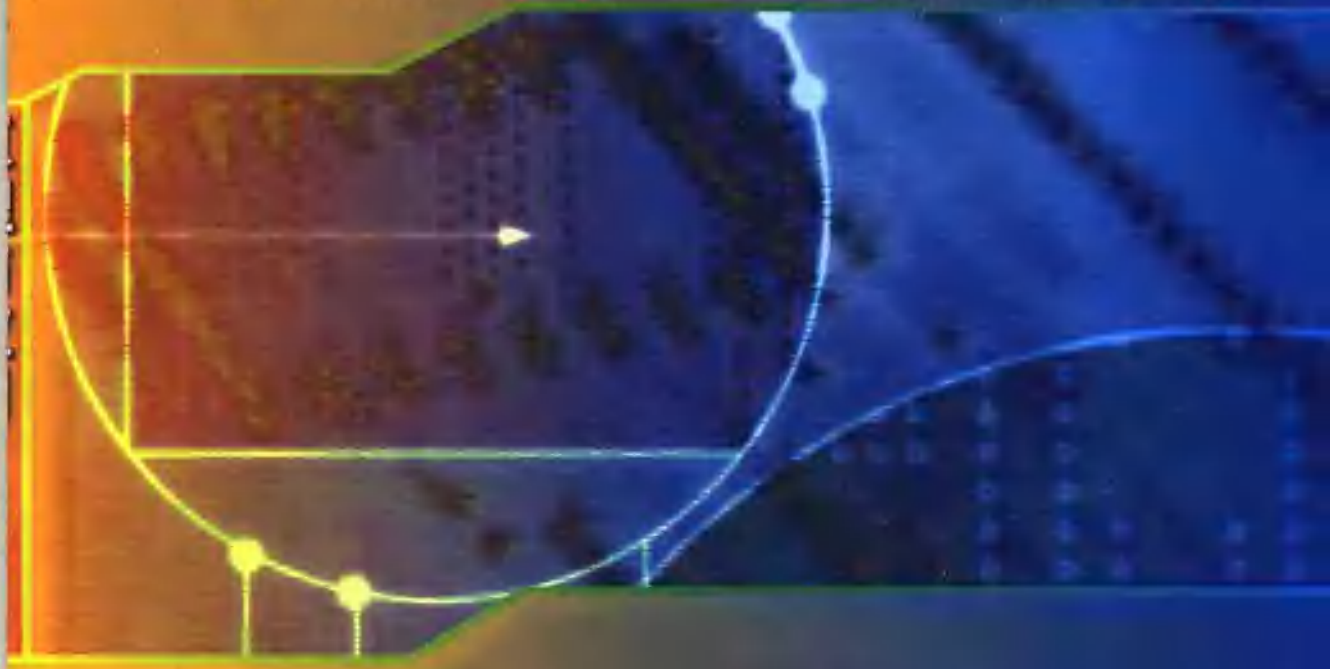
信息通信热点技术应用丛书

信息系统容灾抗毁原理与应用

李 涛 刘晓洁 曾金全 赵 辉 刘才铭 张 冰 编著



人民邮电出版社
POSTS & TELECOM PRESS

信息通信热点技术应用丛书

信息系统容灾抗毁原理与应用

李 涛 刘晓洁 曾金全 赵 辉 刘才铭 张 冰 编著

人民邮电出版社
北京

图书在版编目（CIP）数据

信息系统容灾抗毁原理与应用 / 李涛等编著. —北京：人民邮电出版社，2007.10
（信息通信热点技术应用丛书）
ISBN 978-7-115-16445-2

Ⅰ. 信… Ⅱ. 李… Ⅲ. 信息系统—安全技术—研究
Ⅳ. TP309

中国版本图书馆 CIP 数据核字（2007）第 091873 号

内 容 提 要

本书全面系统地介绍了信息系统容灾抗毁的基本概念、技术与原理，详细论述了信息系统容灾抗毁的体系结构、容灾抗毁目标与等级、容灾抗毁规划问题，全面阐述了信息系统容灾抗毁的关键技术，包括数据容灾、网络容灾、服务容灾等。最后结合实际应用，介绍了信息系统容灾抗毁的实现案例。

