信息系统灾难恢复体系结构*)

张 艳[1] 李 强[2] 李舟军[3] 何德全[1]

(四川大学数学学院 成都 610064)[1] (湖南师范大学数学与计算机科学学院 长沙 410081)[2]

(北京航空航天大学计算机学院 北京 100083)[3]

摘 要 灾难备份与恢复技术能够充分保证灾难发生时,信息系统仍能正常工作,目前已成为信息安全领域一个备受瞩目的研究方向。本文参考 IBM 公司 SHARE78 的 7 个灾难恢复等级,将灾难恢复系统分为数据级、系统级和应用级 3 个层次。根据这种层次划分,重新合理地定义了 9 个灾难恢复等级,并对各个等级详细地给出了定性的说明和定量的规定。本文提出了信息系统的灾难恢复体系结构,并用三维模型描述了灾难恢复指标、备份与恢复技术和灾难恢复计划与措施之间的关系,从而为信息系统的灾难恢复提供了一个完整的框架和解决方案。

关键词 信息系统,灾难备份,灾难恢复

Disaster Recovery Architecture of Information System

ZHANG Yan[1] LI Qiang[2] LI Zhou-Jun[3] HE De-Quan[1]

(School of Mathematics, Sichuan University, Chengdu 610064)[1]

(School of Mathematics and Computer Science, Hunan Normal University, Changsha 410081)[2]

(School of Computer Science and Engineering, Beihang University, Beijing 100083)[3]

Abstract Disaster backup and recovery technology can efficiently ensure the information system to work normally when the disaster occurs, so it becomes a very important field in information security. In this paper, based on the 7 tiers of disaster recovery solutions defined by SHARE 78 of IBM, the disaster recovery system is partitioned into data level, system level and application level. According to these levels, the 9 tiers of disaster recovery solutions are redefined reasonably, and each of them is qualitatively explained and quantitatively prescribed. The disaster recovery architecture of the information system is presented, and the relation among disaster recovery objects, backup and recovery technologies and disaster recovery plans and measures, is described in a three-dimensional model, in order to provide the whole disaster recovery framework and solution of the information system.

Keywords Information system, Disaster backup, Disaster recovery

1 介绍

随着计算机的广泛应用,存储在计算机系统中的数据已成为最宝贵的财富。数据的丢失将造成难以估量的损失,同时对系统的连续可用性的要求也在不断提高。但是,由于各种原因,人们无法预测和防止计算机系统灾难的发生,使得人们对数据的安全性越来越担忧。尤其自"9.11"事件以来,如何更好地保护重要数据,保证计算机系统连续、安全运行,已成为研究热点[1~3]。灾难恢复系统能避免由于各种软硬件故障、人为误操作和病毒侵袭等所造成的损失,并且在发生大范围灾害性突发事件时,充分保护系统中有价值的信息,保证系统仍能正常工作[1,4,5]。

灾难恢复系统通过在异地建立和维护一个备份系统,利用地理上的分散性来保证数据对于灾难性事件的抵御能力。设计一个灾难恢复系统需要考虑多方面的因素,包括:备份/恢复的范围、生产系统和备份系统之间的距离和连接方法、灾难发生时系统要求的恢复速度以及能容忍丢失的数据量、备份系统的管理和经营方法,以及可投入的资金多少等。根据这些因素,IBM 公司的 SHARE 78 标准[4](1992 年)将灾难恢复系统划分为 7 个等级。

0 级 没有异地数据(No off-site Data):数据仅在本地进行备份恢复,没有数据送往异地。事实上,这一级并不真正具备灾难恢复的能力。

1 级 PTAM 卡车运送访问方式(Pickup Truck Access Method):设计一个应急方案,备份关键数据并将其存储在异地,相对来说成本较低,但难于管理。

