数据中心灾备体系设计详细介绍与分析

2010-03-03 网络 网络

数据中心灾备体系设计主要由三部分组成：灾备需求分析、灾备技术体系设计与灾备管理制度设计。灾备需求分析是根据数据中心 的业务特点与系统特点，分析存在的风险；灾备技术体系设计则是为达到灾备需求的旧标而进行的具体技术实现；灾备管理制度设计则是为确保灾备系统规范运作而 设立的管理制度。由于《规范》中对灾备管理制度的设计已经提出了比较明确的设计方法与要求，本文将不再赘述，而将重点放在介绍灾备需求分析与灾备技术体系 设计方面，为相关工作的具体实施提供参考。

一、区域数据中心灾备需求分析

(一)风险分析

全面详尽的风险分析是数据中心灾备体系设计的基础，风险分析方法包括：

1. *资产识别*，主要包括：基础设施、硬件、软件、数据、文档、服务和声誉等。单位应对资产进行分类，以区分资产的不同重要程度并 确定重要资产的范围，应 X 对资产进行标识以区分资产对业务正常运作的影响程度，据此确定资产的等级。

2. *威胁识别*，即识别信息资产构成潜在破坏的可能性因素，如自然因素与人为因素，内部因素与外部因素等。

3. *脆弱性识别*，即识别可能被威胁利用的信息资产的弱点，主要包括技术与管理两个方面。技术脆弱 性涉及物理层、网络层、系统层、应用层等各个层面的安全问题；管理脆弱性可分为技术管理脆弱性和组织管理脆弱性两方面，前者与具体技术活动相关，后者与管 理环境相关。

具体分析活动可通过问卷调查、工具检测、人工核查、文档查阅和渗透性测试等方式开展。完成风险分析后，需要根据灾难发生的可能性、灾难发生后的损失预计等 因素，计算对应的风险值，进行风险分级，为后续分析工作提供参考。

(二)业务影响分析

1．定义

业务影响分析(Business Impact Analysis，BIA)的目的是确定不同业务遭遇到风险后对企业的影响程度。通过分析有形的和无形的影响，估算对停止业务时间长短的接受情况和使影响 降至最低的处理需求，对灾备的其体实现提出明确要求。BIA 的目标包括：(1)识别和量化每个业务单元或者资源对整个企业在业务运行方面的影响；(2)． 识别潜在的失效场景和评估潜在的威胁；(3)定义针对不同的灾难恢复要求所需要的不同级别的投资情况；(4)建立灾难恢复时的恢复流程优先级，指导灾难备 份恢复策略的制订。

2．BIA 业务影响分析的方法

*(1) 业务功能地位分析。*可从业务功能的政策要求、是否核心业务、业务涉及的机构与用户范围、业务处理实时性与频度、业务功能与机 构内外其他业务功能的关联等多个角度综合分析。

*(2)业务中断影响评估。*主 要包括两个方面，一是以量化的方法，评估业务中断可能带来的直接与间接经济损失；二是以非量化的方法，评估业务中断所引发的社会影响、法律影响、信用影 响、品牌影响等。

业务影响分析最终将影响对灾难备份体系的需求，根据《规范》的要求，灾备体系的需求必须明确需求等级、各等级对应的最低恢复要求以及恢复的优先级。主要指 标是 RTO(Recover Time Objec—rive)，即灾难发生后，信息系统从停顿到恢复正常的时间要求，以及 RPO(Recover Point Ohieetive)，即灾难发生后，数据必须恢复到正常状态的时间要求。灾难恢复能力等级与上述两项指标的参照要求如表 1 所示。

表 1 灾难恢复能力等级及 RTO、RPO 指标要求

灾难恢复能力等级	RTO	RPO
1	2 天以上	1 天至 7 天
2	24 小时以上	1 天至 7 天
3	12 小时以上	数小时至 1 天
4	数小时至 2 天	数小时至 1 天
5	数分钟到 2 天	0 至 30 分钟
6	数分钟	