本书取材新颖，内容丰富，可作为高等学校计算机、信息技术类本科生和研究生教材，也可供上述领域专业科研及工程人员参考使用。

信息通信热点技术应用丛书

信息系统容灾抗毁原理与应用

◆ 编　　著　李　涛　刘晓洁　曾金全
　　赵　辉　刘才铭　张　冰
责任编辑　陈万寿

◆ 人民邮电出版社出版发行　　北京市崇文区夕照寺街 14 号
邮编　100061　　电子函件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京艺辉印刷有限公司印刷
新华书店总店北京发行所经销

◆ 开本：787×1092　1/16
印张：15
字数：360 千字　　2007 年 10 月第 1 版
印数：1–3 000 册　　2007 年 10 月北京第 1 次印刷

ISBN 978-7-115-16445-2/TN

定价：35.00 元

读者服务热线：(010)67129258　印装质量热线：(010)67129223

前　言

近十年来，互联网技术及其应用所推动的企业全球化以及计算机信息技术的快速发展，使企业信息系统日益占据着企业竞争优势的主体地位。数据的海量增长，使企业比以往任何时候都更加依赖于数据。尤其对银行、电信等企业，信息系统存储的数据关系着企业的收入与利润，关系着企业的生存与发展。任何关键数据的丢失或者信息系统运行的中断，都将导致不可估量的损失。IDC 的统计数字表明：美国最近 10 年发生过灾难的公司中，有 55%当时倒闭；剩下的 45%中，因为数据丢失，有 29%也在两年之内倒闭；生存下来的仅占 16%。

容灾抗毁是信息系统安全运行的最后一道防线。相关容灾抗毁理论及其应用技术的研究，受到了各国政府、学术界以及工业界的高度关注。然而，由于种种原因，目前我国有关信息系统容灾抗毁技术及其产品与美国等西方发达国家相比尚有一定的距离。正因为如此，我们更应加倍努力，迎头赶上。

在这种背景下，为促进我国信息系统容灾抗毁技术的进步与发展，笔者结合多年来在信息系统容灾抗毁研究中的心得，特编拙著，以期抛砖引玉，对我国的网络安全事业略尽微薄之力。

全书共分为 7 章。

第 1 章论述了容灾抗毁的基本概念、相关术语、国内外的容灾抗毁技术和产品现状，同时阐述了信息系统容灾抗毁体系结构。

第 2 章论述了信息系统容灾抗毁的目标和容灾的等级以及为达到每一个容灾抗毁等级应具备的容灾要素。

第 3 章论述了数据容灾技术，包括本地、远程数据容灾技术以及数据存储技术。本地数据容灾技术主要是磁盘 RAID 技术、磁带/磁盘备份技术；远程数据容灾技术包括基于应用、数据库、文件系统、逻辑卷、智能存储系统的数据复制技术。

第 4 章论述了网络容灾——网络可生存性技术。包括全光网络生存性技术、SDH 网络生存性技术、ATM 网络生存性技术、IP 网络生存性技术、MPLS 网络生存性技术等。

第 5 章论述了服务容灾技术，包括失效检测技术、基于 DNS 和 IP 的服务迁移技术以及集群技术等。

第 6 章论述了容灾抗毁规划的各个阶段的主要任务和工作流程，包括项目计划阶段、风险分析阶段、恢复策略选择阶段，以及项目的实施、测试和维护阶段。

第 7 章是应用案例。结合实际的业务系统，给出了几个实际的容灾抗毁实现案例。

本书在编写过程中得到了国家自然科学基金、国家“863”计划、教育部博士点基金、教育部新世纪优秀人才支持计划的支持，对此表示深切的谢意。同时，笔者还要感谢杨频副教授（博士）、赵奎博士、胡晓勤博士、卢正添博士、孙飞显博士、彭凌西博士和刘孙俊博士。他们为本书收集了大量的文献、资料，并进行了细致的整理工作。