2 级 PTAM 卡车运送访问方式+热备份中心(PTAM + Hot Center):1 级加上拥有足够的备份设备来支持关键数据恢复的热备份中心。

3 级 电子链接(Electronic Vaulting):在 2 级的基础上用电子链接取代卡车,进行数据的传送。由于热备份中心要保持持续运行,增加了成本,但提高了灾难恢复速度。

4 级 活动状态的备份中心(Active Secondary Center):两个中心同时处于活动状态并同时互相备份业务数据。

*)国家自然科学基金项目(60073001, 90104026, 60473057)、国家"十五"科技攻关计划项目"银行计算机灾难恢复系统研究"(编号:2001BA102A07-04-01)。张 艳 博士研究生,研究方向为计算机网络与信息安全、灾难备份与恢复;李 强 硕士研究生,主要研究方向为灾难备份与恢复;李舟军 博士,教授,博士生导师,主要研究方向为进程代数理论、安全协议的形式化验证、灾难备份与恢复、数据仓库与数据挖掘;何德全 中国工程院院士,博士生导师,研究方向为计算机网络与信息安全。

5级 两中心两阶段提交(Two-Site Two-Phase Commit):采用两阶段提交来同步两个中心的数据。在灾难发生时,仅仅丢失传送中尚未完成提交的数据。

6级 零数据丢失(Zero Data Loss):灾难恢复的最高级别,可实现零数据丢失和故障自动切换。

尽管人们对灾难恢复进行了广泛的研究,提出了多种用于灾难恢复的信息技术[1,4,6]和管理灾难恢复的计划和措施[7~9],但只是从某一个方面来考虑,未从整体上形成一个灾难恢复系统的框架,很难根据具体情况和应用需求为信息系统选择一个合适的灾难恢复解决方案。SHARE 78的分级方式主要以业务数据的备份与恢复为中心,只是在一定意义上保证业务数据的完整性,对系统和应用的备份与恢复没有进行深入研究,没有考虑到信息系统提供的服务的完整性、可靠性和安全性以及如何向用户提供透明的不间断服务。

为此,本文对该分级方式进行了扩展和改进,将灾难恢复系统分为数据级、系统级和应用级3个层次,根据这3个层次重新制定了灾难恢复等级,并对各个等级详细地给出了定性的说明和定量的规定。本文对灾难备份与恢复的多个方面进行了分析与综合,以灾难恢复等级为中心,提出了信息系统的灾难恢复体系结构,并用三维模型描述了灾难恢复指标、备份与恢复技术和灾难恢复计划与措施之间的关系,从而为信息系统的灾难恢复提供了一个完整的框架和解决方案。

<table>
<tr><td rowspan="2">灾难恢复层次</td><td>灾难恢复等级</td><td colspan="2">备份与恢复技术</td><td>衡量指标</td><td colspan="3">计划与措施</td></tr>
<tr><td>第0级:无异地备份数据</td><td colspan="2"></td><td rowspan="9">RPO
RTO
NRO
DOO</td><td colspan="3">无应急计划</td></tr>
<tr><td rowspan="4">数据级容灾层</td><td>第1级:备份介质异地存放</td><td colspan="2">数据拷贝</td><td rowspan="8">风险分析、应急决策、意识培养和培训、计划的维护和演练</td><td rowspan="8">数据备份与恢复计划</td><td></td></tr>
<tr><td>第2级:备份介质异地存放及存在备用系统</td><td colspan="2">设备备份</td><td>设备保护</td></tr>
<tr><td>第3级:数据电子传输</td><td colspan="2">电子链接</td><td rowspan="2">网络恢复策略</td></tr>
<tr><td>第4级:定时数据备份及活动状态的备份中心</td><td>快照等技术</td><td rowspan="4">存储网络与互联技术</td></tr>
<tr><td rowspan="2">系统级容灾层</td><td>第5级:实时系统备份及活动状态的备份中心</td><td>异步镜像和复制</td><td rowspan="2">系统、用户、应用恢复策略</td></tr>
<tr><td>第6级:实时数据和系统备份</td><td>同步镜像和复制</td></tr>
<tr><td rowspan="2">应用级容灾层</td><td>第7级:灾备系统实时切换</td><td>集群技术和远程动态监测等</td><td rowspan="2">业务连续性运行方案</td></tr>
<tr><td>第8级:零数据丢失和业务连续可用性</td><td>自动应用切换等</td></tr>
</table>