(三)基 础架构分析

数据中心技术体系分析是灾备技术体系建设的基础，灾备技术体系与数据技术体系匹配程度的高低，决定了灾备中心对数据中心生产环境的可替代程度，对于高效实 现灾难恢复，提高灾备中心可用性有重要意义。对数据中心技术体系的分析主要从以下两方面人手。

*1. 基础运 行环境分析。*在确保灾备中心与数据中心技术架构基本一致的前提下，明确所需要的设备类型和数量，对机房配电、空调、地板承重 以及布线的具体要求等基础环境信息，为选择具体的灾备环境提供参考。

*2. 应用部署特点分析。*主 要分析各类应用部署平台的情况、应用之间的数据依赖关系、应用正常运行需要数据质量、应用正常启动和异常启动需要的时间等关键因素，作为灾备中心应用体系 构建的基础。

二、区域数据中心灾备技术体系设计

(一)灾备模式的基本体系架构

灾备模式主要有“同城灾备”、“异地灾备”以及“同城一异地灾备”三种主要方式。同城灾备，是指灾备中心与生产中心处于同一城市内，可同时采用同步备份与 异步备份技术。其具有最低的投资成本，最快的灾难恢复速度，极

高的数据保障，但无法应对区域性的灾难风险。异地灾备，是指灾备中心与生产中心在不同的城 市，一般只能实现异步备份。其投资成本较高，灾难恢复速度与数据保障能力略低，但可应付广泛的灾难风险。同城一异地灾备则是两者的结合，投资成本最高，但 同时具有前两者优点。同城一异地模式也分两种实现方式，一种是首先建立同城灾备中心，然后异地灾备中心实现对同城灾备中心的备份；一种是同城灾备中心与异 地灾备中心分别独立为数据中心实施备份。

具体选择何种灾备模式，需要综合考虑所面 I 临的风险特点、业务特点、成本投入等多种因素。由于数据中心面临的重大风险绝大多数都发生在数据中心范围内，而 同城灾备中心在业务迅速恢复方面具有比较突出的优势，因此同城灾备中心的建设一般是必须的。灾备模式的选择建议如下。

1．全国性数据中心采用同城一异地灾备模式。由于其业务系统与数据的影响面广，由此必须采用最为可靠的灾备模式。

2．建立总中心一区域两级数据中心的机构，在区域数据中心建立同城灾备，并通过数据总中心的异地灾备中心，实现对各区域数据中心的集中式异地灾备。当区域 数据中心出现严重故障时，可通过同城灾备中心实现对全省业务的迅速接管，而出现区域性重大灾难时，可通过数据总中心的异地灾备中心实现区域业务的恢复。这 一模式既减少了区域自建异地灾备中心所需的庞大投资，又能提供全面的灾备保护。

(二)灾备中心基础环境建设

灾备中心基础设施建设应重点考虑以下因素：

*1．选址。*灾难备份中心与生产中 心之间距离合理，应避免灾难备份中心与生产中心同时遭受同类风险。综合考虑生产中心与灾难备份中心交通和电讯的便利性与多样性，以及灾难备份中心当地的业 务与技术支持能力、电讯资源、地理地质环境、公共资源与服务配套能力等外部支持条件。

*2。基础条件。*机 房环境要求与主中心相同，各项建筑基础环境(如防雷、防火、防静电、承重、分区隔离等)、供配电环境、温湿度空调环境、消防和监控安全环境等，都应参照生 产数据中心机房环境设计，至少达到生产数据中心机房环境所属等级要求。考虑到灾备恢复情况下额外的外部技术支援，灾备中心在工作人员容纳方面应作适当考 虑，以保证有足够空间容纳一定数量的技术人员集中协同办公。