由于书稿涉及许多新的内容和研究领域，尽管笔者已经尽了最大的努力，但仍感问题难免，望各位同仁不吝赐教，以利再版修订。

作　者

目　录

此为试读，需要完整PDF请访问：www.ertongbook.com

第1章 概 述

人类对计算机信息系统的依赖正在不断增强，信息系统的脆弱性也日渐明显。“9·11”事件再次说明，灾难的不确定性将对信息系统造成毁灭性的破坏；如何寻求一种有效方式来保护信息系统，已经成为人们关注的热点。信息系统容灾是信息系统安全运行的最后一道防线，其目的是有效保护信息系统的数据，同时维持信息系统所支撑业务的连续运行。本章对信息系统容灾的相关背景、相关术语、容灾系统、容灾标准与规范及容灾系统的体系结构等容灾的基本知识进行概要介绍。

1.1 相关背景

“9·11”恐怖事件至今令人心有余悸，它是人类一次重大的灾难，除了夺走无数无辜者的生命，还带来了巨大的财产损失。同时，它还使得一大批公司因为重要业务数据和客户资料的毁灭而无法恢复运营，最终只得倒闭。这样的结果让全世界的企业意识到：企业信息系统在灾难面前非常脆弱，信息系统的容灾抗毁能力与企业的生存发展息息相关。其实，除了“9·11”这样的人为恐怖事件之外，还有其他许多灾难，如地震、火灾、水灾等自然灾难，以及战争、网络攻击、设备系统故障和人为破坏等无法预料的突发事件，可谓“天灾人祸无所不包”。这些灾难给社会生活带来了巨大的破坏，特别是给人们越来越赖以生存的信息系统及其数据造成了毁灭性的破坏。

1.1.1 灾难对信息系统的破坏

众多事实表明，各种自然灾害和突发事件都有可能导致企业信息系统的瘫痪，甚至带来更为严重的灾难性后果。1993 年，纽约世贸中心发生爆炸，一年后，重新回到世贸中心的公司由原来的三百多家变成了一百多家，有二百多家企业由于无法恢复重要的信息系统数据而倒闭，并最终消失；1999 年 6 月，美国一家著名的商业交易网站的主机宕机，由于 24h 内未能恢复访问，事件发生的两个星期后，该公司的股票值下跌了 36%。IDC 的统计数字表明，美国在 20 世纪 90 年代的 10 年间，发生过灾难的公司中，有 55%当时倒闭。因为数据丢失，有 29%也在两年之内倒闭，生存下来的仅占 16%。国际调查机构 Gartner Group 的数据也表明，在经历大型灾难而导致信息系统停运的公司中有 2/5 再也没有恢复运营，剩下的公司中

也有 1/3 在两年内破产。

随着科学技术的迅猛发展和信息技术的广泛应用，政府及各行业对信息系统的依赖日益增强，尤其是银行、电力、铁路、民航、证券、保险、海关、税务等八大重点行业和部门的信息系统以及电子政务系统已经成为国家的重要基础设施。重要信息系统的安全直接影响到国民经济的正常运行，直接关系到社会稳定和人民群众的日常生活。这就使得人们迫切需要一种能有效保护信息系统的方法，这种方法既能保护信息系统的数据不受损失，又能保证信息系统所支撑的业务不会中断。

更加值得关注的是，信息技术逐渐采用“数据集中”的模式来构架网络信息系统，即各个基层单位子系统所产生的业务数据不再由本地计算机处理和保存，而是集中在数据中心进行统一的处理和存储。这种模式反映了数据存储模型逐步从传统的“分布式存储”模型向先进的“集中式存储”模型转变，在很大程度上提高了信息和数据管理的自动化，提高了效率，降低了成本。但是，由于企业对信息和数据的高度依赖性，对于“数据集中”的应用模式，如果发生的灾难影响到企业数据中心，将不仅导致企业业务中断，而且还会造成企业数据中心所存储的大量数据和信息丢失，甚至遭受破坏。

