第十八章 灾难恢复计划

18.1 灾难的本质

- 灾难恢复计划围绕组织正常运营被终端，为混乱的时间带来正常的工作秩序
- 灾难恢复计划应该被配置为几乎是自动执行的

18.1.1 自然灾难

- 地震：美国的大部分地区都出现至少属于中级的地震事件
- 洪水：
- 暴风雨：
- 火灾：
- 其他的地区性事件： 世界上某些地区具有地区性的自然灾害

18.1.2 人为灾难

- 火灾：
- 恐怖行为：恐怖行为不可预测，为DRP团队带来的特殊挑战
- 爆炸/煤气泄漏：
- 电力中断：最基本的灾难恢复计划也包括了对短时间电力中断威胁的应对方法，关键业务使用ups

18.1.3 其他公共设施和基础设施故障

1. 硬件/软件故障
    - 硬件组件可能受到磨损且无法继续运行或受到物理损坏
    - 由于财务上的限制，维持全冗余系统并非总能实现
2. 罢工/示威抗议
    - 人为灾难形式可能是罢工或其他劳工危机
3. 盗窃/故意破坏
    - 业务连续性计划和灾难恢复计划应当包括充分的预防性措施，以控制这些事件的发生频率

18.2 理解系统恢复和容错能力

- 增加系统应变能力和容错能力的技术控制会直接影响到可用性，系统恢复和容错能力的主要目的是销毁单点故障
- 单点故障可以发生在任何组件上，能够导致整个系统崩溃

- 容错能力时指系统在发生故障的情况下仍然继续运行的能力
- 系统恢复能力指的是系统在发生不利时间时保持可接受的服务水平的能力

18.2.1 保护磁盘驱动

- 添加容错和系统恢复组件的常见方法是增加冗余磁盘矩阵（RAID）
- 常见RAID配置：
  - RAID-0：称为条带，使用两个或两个以上的磁盘，提高磁盘系统性能
  - RAID-1：称为镜像，使用两个磁盘，并含有相同的数据信息，实现高可用
  - RAID-5：称为奇偶校验，使用三个或更多磁盘，坏1个速度会变慢
  - RAID-10：条带镜像，至少使用4个磁盘，提高可用性和性能

18.2.2 保护服务器

- 故障转移集群包含两个或两个以上的服务器，一台服务器出现故障，其他服务器通过称为故障转移的自动化过程接管负载

18.2.3 保护电源

- 不间断供电电源（UPS）、发电机或他们两者提供容错能力，UPS提供5-到30分钟供电，发电机提供长时供电

18.2.4 受信恢复

- 受信恢复保证系统在发生故障或崩溃后，能够还原到之前的状态，还原分为自动还原和管理员手动干预
- 系统可以被预制，在损坏时能够处于故障防护状态或应急开放状态
- 四种类型的受信恢复：
  - 手动式恢复
  - 自动式恢复
  - 无过度损失的自动式恢复： 系统能够自动执行恢复过程，包括对数据以及其他对象的恢复
  - 功能恢复：支持功能恢复的系统能够偶自动恢复某些特定功能

18.2.5 服务质量

- QOS（服务质量）控制能够保护负载下的数据网络的完整性：
- QOS因素：
  - 宽带
  - 延迟时间
  - 抖动
  - 数据包丢失

- 干扰

18.3 恢复策略

- 灾难恢复计划应该能够几乎全自动起到作用并开始为恢复操作提供支持
- 除了提高响应能力外，保险也能够减少经济损失
- 有效行政保险责任范围为记名的、打印的或书面的文档与手稿

