉴作用。

关键词：容灾

崔可升 （山东移动通信有限责任公司）

王玉春 （山东临沂师范学院）



美国“9.11”事件后，国内对计算机系统的容灾意识普遍得到加强，对于许多企业而言，数据就是企业的生命。因灾难造成数据丢失或业务长时间中断，严重的会造成企业破产，轻微的会影响客户服务质量和企业收入，使大量客户流失。这一严峻的事实使得容灾系统成为许多企业共同的选择。

但容灾系统的建设远远不是投入一笔金钱，在异地建设一套相同的系统。因为容灾是一个系统工程，需要多方面的考虑才能确保其成功。企业应该针对自身的IT应用情况，对数据的重要性和应用的重要程度进行考虑，以下几点供参考。

1 容灾容“什么”？

企业作为一种商业实体，其投入必然是为了有所回报。对于容灾系统的搭建，更应该如此。引起计算机系统毁灭的因素很多，可以是系统中的硬件故障，还可以是因火灾、飓风、地震而引起的数据处理设备的损坏，以及误操作或人为破坏造成数据丢失，数据库崩溃等，只要造成了关键业务的中断，都是灾难。容灾技术就是为恢复计算机系统提供的保证，包括备份中心、备份设备和备份数据等。

所以，企业首先要分析各业务数据的重要性，不同业务允许中断的时间，企业可以为容灾投入多少预算等。

(1) 列出在实施容灾系统前IT系统各项目的情况。把当前使用的IT系统的运行情况进行列表，内容包括应用项目、已采取的备份措施、业务允许中断的时间、恢复的时间（RTO）、数据的损失量（RPO）等进行分析，考虑哪些项目必须实施容灾，哪些项目可以考虑脱机备份，哪些项目目前的状况可以满足等。

(2) 对不同的灾难情况进行列表，看哪些考虑容灾，哪些不考虑容灾。如地震灾难，考虑企业数据和业务的重要性以及企业允许的投资是否考虑，如果考虑，需要建设异地容灾；如果是防范火灾、建筑物破坏等，采用同城容灾即可，两者线路租费差别很大。还有考虑对数据误删除或人为破坏的保护措施，对数据库崩溃的容灾措施等，这些都是保证出现灾难后及时得以恢复的应急措施。

(3) 确定各项目的容灾系统级别，对容灾的投入、恢复时限、业务中断时间等因素进行综合考虑。如图1所示，要求的恢复时间越短，投入和实现难度越大。考虑企业的数据和业务特点以及项目投入，选择合理的容灾级别。

2 如何选择容灾类型？

容灾系统的实现方式有多种，从要求时限的角度分，容灾分非实时和实时两种模式；从实现方式上，容灾可以分应用级容灾、主机级（系统级）容灾、阵列级容灾、数据库级容灾等；实时模式还可以分同步和异步两种运行模式，如主机级、阵列级容灾一般既可以在同步，也可以在异步模式下运行。数据库级容灾既可以是通过同步

©《计算机系统应用》编辑部 http://www.c-s-a.org.cn

写方式的实时模式，也可以是通过数据库归档日志恢复的非实时模式。

非实时模式，可以利用磁带或磁带库备份技术，通过制定备份策略，实现及时的增量备份或全备份，并把介质放到或传输到其他建筑物内。在发生意外时，利用保存的介质进行恢复。这种模式的优点是投资少，备份策略简单，易于实现。缺点是很难保证生产中心与备份中心的实时性一致。该方式比较适合业务重要性较低，数据重要性不高，或数据很少有变化的系统，比如办公系统、MIS系统等。非实时模式的一个优点是可以解决数据变化不大时误操作等带来的数据丢失。

实时模式，就是通过主生产中心和备份中心之间的传输线路，把主生产中心变化的数据实时地传输到备份中心，在灾难发生时，通过由备份中心接管所有或关键业务，实现灾难备份。实时模式又可以分为应用级的实时灾难备份和数据级的灾难备份。数据级的灾难备份是指生产中心的数据经过网络实时地传送到灾难备份中心的系统上，在生产中心发生灾难或故障时，备份中心立即启动相应的运行环境和应用，切换的时间较长。

从实现的难易程度上，实时模式比非实时模式相对难度要大一些，应用级容灾实现比较困难，主要取决于业务的复杂性，业务越复杂，要求越实时，实现起来越难，对软件的质量也越高，尤其是控制数据的一致性比较难，但应用级容灾通过开发软件来实现，可控性强，可以实现基于规则的自动业务切换和接管。阵列级容灾和主机级容灾几乎对应用没有什么改造，对应用来说基本是透明的，但要求阵列厂家或主机厂家具有支持异地容灾的软件。