网络互联技术的发展，使企业可以很方便地联网（包括企业内部网络、企业的合作伙伴网络和企业的用户网络），也使得业务系统可以高效地运行，增强了企业的竞争力和提高了工作效率。随着企业信息化程度的提高，企业对信息系统的依赖性逐渐增强，在企业对信息系统的依赖性增强的同时，企业对信息系统也提出了更高的要求，要求信息系统 7×24h 连续可靠地运行。越来越多的业务通过网络运行，业务的连续性也越来越重要。同时，企业的风险也在不断地增加，灾难所造成的数据丢失和业务中断，可能会导致巨大的损失。市场调研公司 Strategic Research Corporation 的研究报告指出，各行业在遭受灾难打击造成服务中断时所带来的损失是十分巨大的：证券业每小时的平均损失为 650 万美元，信用卡服务每小时平均损失为 260 万美元，ATM 系统中断造成的每小时损失为 14500 美元，而各行业中断服务平均每小时损失为 84000 美元。

1.1.2 信息系统容灾的重要性

为了降低灾难对计算机信息系统造成的影响和保证业务的连续运行，容灾技术应运而生。信息系统容灾是信息系统安全运行的最后一道防线，它通过特定的容灾机制，在灾难发生后，能够确保信息系统连续运行。信息安全是一个企业持续发展的重要保障，信息系统的容灾因而成为企业最迫切需要解决的问题之一。尤其是在“9·11”事件之后，越来越多的企业认识到信息系统容灾的重要性，纷纷采取了相应的容灾措施，建立了容灾中心。

信息系统的容灾是减少灾难造成的损失和保证计算机系统连续运行的重要手段，越来越多的企业已经采用或者准备采用容灾技术来减少灾难带来的损失。由于有 1993 年爆炸的前车之鉴，世贸中心的部分公司建起了自己的容灾系统，因此，在“9·11”事件后，有一批公司仍可及时地通过容灾措施来重整旗鼓。而另外一些企业，则在“9·11”事件后因丢失了关键业务数据和暂停了业务服务而倒闭。

容灾最初实现的目的还只是为了数据的备份，但规模很小。最先出现的容灾技术是通过磁带备份并在异地保存，当互联网快速发展起来后，才得以利用网络实现容灾。随着网络技

此为试读，需要完整PDF请访问：www.ertongbook.com

术的发展，网络带宽得到了提高，数据备份和数据恢复便可以通过网络实现，容灾系统的范围也不断扩大。目前，容灾已成为许多研究机构研究的热点，很多公司也开发出了容灾的相关产品，并且越来越多的容灾解决方案被企业所采用并投入实际运行。

灾难是难以避免的，但我们可以在灾难发生前做好发生灾难时的准备，特别是对于人们越来越依赖的信息系统，容灾工作势在必行。通过近年来灾难给信息系统带来的巨大损失可知，提前做好容灾准备完全可以消除或降低灾难带来的不良影响。容灾对信息系统的保护作用主要体现在以下几个方面。