图1 信息系统的灾难恢复体系结构

2 信息系统的灾难恢复体系结构

本文提出了信息系统的灾难恢复体系结构(如图1所示),根据处理的数据和系统的功能将体系结构划分为数据级、系统级和应用级3个层次;根据这些层次重新定义了9个灾难恢复等级,为对灾难恢复等级进行量化分析,引入4个衡量指标;同时,给出了贯穿于体系结构各个层次的备份与恢复技术和灾难恢复计划与措施。

2.1 灾难恢复系统的层次

数据级容灾层:数据容灾指建立一个异地或本地的数据系统,作为生产系统关键业务数据的一个备份。数据级容灾系统需要保证业务数据的完整性、可靠性和安全性,而对于提供实时服务的信息系统,用户的服务请求在灾难中会中断。数据级容灾只是对业务数据备份,不对系统数据与应用程序进行备份,需要通过安装盘重新安装来进行系统的恢复。

系统级容灾层:不但进行业务数据的备份,而且要对信息系统的系统数据、运行场景、用户设置、系统参数、应用程序和数据库系统等信息进行备份,以便迅速恢复整个系统。系统级容灾系统需要同时保证业务数据和系统数据的完整性、可靠性和安全性。在网络环境中,系统和应用程序安装起来并不是那么简单:必须找出所有的安装盘和原来的安装记录进行安装,然后重新设置各种参数、用户信息、权限等等,这个过程可能要持续好几天。因此,最有效的方法是对整个系统进行备份。这样,无论系统遇到多大的灾难,都能够应付自如。系统级容灾同数据级容灾的最大区别在于:在整个系统都失效时,用灾难恢复措施能够迅速恢复系统。而数据级容灾则不行,如果系统发生了失效,在开始数据恢复之前,必须重新装入系统。数据级容灾只能处理狭义的数据失效,而系统级容灾则可以处理广义的数据失效。

应用级容灾层:应用级容灾系统提供不间断的应用服务。在灾难发生时,让用户的服务请求能够透明(用户对灾难的发生毫无觉察)地继续运行,保证信息系统所提供服务的完整性、可靠性和安全性。应用级容灾要同时进行业务数据和业务应用的异地备份。当某地方的一个应用节点突然停掉的话,容灾系统能够在另外一个地方启动相同的应用。这就需要建立一个同生产系统功能完全一致(包括数据与应用的一致)的备份系统。在未发生灾难的情况下,生产系统提供信息服务,备份系统则实时跟踪生产系统的处理,备份生产系统的相关信息,保证在灾难发生时,能将信息服务功能切换到备份系统,承担生产系统的职责,抵御灾难,而且服务对于用户完全透明,没有任何损失和影响。应用级容灾是在数据级容灾和系统级容灾的基础上,增加对整个应用的实时备份,使得实现的难度大、费用高,因此一般用于对业务连续性要求很高的系统(如银行业务系统)中。目前国际上对于灾难恢复系统的研究已经由数据的备份及恢复转向系统的连续可用性[2,4,7,8]。

2.2 灾难恢复等级

灾难恢复等级是整个体系结构合理、协调工作的核心。

根据企业确定的灾难恢复等级目标，可选取体系结构中的相应技术和规划措施来统筹考虑，将其集成起来，统一、协调地工作，从而为信息系统提供整体的灾难恢复解决方案。本文参考 SHARE 78 标准所给出的 7 个等级，根据容灾层次，重新合理地定义了 9 个灾难恢复等级，对各个等级给出了详细的规定和说明，并用灾难恢复指标对灾难恢复等级进行了定量的分析。