从设备的依赖性上，主机级容灾要求具有相同厂家的操作系统，如同为IBM的AIX或HP的HP-UX；数据库要求是相同的数据库和操作系统；阵列级容灾要求相同厂家的阵列；应用级容灾基本上是主机、阵列、数据库无关性，但在相同的运行环境，实现起来相对要容易些。

从对生产中心的影响上，应用级容灾对主生产中心的影响程度最小，其次是阵列级容灾。

具体选择何种容灾类型，并非千篇一律，根据企业的实际情况而定，如主机选型、主数据中心与备份数据中心之间的链路连接、容灾系统与其他系统的接口等，企业需要考虑以下几方面：

(1) 考虑业务的特点，哪些业务是关键业务，哪些业务不需要进行容灾；需要接管的业务可以承受的中断时间。对于银行、民航、电信等时限性要求强的系统，需要分钟级的容灾；对于企业的MIS系统、网管系统等，可能需要几个小时甚至几天的时间等。

(2) 对数据的保护程度。但灾难发生时，保证关键数据100%不丢失，或数据可以在最近几分钟丢失等，所采用的容灾方案是不同的。

在了解了自身企业的数据和业务特点后，结合不同容灾方案的特点，确定采用何种类型的容灾方案。

3 如何确保容灾成功？

建设容灾系统的目的，是在灾难发生时，能够派上用场。就像我们布置消防器材一样，在火灾发生时，能够用来灭火，如果这时灭火器失效，后果是可想而知的。如何保证容灾系统的成功？

(1) 合理确定容灾的目标，结合企业自身的资源，确定合理的容灾方案。

(2) 在容灾系统建立之后，还需要建立完善的管理机制，以最大限度地发挥容灾系统地作用。有人说，"容灾更是一种管理策略"，不管IT厂商采用地技术有多好，设计有多高明，这些都只是最初实施地保证，真正到了后期能长期稳定地运营还是在于完善地管理机制。据相关数据显示，容灾系统40%故障率来自人为因素，另40%的故障源自应用系统故障，而只有20%的故障是由于火灾、水灾、地震等天灾造成的。很多企业花费大量的人力、财力去保证20%的天灾，却疏忽了80%的人为故障。忽视管理机制是许多企业经常陷入的一个严重误区，最关键的是怎么保证买的东西能按照既定的策略严格运行。如应急预案的制定，周期性的切换试验，数据的实时一致性检查等，是保证备份系统正常接管的前提。因此，对于实施容灾系统的企业，完善的管理机制是不可缺少的。

4 结束语

灾难是可怕的，但真正的灾难是毫无准备；容灾是重要的，但真正重要的是容灾策略的严格实施。

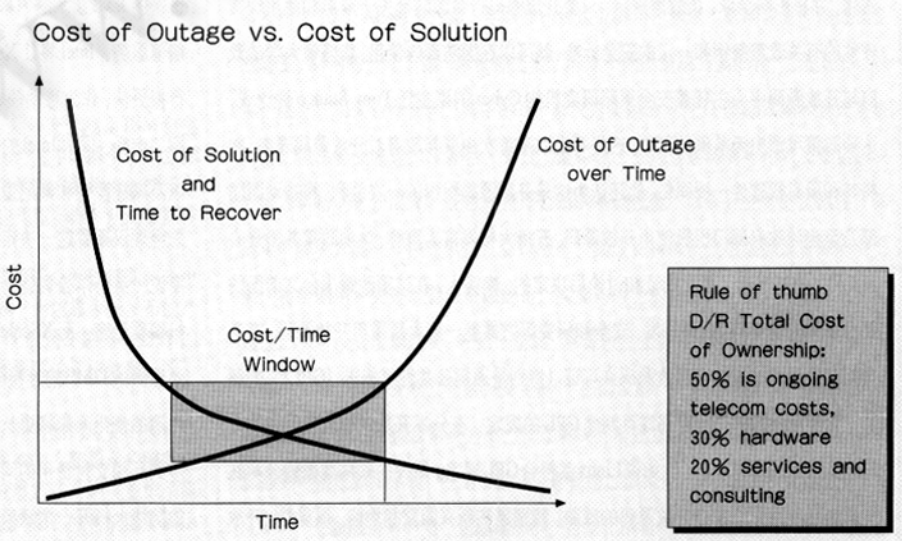


图1 恢复时限与投入关系

©《计算机系统应用》编辑部 http://www.c-s-a.org.cn