- 减少企业因灾难而造成的损失。对产品和服务的全天候可用性的要求迫使企业在业务的每个方面都越来越依赖于信息系统。技术快速发展的同时带来了新的灾难类型的发展，同时也使企业业务越来越易受到灾难的威胁。当出现与企业信息系统有关的灾难时，企业对信息系统不断增加的依赖性将导致严重的后果。容灾技术能够有效保护信息系统的重要数据，减小企业经济利益的损失、客户的流失和对企业形象的负面影响，并能使灾难对企业的影响降到最低。
- 保护关键资源和业务流程。要确保业务连续性，就需要识别和保护关键的资源和业务流程。容灾技术能够最大限度地保障信息系统的运行，这增强了企业的生存能力，也保护了商业伙伴的利益。
- 在尽可能短的时间内恢复企业业务。在出现影响信息系统的灾难时，所有依赖它的重要功能，如通信和交易，都将受到严重影响。也许企业能在业务中断的情况下维持一段时间，但是长期的中断将使企业破产。容灾技术对业务数据以及业务状态数据进行备份，在生产中心发生灾难时，企业的业务能快速切换到容灾中心，使企业业务能快速恢复运行。
- 履行合同义务。直接向消费者或客户提供产品和服务的企业在履行义务时要受到协议的约束。供应商在这些协议中保证：在出现灾难时，他们将不受阻碍地继续提供服务。容灾技术能保障信息系统的连续运行，使企业能高质量地完成对客户的承诺。

1.2 相关术语

在本书中，会用到一些容灾技术术语，这些术语可能会区别于计算机领域或其他领域的相同名词。为了更好地理解本书内容，下面对容灾技术中广泛使用的术语做一个概括性的介绍。

1. 灾难

从广义上讲，对于一个计算机信息系统而言，一切引起系统发生严重故障、非正常停机、信息系统支持的业务功能停顿或服务水平不可接受的事件都称之为灾难。《灾难恢复杂志》（DRJ）将灾难定义为“造成机构的某一部分无法在预定的一段时间内提供关键业务功能的事件”。从狭义上讲，灾难主要指地震、洪水、火灾、飓风和海啸等自然灾害，它们会对信息系统的硬件设备及其建筑物造成毁灭性的破坏。

2. 容灾

容灾是指在灾难发生时确保企业正常经营活动保持连续性的过程。这个过程不仅着眼于

企业主要功能和系统的恢复，而且强调在尽可能短的时间内恢复它们。

3. 容灾技术

容灾技术是指为防止信息系统在遭受诸如人为破坏、战争、火灾、水灾和地震等灾难时造成系统服务停止和数据丢失而采取的解决方案。

4. 生产中心

生产中心是指在正常情况下，企业信息系统运行所在地（包括支持企业业务应用系统正常运行所需的机房、数据存储设备、主机设备、网络设备及相应的办公配套设备等硬件设施，相应的应用软件和系统软件）。

5. 容灾中心

容灾中心是指为了减少灾难给企业造成的损失而在异地建设的一套生产中心的同级克隆或降级克隆（包括与生产中心相一致的机房、数据存储设备、主机设备、网络设备及相应的办公配套设备等硬件设施，以及相应的应用软件、系统软件），在灾难（生产中心不能处理的灾难）发生后，容灾中心接管生产中心的业务，保证企业业务的连续性。

6. 容灾外包

容灾外包是指单位选择外部专业技术与服务资源替代内部资源来承担容灾系统的规划、建设、运营、管理和维护。

7. 容灾规划

容灾规划是指为了减少灾难对业务信息系统的关键业务流程造成的影响而采取的一系列的阶段和行为。

8. 业务影响分析

业务影响分析是指分析业务功能及其相关信息系统资源，评估特定灾难对各种业务功能的影响。

9. 关键业务功能

关键业务功能是指如果中断一定时间就将显著影响企业或单位运作的服务或职能。

10. 容灾演练

容灾演练是指用于训练人员和提高灾难恢复能力的活动，包括桌面演练、模拟演练、操作演练和演习等。

11. 应急响应

应急响应是指为了应对紧急事件（包括系统故障和自然灾难等），尽量减少紧急事件对企业业务或单位的职能带来的影响而采取的措施。

12. 应急响应计划

要在最短的时间内达到最快的恢复，就需要制作一个路线图，详细说明在灾难之前、之中和之后应当采取的行动，这个路线图被称为应急响应计划。应急响应计划是一组内容广泛的声明，用于解决可能损害企业的灾难性问题。执行应急响应计划的目的在于不管引起灾难的原因是什么，都要确保快速、有效和经济地恢复企业业务的连续运行。