第 0 级 无异地备份数据：数据仅在本地进行备份和恢复，不需要将其送往异地，不需要建立备援硬件平台，未制定灾难恢复计划，因而不具备灾难恢复的能力。

第 1 级 备份介质异地存放：要求设计一个数据备份方案，根据该方案在平时备份所需要的信息，并通过 PTAM 方式将数据拷贝（一般是磁带拷贝）运送到异地保存。没有可用的能恢复数据的系统，未制定灾难恢复计划。灾难发生时，将根据需要有选择地建立备援的硬件平台并在其上恢复数据，但事先并不提供处理数据的硬件平台。这种灾难恢复方式相对来说成本较低，但由于在灾难发生时需要临时建立系统和应用平台，恢复的时间长，且数据不够新。

第 2 级 备份介质异地存放，有备用系统：第 1 级再加上具有热备份能力的备用系统，并制定了相应的灾难恢复计划。备用系统拥有足够的硬件和网络设备，来维持关键应用的安装需求。这种灾难恢复的方式依赖于 PTAM 方式，将日常数据放在异地存储。当灾难发生的时候，再将数据恢复到备用系统上。灾难备份的时间没有减少，但却明显减少了灾难恢复的时间，系统可在几天内得以恢复。

第 3 级 电子链接：在第 2 级的基础上，采用电子链接来传输关键数据。电子链接将磁带备份后更改的数据进行记录，并传到备份中心，使用此种方法会比使用传统的磁带备份更快地得到新数据。所以，当灾难发生后，只有少量的数据需要重新恢复，恢复时间会缩短。由于备份中心要保持持续运行，与生产中心间的通讯线路要保证畅通，增加了运营成本。但消除了对运输工具的依赖，提高了灾难恢复速度。

第 4 级 定时数据备份及活动状态的备份中心：第 4 级对数据的实时性和快速恢复性要求更高些。1～3 级方案通常使用磁带备份，第 4 级开始使用基于磁盘的解决方案。此时仍然会出现几个小时的数据丢失，但同基于磁带的解决方案相比，通过加快备份频率，使用最近时间点的快照拷贝[10]，恢复数据会更快。系统可在一天内恢复。第 4 级灾难恢复可有两个中心同时处于活动状态并管理彼此的备份数据，允许备份行动在任何一个方向发生。工作负载可在两个中心之间分享，中心 1 成为中心 2 的备份，反之亦然。在两个中心之间，彼此的部分关键数据通过通信网络定时批量地相互传送着。在灾难发生时，需要的关键数据通过网络可迅速恢复，但是该系统会丢失最近一次数据复制以来的业务数据，其它非关键业务数据也将需要手工恢复。

第 5 级 实时系统备份及活动状态的备份中心：在第 4 级的基础上对业务数据、系统数据、运行场景、用户设置、系统参数等信息进行实时备份。采用异步的磁盘、软件、数据库镜像[6,11,12]或异步的卷、文件系统、数据库复制技术[6,13]将数据实时备份至备份中心，可在备份中心利用实时备份数据和通过网络的切换，快速恢复整个系统，业务的恢复时间降低到了小时级。

第 6 级 业务完整性：生产中心和备份中心由高速的宽带连接，数据在两个中心之间相互映像。采用同步镜像或复制技术，同时更新本地和远程的数据。只有当两地的数据都完成更新后，才认为此次业务处理成功，要求保证生产中心与备份中心的数据的一致性。当灾难发生时，仅仅丢失传送中尚未完成提交的数据，由于恢复数据的减少，恢复时间也大大缩短。恢复的时间降低到了小时级或分钟级。

第 7 级 应用可用性：灾难发生时，几乎不丢失数据并能将应用切换到备份中心。这一级采用集群技术和远程动态监测[14]，生产中心和备份中心都必须能够运行相同的应用和访问相同的数据。中心之间除了网络连接，还需要专线做心跳监测。远程动态监测通过心跳线实时监测主机及其应用的状态。当主机或应用发生故障时，会马上监测到并将故障情况向管理员报警，然后手工快速地将应用切换到远程的主机上。当生产中心发生故障时，除了很短的响应延迟外，客户一般不会有什么影响。