*3. 建设方式。*灾 备中心的建设方式可采用自建、共建与外包建设等方式，三种方式各有优势，需要结合各类机构的实际情况加以选择。自建是指金融机构独立建设区域数据中心，此 模式具有较高的可靠性与安全性，但投入庞大，适用于大型金融机构。共建是指数家金融机构共同规划投资，建设参与各方共同使用的区域灾备中心。共建模式减少 了各方的投资压力，但需要各方充分协调，有效实现灾备中心的建设管理，参与机构不宜过多，适用于中型金融机构。托管是指将区域灾备中心由专业的灾备服务商 建设管理，金融机构向其租用灾备物理环境，实现数据与系统的区域灾备体系建设，此模式充分利用了灾备服务专业化的优势，在最大限度减少建设投资的同时，为 信息系统提供可靠保护，适用于中小型金融机构。

表 2 数据备份复制主要方式之比较

	快照技术	异步复制技术	同步复制技术
原理	数据指针定时对数据中心数据变化情况进行记录，并传输到灾备中心进行备份，两个快照时点之间的数据变化是不受保护	通过缓存与批量处理的方式，在较短的时延内，将数据中心生产数据复制到灾备中心	同时对生产数据与灾备中心数据进行同步写入的复制技术。在灾备中心数据成功写入前，数据中心存储系统将不处理后续的数据 I/O 请求
数据备份空间	少	多	多
适用 RPO	30 分钟以上	分钟级以上	毫秒级以上
对生产系统的影响	无	无	

(三)网 络备份体系设计

数据中心与灾备中心应建立网络热备份体系，当数据生产中心无法正常工作时，业务数据流可自动切换到灾备中心，保证灾备中心的备份业务系统顺利接管业务数 据。目前网络热备份技术已经比较成熟，可利用多种动态路由协议(如OSPF，BGP 等)实现。网络备份设计参考要点如下。

*1. 建立核心网络热备体系。*数据中心是面向某个区域的庞大数据处理节点，必须在核心网络层面(如广域网、核心服务器运行的 局域网)实现热备，才能保证灾备中心对区域内通信的可靠性。同时，前述灾备中心的选址要求，决定了数据中心与灾备中心之间必须建立广域网互联，因此在广域 网层面实现线路热备显得尤为必要。

*2. 灾备中心网络容量设计。*灾备中心网络 容量应与生产中心网络容量基本一致，网络应采用一致的技术标准。灾备中心与数据中心同步传输的链路，其带宽必须大于数据中心的峰值数据变化量。因此，同城 灾备网络，应灾备中心与生产中心之间应建立光纤网络。

3. 灾备网络应与数据中心网络采用不同运营商物理线路。《规范》明确要求，灾备中心对外的通信线路应采用与数据中心不同的运 营商，降低风险关联。而数据中心与灾备中心之间同样需要建立两条不同运营商通信线路，以捆绑技术建立两地路由器互联，从而提高两地之间通信的可靠性，确保 热备功能的有效性。

*4. 尽量建立数据中心网络与灾备中心网络的负载均衡，有利于提高灾备网络利用率与提高 灾备网络可用性。*灾备中心网络基本是数据中心网络的复制，目前网络热备份技术主要有两种模式。一种是主-备模式，数据流正常 情况下使用数据中心生产网络，当数据中心生产网络出现故障时，才使用灾备中心网络。这一模式实现简单，但灾备网络 13 常实际并不使用，既造成资源浪费，也 不利于提高灾备网络的可用性。另一种是负载均衡模式，正常情况下数据流同时使用两个中心的网络，生产中心网络出现故障时，则全部数据流向灾备网络。后者的 实现技术比较复杂，需要专用负载均衡设备支持，但可以充分利用网络资源，也可以在日常使用中验证灾备网络的可用性，建议尽可能采用此模式。