1.3 容灾系统

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。容灾的实现主要通过在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。

信息系统是一个由数据处理系统和网络互联系统等组成的复杂系统，其对应的容灾系统主要由备份数据处理系统和备份通信网络系统组成。为了成功地实施容灾备份和保证在灾难发生的情况下有条不紊地进行灾难恢复，还必须有完善的容灾抗毁规划。

数据是企业的生命和灵魂，数据的破坏和不可恢复性，将导致整个容灾的失败。因此，数据容灾是整个容灾系统的基础和关键所在。目前，由于独立的而不与其他系统互联的应用系统越来越少，而基于网络互联的应用越来越普遍，因此，网络的中断将导致业务的停顿、信息服务的不可用，这个问题可以用网络容灾来解决。对用户而言，要求在任何时刻（即使在灾难发生时）服务都保持可用。为了实现业务的连续可用性，必须保证在灾难发生时，服务能够快速迁移，而且对用户保持通明，使用户感觉不到灾难的发生和服务的迁移，这正是服务容灾要解决的问题。除此之外，还必须制定容灾规划，确保容灾的成功实施。

综合容灾系统的主要功能，一个容灾系统应包括数据容灾、网络容灾、服务容灾和容灾规划等几个主要部分。

1.3.1 数据容灾

在容灾系统的建设中，要成功地实施容灾，数据容灾是最重要的问题之一。如何将数据（包含系统、应用和业务等数据）实时完整地复制到容灾中心，是企业容灾系统建设中需要考虑的首要事项。随着 IT 技术的不断发展和容灾技术的日趋成熟，有多种数据容灾技术可供选择。

可以根据不同的划分标准对数据容灾技术进行分类。一种是按照距离的远近来进行划分，可分为本地数据容灾技术和远程数据容灾技术。本地数据容灾技术（如磁带备份和磁盘 RAID 技术等）相对比较成熟，但只能抵御一些局域的灾难（如本地磁盘损坏），而不能抵御大范围的灾难（如地震），因此，目前主要的研究领域是如何实现跨地域的远距离数据容灾。另一种划分方式是根据容灾技术的实现层面将容灾技术分为基于硬件的和基于软件的方式。基于硬件的方式主要是通过智能存储设备来完成，而基于软件的方式由数据库和逻辑卷管理等软件来完成。

1．基于智能存储设备的数据容灾技术

基于智能存储设备的远程数据容灾技术是以磁盘系统为基础，利用磁盘控制器提供的功能，采用磁盘镜像技术在物理磁盘卷级上实现两地磁盘系统之间数据的复制。这种方式独立于主机和主机操作系统，不占用主机 CPU、主机通道和网络资源，对应用透明，不需要对现有应用系统做任何改动和变化。

2．基于软件的数据容灾技术

基于软件的数据容灾技术包括采用数据库方式和服务器逻辑卷等方式，通过通信网络，实现数据在本地生产中心和远程容灾中心之间的实时备份，保证两中心之间的数据同步。但这种方式一般占用主机的资源，增加了主机的处理负担。

3．其他数据容灾技术

还可以利用其他一些数据远程复制技术来实现数据容灾，如通过磁带库备份技术实现数据远程备份解决方案。

1.3.2 网络容灾

网络容灾是指在网络出现故障或遭受灾难时，采用相应的技术手段使网络性能仍能维持一个可接受的服务水平。目前的网络基础设施是一个包括传送网和业务网的复杂的网络结构，在不同的网络层可以采用不同的网络容灾技术，如全光网络容灾技术、SDH 网络容灾技术、ATM 网络容灾技术、IP 网络容灾技术和 MPLS 网络容灾技术。每一层的网络容灾技术都具有自己的优点，但也存在一些缺点。如低层网络容灾技术恢复速度快，可有效地用来恢复资源。但是，其恢复粒度粗，不能针对具体的业务进行恢复。因此，为了发挥各层容灾机制的优势，出现了多层网络的容灾技术。