第 8 级 零数据丢失和业务连续可用性：在第 7 级的基础上，集成了自动应用切换的功能。在保证数据一致性的同时，增加了应用的自动切换功能，使得系统和应用恢复的速度更快、更可靠。第 8 级在本地和远程的所有数据被更新的同时，采用了双重在线存储和完全的网络切换技术，可以实现零数据丢失和业务连续可用性，是灾难恢复的最高的级别，最昂贵也是速度最快的恢复方式。

第 4 级到第 8 级采用的存储网络和互联技术[8]是灾难恢复系统中数据访问的基础设施和提供完整、可靠、安全服务的保障，它使用不同的介质（如 100Base-T 以太网、千兆以太网、ATM、FDDI、光纤信道和 InfiniBand）和协议（如 SCSI、ESCON、FICON、VI、TCP/IP 和 iSCSI）把生产系统与备份系统连接起来并构成存储网络。目前，生产系统与备份系统之间的连接主要有两种方式：一种方式为光纤通道连接，可以提供很高的性能，但是成本较高；另一种方式是近期发展的基于 IP 的互联技术，包括 FCIP、iFCP、iSCSI 等，可以跨越 LAN、MAN 和 WAN，成本低，可扩展性好，具有广阔的发展前景。

2.3 灾难恢复的衡量指标

选择信息系统的灾难恢复解决方案，主要以灾难恢复等级为中心。我们用灾难恢复指标对灾难恢复等级进行定量分析，不同等级具有不同的指标要求，图 2 给出了灾难恢复等级与指标的对应情况和当前各个等级在企业中的应用比率。

衡量灾难恢复的主要技术指标有恢复点目标 RPO（Recovery Point Object）和恢复时间目标 RTO（Recovery Time Object）[1,8]。RPO 是指灾难发生时刻与最近一次数据备份时刻的时间间隔，即尚来不及对数据进行备份（导致数据丢失）的时间，代表了丢失的数据量；RTO 是指系统从灾难发生到重新启动的时间，代表了系统恢复的能力。RPO 与 RTO 二者没有必然的关联性。RPO 与 RTO 的确定必须在进行风险分析和业务影响分析后根据不同的业务需求确定。对于不同企业的同一种业务，RTO 和 RPO 的需求也会有所不同。

此外，网络恢复目标 NRO（Network Recovery Object）和降级运作目标 DOO（Degrade Operation Object）[8]对灾难恢复来说也是至关重要的。NRO 代表灾难发生后网络切换需要的时间。DOO 是恢复完成以后到防止第二次故障或灾难的所有保护恢复以前的时间间隔，反映了系统发生故障后降级运行的能力。例如，如果某个镜像磁盘发生故障，而恢复点目标为即时——冗余磁盘会立即处理所有服务请求。但 DOO 为故障磁盘被替换，并且数据拷贝到冗余磁盘为止的时间。此时可能只是轻微的性能降级（因为输入/输出负载不能

在两个数据镜像之间均衡),但更重要的是,第二次磁盘故障会导致信息服务的宕机。DOO 期间系统运行的能力对系统来说非常重要,因为如果在降级运行期间发生第二次故障,再从第二次故障或灾难中恢复几乎不可能,从而导致更长的停机时间。

等级	恢复点目标 (RPO)	恢复时间目标 (RTO)	网络恢复目标 (NRO)	降级运作目标 (DOO)	企业应用比率
0	—	—	—	—	<0.3%
1	24—48 小时	>48 小时	—	—	<0.1%
2	24—48 小时	24 小时	—	周	80%
3	<24 小时	<24 小时	<24 小时	天－周	12%
4	小时级	<24, >2 小时	<24, >2 小时	天－周	<2%
5	小时级	<2 小时	<2 小时	天－周	<2%
6	秒级	<1 小时	分钟级	<24 小时	<2%
7	秒级／无	分钟级	秒级	<2 小时	<0.6%
8	无	秒级	秒级	<1 小时	<1%