(四)数据 环境备份设计

1．备份介质

目前主流的备份介质包括磁带库、虚拟带库与磁盘阵列。虚拟带库是将低性能磁盘组模拟成磁带方式进行读写存储的备份介质，它既保留了磁带顺序写入在数据备份 过程中特有的高性能，又可避免磁带受外环境破坏、不宜多次读写的缺点，有利于数据保存与对备份数据的恢复验证。但虚拟带库与磁带库同样存在读取效率低的缺 陷，只适用于数量庞大而 RTO 要求较低(恢复能力等级为 3 以下)的数据备份环境。磁盘阵列则是以普通硬盘读写的方式，对数据进行备份的备份介质。磁盘阵列 一般由具备高性能磁盘所组成，并通过高容量缓存与 I / O 负载均衡技术提高数据读写效率，适用于 RTO 性能要求较高(恢复能力等级为 3 以上)的数据备份环 境。

2．备份传输

(1)数据备份传输的技术选择

数据备份复制方式主要有快照技术、异步复制、同步复制(如表 2 所示)。数据复制方式的选择主要取决于灾备需求分析中业务系统对 RPO 的要求。

(2)数据备份传输的实现

目前金融机构数据中心普遍建立了集中存储系统，因此存在存储传输网络与业务传输网络两套专用网络，从而派生出数据备份传输技术的三种实现方案——主机代理 模式、存储阵列模式与代理模式。三种模式的选择主要取决于灾备恢复需求与可用于灾备建设的资源投入。从目前情况看，CDP 方式是适用面较广的数据备份传输 实现方式。比较情况如表 3 所示。

表 3 数据备份传输三种模式之比较

	主机代理模式	存储阵列模式	CDP代理模式
原理	依托在业务主机中的备份软件，对数据备份传输过程进行管理，并通过业务传输网络传输到灾备中心	通过专用存储传输网络，实现数据中心存储与灾备中心存储之间数据复制	部署专用的CDP备份设备，令CDP设备本身通过数据中心存储网络实现对存储系统数据的同步复制，然后再以异步模式，将同步复制后的数据通过业务传输网络的空闲带宽传输到灾备中心
资源占用情况	占用一定主机资源，影响业务网络	基本不占用主机资源，不影响业务网络	基本不占用主机资源，对业务网络影响很小。
适用备份方式	异步备份	同步备份或异步备份	异步为主，也适用与部分同步备份需求
建设投入	较低	高，需扩展存储传输网，购置高性能存储	较高，需部署专用CDP设备
数据备份效率	一般	很高	较高
适用RPO	建议30分钟以上	毫秒级别以上	分钟级以上

(五)应 用环境备份设计

应用环境备份的目的是确保灾备中心能够快速重建数据中心应用系统环境，并实现备份业务系统对生产系统有效替代。对应用环境备份的设计要点包括：

*1．通过配置同步技术，实现数据中心应用环境的一致性。*灾备中心的应用环境在技术路线、设备部署 方面应尽量保证与数据中心应用环境一致。这样有利于提高灾备应用环境与生产应用环境之间手工切换的效率，也有利于日常检验灾备应用环境的可用性。一般可通 过灾备应用环境定期向生产应用环境读取配置文件、参数等方式，实现两者配置的同步。

*2．灾备中心关键型业 务系统实现集群间自动切换，其余业务系统则采用手工切换模式。*数据中心应用服务器一般通过HA等技术建立高可用性集群，保证 本地应用服务的高可靠性。同样，只要建立数据中心与灾备中心之间的高可用性网络监控技术，灾备中心备份应用服务器集群可实现与数据中心生产服务器集群之间 的高可用性自动切换。为节约成本投入，建议对关键性业务系统采用此方式，以满足RTO一小时以内的灾备恢复需求。对于其余业务系统，只要如前所述，保证应 用环境一致性，通过手工方式进行切换即可。

*3. 采用虚拟化技术对备份环境进行整合。*灾 备中心应用环境备份资源毕竟有限，充分利用备份应用资源对数据中心应用环境保护十分重要。虚拟化技术可实现一台物理应用服务器对多台逻辑服务器的虚拟。这 样在数据中心里，大量性能要求不苛刻、RTO 要求在数小时以上的应用系统灾备环境就可以集中部署在少数的硬件服务器资源中，有利于灾备中心尽可能提高对数 据中心应用系统的灾备范围。