1.3.3 服务容灾

服务容灾是指在灾难发生时，为了保证服务快速有效地迁移和保持业务连续性所采用的技术。在服务容灾中首要的技术是失效检测技术，确保在灾难发生时，快速、准确地检测到服务的中断或不可用。其次是服务的迁移，确保服务在生产中心和容灾中心之间无缝迁移，当灾难发生时，使用户感觉不到服务已经发生了迁移，保持服务的连续可用性。本书主要讨论服务迁移的以下几种技术：基于 DNS 的服务迁移技术、基于 IP 的服务迁移技术和基于集群的服务迁移技术。

1.3.4 容灾规划

为了确保容灾的成功实施，必须制定容灾规划，详细描述在灾难之前、之中和之后做什么，怎么做；制定在项目实施的各个阶段的任务和工作流程，确保人、技术、流程三要素的

有机结合。容灾规划将容灾活动划分为以下几个步骤：项目计划阶段、风险分析阶段、恢复策略选择阶段、项目实施阶段、项目测试阶段和维护阶段。制订容灾规划的目的，是要保证在灾难发生时有条不紊地进行灾难恢复，以减少灾难带来的损失，并及时有效地恢复业务的运行。

1.3.5 容灾相关产品

随着信息系统在各行业的广泛应用，各种业务的运行对信息系统的依赖程度在不断加大，越来越多的企业意识到数据保护和信息系统所支撑业务连续运营的重要性，企业在容灾建设上逐渐加大投入，这促使了各行业对容灾产品的需求越来越大。在一些标准组织和存储领域企业的进一步推动下，逐渐涌现出许多用于容灾的软硬件产品及其解决方案，各种容灾产品从不同的技术角度满足了不同类型容灾的要求。Veritas、IBM、EMC 和 HP 等知名企业都提供了容灾的相关技术和解决方案。下面介绍一些企业具有代表性的容灾相关产品和解决方案。

1. Veritas 容灾相关产品

Veritas 公司已被 Symantec 收购，但为了读者更好地了解其容灾相关产品，下面仍以 Veritas 冠名进行介绍。Veritas 公司的容灾系统可分为三个部分：备份中心主机网络存储系统以及应用系统、生产中心与备份中心的数据同步传输系统和基于广域网的集群系统。

远程数据同步复制的实现又包括有足够带宽的网络连接和数据复制管理软件两个部分。数据复制管理软件采用 Veritas 的 VVR（Veritas Volume Replicator）。VVR 是一个灵活和高性能的基于逻辑卷的复制软件，它采用可靠的连接和监听协议，可向远程备份系统同步进行逻辑卷复制。VVR 支持广域网节点间数据的同步和异步复制，支持多点到多点的复制。VVR 属于从操作系统的级别对信息系统进行容灾备份。基于操作系统的容灾技术主要以软件的形式实现。采用软件数据复制方式具有配置灵活、价格低、性能高等特征，其缺点是主机资源占用大，复制的压力大。一个大型系统，如果既要保证系统能正常运行，又要做大量的复制和备份工作，系统性能会受到一定的影响。

Veritas 的 GCM（Global Cluster Manager）软件可实现广域网的集群管理。GCM 软件可与 VCS（Veritas Cluster Server）有机集成，从单控制台管理多达 32 个地域的 VCS 集群系统，实时监测每个 VCS 集群的运行状况，并可根据用户应用要求制定多种切换策略。当某个地域发生故障或灾难而导致该地域的集群终止时，GCM 会马上检测到，并可根据策略自动或手工快速地将应用切换到远程的集群。

2. IBM 容灾相关产品

IBM 公司根据异地远程容灾的需要，提出基于大型计算机主机的容灾技术，即跨域并行系统耦合体技术 GDPS（Geographically Dispersed Parallel Sysplex）。GDPS 是一种多站点应用可用性的解决方案，具有管理远程拷贝配置和存储子系统、自动执行并行耦合体操作任务、从单一控制点执行故障恢复等功能，从而达到了提高应用可用性的目的。