图 2　灾难恢复等级标准

灾难恢复方案的恢复时间通常是指恢复业务服务所需的时间。然而在现实的灾难中,需要对其他更多的事项进行考虑。例如,有些业务可以容忍较长时间的停机服务,但要求一旦业务开始就需要使用最多的实时数据;有些业务必须在尽可能短的时间内恢复服务,而不考虑数据的实时性;还有一些既需要在最短的时间内恢复服务,也需要最多的实时数据。通过评估具体的灾难恢复需求,确定要达到的恢复指标,为选用灾难备份与恢复技术和制定灾难恢复计划与措施打好基础。

2.4　灾难恢复计划与措施

灾难恢复计划(DRP)与措施是灾难恢复体系结构的重要组成部分,它以实现灾难恢复指标为目的,结合多种灾难备份与恢复技术,对整个灾难恢复系统进行统一管理。灾难恢复的关键在于,一是建立切实可行的应急机制,这主要包含一套基于充分且清楚地将风险予以分类定义的灾难恢复计划和措施;二是在危机突然降临时,此计划与措施能被有效执行。灾难恢复的实质是确保企业业务的连续运营以及数据的安全。灾难恢复计划与措施的建立和实施过程,实际上是进行一个企业运营的项目,因此也涉及到项目管理的方方面面。标准的灾难恢复计划项目应按如下流程进行。

(1)项目启动和管理:确定灾难恢复计划实施过程的相关需求,包括获得管理支持以及组织和管理项目,使其符合时间和预算的约束。

(2)风险分析:识别业务流程和相关的 IT 基础设施资源需求(进行业务流程时需要使用的数据、系统和网络),并根据时间敏感性和任务关键性为各个业务流程确定优先级。确定可能造成业务流程和基础设施中断的灾难、具有负面影响的事件和周边环境因素,以及事件可能造成的损失、防止或减少潜在损失影响的控制措施,提供成本效益分析以调整控制措施方面的投资,达到消减风险的目的。同时,由于风险会随着系统的发展而变化,因此风险管理过程也必须是动态的。确定由于中断和预期灾难可能对系统造成的影响,以及用来定量和定性分析这种影响的技术。确定关键功能、恢复优先顺序和相关性,以便确定灾难恢复指标。

(3)设备保护:对系统的设备进行保护,包括水灾探测系统、可燃气体探测系统、空气污染级别探测系统、消防系统、后备电力系统和物理保障系统等的评估、选择、成本估算和安装。这些系统的目的是提供某种自动化设备,以便在某些特定的潜在威胁发展到打断业务正常运营之前就探测到它们(如果可能的话,还应当自动采取补救措施)。

(4)数据备份与恢复计划:数据访问的恢复时间是用来衡量灾后业务流程可存活性的关键因素。就业务而言,成功的灾难恢复归结为如何在最短的时间内恢复对数据的访问能力。制定数据备份与恢复计划,保证数据拷贝和数据更新所使用的系统资源不会受到灾难的影响,具有合适的数据访问恢复时间,保证这些数据可以被系统、网络以及最终用户所使用。数据备份与恢复计划包含以下内容:根据数据恢复的重要性对数据进行分析和分类;参照现有的备份程序,评估并选择合适的备份策略,以自动或人工程序的方式将数据转移到安全的离站的位置。考虑到与系统恢复、网络恢复以及终端用户恢复之间的相关性,在整个灾难恢复计划中,数据恢复通常和其他备份恢复机制采取一致的策略和步调。

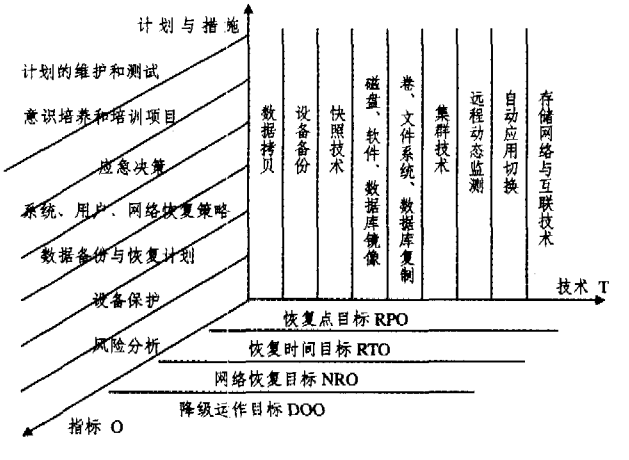

图 3　灾难恢复体系结构的三维模型

(5)系统、用户、网络恢复策略:确定和指导备用系统、用户、网络恢复运行策略的选择,以便在指定的恢复指标范围内维持系统的关键功能和恢复业务。

(6)应急决策:制定和实施用于事件响应以及对事件所引起状况进行稳定的规程,包括建立和管理紧急事件运作中心,

该中心用于在紧急事件中发布命令。

(7)意识培养和培训项目:建立对机构人员进行意识培养和技能培训的项目,以便灾难恢复计划能够得到制定、实施、维护和执行。

(8)维护和测试灾难恢复计划:对计划进行演练测试,并评估和记录演练的结果。制定维持连续性能力和 DRP 文档更新状态的方法,使其与企业的策略方向保持一致。通过与适当标准的比较来验证 DRP 的效率,并使用简明的语言报告验证的结果。

3 灾难恢复体系结构的三维模型

灾难恢复利用先进的软、硬件设备和环境,以灾难恢复等级(量化指标)为中心,综合运用各种技术手段(灾难备份与恢复技术)和管理措施(灾难恢复计划与措施),实现信息系统的灾难恢复要求。为了更好地表示信息系统的灾难恢复的层次结构、备份与恢复技术、灾难恢复计划与措施以及灾难恢复指标之间的关系,本文用图 3 所示的三维模型来进一步阐述体系结构中各元素之间的关系。

一个特定信息系统的灾难恢复体系结构(Disaster Recovery Architecture)可定义为一个三元组:$DRA=(O,T,P)$,其中:

$O=\{\langle O_1,O_2,O_3,O_4\rangle \mid O_1,O_2,O_3,O_4$ 分别表示不同类型指标 RPO,RTO,NRO,DOO 的值约束$\}$,即 O 表示该信息系统所要达到的各种灾难恢复指标;

$T=\{T_i\}$ 表示为保证达到该系统的各种灾难恢复指标,必须提供的多种备份与恢复技术 T_i;

$P=\{P_j\}$ 表示为保证达到该系统的各种灾难恢复指标,必须实施的各种灾难恢复计划和措施 P_j。

在灾难恢复体系结构的三维模型中,可根据三元组定义若干的规则点。由若干规则点构成的集合,则形成特定信息系统的灾难恢复解决方案,为整个体系结构的各个层次、各个组件协调工作起到核心控制作用。

结论 信息系统的灾难恢复体系结构以灾难恢复等级为中心,对备份与恢复技术及灾难恢复计划与措施统一进行管理,使体系结构中的各个层次、各个组件有机、协调地统一运作,为在发生灾难性事故的时候,以灾难恢复指标为标准对原系统进行恢复,以保证数据的完整性、可靠性和安全性以及业务的连续可用性。本文详细分析了灾难恢复系统的各个组成部分,根据容灾层次重新制定了灾难恢复等级,提出了灾难恢复系统的体系结构及相应的三维模型,从而为信息系统提供一个整体的灾难恢复解决方案。