在 GDPS 的方式下，IBM 推出了两种远程数据拷贝功能。一种是基于同步数据复制方式的端到端远程复制技术 PPRC（Point-Point Remote Copy），远程备份距离可达 100km；另一

种被称为扩展远程拷贝 XRC（Extended Remote Copy），提供广域网范围的数据备份，一般采用异步方式。PPRC 和 XRC 在远程复制控制机制下自动对 DASD（Direct Access Storage Device）卷上的数据进行跟踪。这种跟踪的发生独立于这些数据的应用。因此，不需要对不同应用提供独立的远程复制功能。PPRC 和 XRC 都试图通过维护 DASD 卷间的实时复制来达到数据保护的目的。PPRC 提供有助于保留数据当前值和完整性的两类选择。可以选择将卷标记为“关键”，保证在副卷不能更新时，原有的更新也无效，不论卷是处于同步状态还是异步状态，甚至是在灾难发生时也如此。

IBM-DB2-HADR 和 IBM-INFORMIX-HDR 从数据库的级别对信息系统进行容灾备份。基于主机的数据库复制是指把数据从主数据库服务器复制到从数据库服务器，二者通过 TCP/IP 建立连接。数据库复制技术可以提供一种可靠、即时的备份机制。除此之外，数据库复制技术还具有一大优点，即作为备份的从服务器可用于一些只读操作，以分担主机的部分负载。主数据库服务器在把逻辑日志缓冲区中的内容写到磁盘之前，先将其拷贝至数据复制缓冲区，数据复制缓冲区的内容在满足一定条件时通过 TCP/IP 由网络传送到从服务器一端的数据复制缓冲区中。再从服务器一端，接收数据复制缓冲区的内容并将其存入恢复缓冲区，同时根据这些逻辑日志记录操作数据库，从而实现从服务器对主服务器的备份。这种方案虽然开支较小，但是增加主系统开销，如果做到同步，会使延迟增大，并且这种方案也仅仅实现了数据级的容灾备份，缺乏应用级容灾备份的状态检测、应用切换和数据库以外的其他数据恢复等。

IBM-ESS-PPRC 和 IBM-DS4000-RM 从存储设备层进行容灾备份。基于存储设备的数据复制技术又称为智能存储系统的远程镜像，它的数据复制是在存储系统内部实现的，与主机和应用系统无关。这种方案与应用无关，并且一般都能够保证数据复制的同步性，但是由于受采用的传输介质、传输技术和同步响应时间的限制，存在生产中心与容灾中心距离上的限制。

3．EMC 容灾相关产品

EMC 公司的远程数据备份软件 SRDF（Symmetrix Remote Data Facility）是一个在线的并且独立于主机的数据镜像存储解决方案，可在多种操作系统下使用，它能够同时为大型机、UNIX、Windows NT 和 AS/400 系统提供完整的业务连续可用性能力。数据复制通道既可以采用传统的 IP 网络，也可支持光纤通道、T1/T3、E1/E3、ATM 和波分多路复用等多种方式。EMC SRDF 可在多达 16 个本地或远程的磁盘 Symmetrix 系统间提供完整的数据备份。在生产中心操作发生故障时，系统管理人员可以快速地从主系统切换到备份系统。当主节点的故障排除之后，通信连接被重新建立，SRDF 能够自动地在节点之间进行数据同步，从而使正常的操作得以恢复。

4．HP 容灾相关产品

HP 容灾解决方案由主数据中心和备份中心组成，它们通过光纤或电信网连接。主数据中心系统配置包括两台或多台 HP UNIX 服务器以及其他相关服务器，通过 HP 的 MC/ServiceGuard 软件组成多机高可靠性环境。数据存储在主数据中心存储磁盘阵列中，同时在异地备份中心配置相同结构的存储磁盘阵列和一台或多台备份服务器。主、备中心距离

此为试读，需要完整PDF请访问：www.ertongbook.com