参 考 文 献

1 Keeton K, Santos C, Beyer D, et al. Designing for disasters. In: Proceedings of the 3th USENIX Conference on File and Storage Technologies, San Francisco, CA, USA, 2004. 59~72

2 Lewis W, Richard Jr, Watson T, et al. An Empirical Assessment of IT Disaster Risk. Communications of the ACM, 2003, 46(9): 201~206

3 Zussman G, Segall A. Energy efficient routing in ad hoc disaster recovery networks. Proc of INFOCOM, 2003

4 IBM公司. IBM 容灾白皮书. http://www-900.ibm.com/cn/support/download/Disaster_recovery.pdf

5 Kim S-K, Dshalalow J H. Stochastic disaster recovery systems with external resources. Mathematical and Computer Modelling, 2002, 36(11): 1235~1257

6 Choy M H, Leong H V, Wong M H. Disaster Recovery Techniques for Database Systems. Communications of the ACM, 2002, 43(11)

7 *Toigo J W. Disaster Recovery Planning: Strategies for Protecting Critical Information Assets.* Prentice Hall PTR, 3rd edition, 2002

8 Veritas软件公司. 企业重生——信息系统的灾难恢复. 北京:机械工业出版社, 2004

9 牛云,等. 数据备份与灾难恢复. 北京:机械工业出版社, 2004

10 Azagury A, Factor M E, Satran J. Point-in-time copy: Yesterday, today and tomorrow. In: Proceedings of the Tenth Goddard Conference on Mass Storage Systems and Technologies. 2002. 259~270

11 Patterson H, Manley S, et al. SnapMirror: file-system based asynchronous mirroring for disaster recovery. In: Proc. File and Storage Technologies(FAST), 2002. 117~129

12 Ji M, Veitch A, Wilkes J. Seneca: remote mirroring done write. In: Proceedings of USENIX Technical Conference, 2003. 253~268

13 Wiesmann M, Pedone F, Schiper A, et al. Understanding replication in databases and distributed systems. In: Proceedings of 20 th International Conference on Distributed Computing Systems(ICDCS'2000), 2000. 264~274

14 Ahmad I. Cluster Computing: A Glance at Recent Events. IEEE Concurrency, 2000, 8(1): 67~69

(上接第 92 页)

相关工作的比较可以看出,本算法在调度长度与处理器使用数目上均优于 CGaTDS 算法或与其相当。

参 考 文 献

1 Di Martino V. Scheduling in a grid computing environment using genetic algorithms. In: Mililotti M, ed. 16th International Parallel and Distributed Processing Symposium (IPDPS2002). Florida, USA, April, 2002

2 Di Martino V, Mililotti M. Sub optimal scheduling in a grid using genetic algorithms. Parallel Computing, 2004, 30: 553~565

3 Abraham A, Buyya R. Nature's Heuristics for Scheduling Jobs on Computational Grids. In: The 8th International Conference on Advanced Computing and Communications(ADCOM 2000). Cochin, India, 2000

4 XU Zhihong, HOU Xiangdan, SUN Jizhou. An Algorithm-Based Task Scheduling in Grid Computing. CCECE 2003 - Canadian Conference on Electrical and Computer Engineering. Montreal, Canada, 2003

5 Park Chan-Ik, Choe Tae-Young. An optimal scheduling algorithm based on task duplication. In: The 8th International Conference on Parallel and Distributed Systems(ICPADS2001), Kyongju City, Korea, June 2001. 9~14

6 Ranaweera S, Agrawal D P. A task duplication based scheduling algorithm for heterogeneous systems. In: The 14th International Parallel and Distributed Processing Symposium (IPDPS2000), Cancun, Mexico, May 2000. 445~450

7 Tsuchiya T, Kikuno T, Osada T. A new heuristic algorithm based on GAs for multiprocessor scheduling with task duplication. In: 3rd International Conference on, Dec. 1997. 295~308

8 王小平,曹立明. 遗传算法. 西安:西安交通大学出版社, 2002