18.3.1 确定业务单元的优先顺序

- 优先级别最高的业务最先被恢复

18.3.2 危机管理

- 危机管理是一门科学和技术，如果培训预算支出允许，进行危机培训是个好办法

18.3.3 应急通道

- 灾难来袭，组织能够内部与外部之间通讯是很重要的

18.3.4 工作组恢复

- 灾难恢复计划目标是让工作组恢复到正常状态并且重新开始日常工作
- 为了推动这项工作，为不同的工作组开发独立的恢复设施是最好的办法

18.3.5 可替代的工作站点

- 灾难恢复计划中重要要素之一就是，主要的工作站点无法使用时选择考研替代的工作站点
  - 冷战点：足够大的地方处理组织运营工作，适当的电子环境支持，没有预先安装计算机设施，也没有通信宽带链接，成本相对便宜
  - 热站点：建筑布局中具有固定的被维护的固定工作设施，并且富有完备的服务器、工作站和通信链接设备，，服务器和工作站都是预先配置好的，装置了适当的操作系统和应用软件，服务器数据是最新的
  - 温站点：介于热站点和冷战点之间，包含设备和数据线路，不包含客户的备份数据，重新激活站点至少需要12个小时
  - 移动站点：设备起源的拖车或其他容易重新安置的单元组成，为了维持安全计算机环境所需的所有环境系统
  - 服务局：租借计算机时间的公司，购买部分处理能力，发生故障时，能够为IT需求提供支持，
  - 云计算：在云站点被激活之前能够避免大部分的操作成本

18.3.6 相互援助协议

- 在灾难发生时通过共享计算机设施或其他资源彼此相互援助
- MAA协议缺点：
  - 很难强制实施
  - 可能受同样的威胁
  - 机密性

18.3.7 数据库恢复

- 灾难恢复计划汇总包括数据恢复技术是很重要的
- 数据库恢复的主要技术手段
  - 电子链接：数据库备份通过批量传送的方式被转移到远处的某个场所，需要测试备份解决方法
  - 远程日志处理：更加迅速的方式完成数据的传输，以批量的方式进行，但是发生的更频繁，
  - 远程镜像：最先进的数据库备份解决方法，费用也是最贵的，实时数据库服务器在备份站点进行维护

18.4 恢复计划开发

18.4.1 紧急事件响应

- 重要人员在是被灾难或灾难即将来临应立即遵守、简单但内容全面的指令

18.4.2 人员通知

- 维护一份人员列表，以便在发生灾难时进行联络

18.4.3 评估

- 灾难恢复团队到达现场的收到任务就是评估现状

18.4.4 备份和离站存储

完整备份：存储着受保护设备上包含的数据的完整副本，每个文件的归档比特都会被重置、关闭或设置为0

增量备份：只存储哪些自从最近一次完整备份依赖被修改过的所有文件，增量备份只复制归档比特被打开、启用和设施为1的文件，一旦备份完成，重置、关闭或设置为0

差异备份：存储哪些自从最近一次完整备份依赖被修改过的所有文件，差异备份只复制归档比特被打开、启用或设置为1的文件

1. 备份介质格式
   - 数字数据存储（DDS）/数字音频磁带（DAT）

    - 数字线性磁带（DLT）和超强DLT
    - 线性磁带开放式技术（LTO）
2. 磁带到磁带（D2D）备份
    - 采用完整的磁带到磁盘备份方法的组织，必须确保地理多样性
3. 最佳备份做法
    - 数据备份量会随着时间的推移而增加
    - 使用定期备份的情况下，总有可能存在备份依赖的数据丢失
    - 最后需要测试组织的恢复流程
4. 磁带轮换
    - 磁带轮换策略:（GFS测试、汉罗塔测试、六磁带每周备份），商用备份软件、全自动分层存储管理系统实现自动备份策略

18.4.5 软件托管协议

- 软件托管协议，对公司起到保护作用，避免公司受软件开发商的代码故障影响，防止出现由软件开发商破产而造成产品失去技术支持的情况

18.4.6 外部通信

- 灾难恢复期间，与组织外部不同的实体进行通信很有必要

18.4.7 公用设施

- 灾难恢复计划中应该包括解决这些服务在灾难发生过程中出现问题的关联信息和措施

18.4.8 物流和供应

- 灾难恢复操作中有关物流的问题是值得注意

18.4.9 恢复与还原的比较

- 抢救团队必须确保新的IT基础设施的可靠性
- 在结束所有灾难恢复工作之后，就需要在原有场所执行还原操作，并且终止灾难恢复约定下的任何处理场所操作

18.5 培训、意识与文档记录

- 灾难恢复计划应该进行完整的文档记录
- DRP应当被视为极其敏感的文档，并且只有分类和需知的基础提供给个人

18.6 测试与维护

- 每一种灾难恢复计划都必须顶起进行测试，以确保计划的条款是可行的并且符合组织变化的需要

18.6.1 通读测试

- 通读测试是最简单的也是最重要的测试，只需灾难恢复团队分发灾难恢复清单的副本

18.6.2 结构化演练

- 灾难恢复团队成员聚集在一间大会议室，不同的人在灾难发生时扮演不同角色**（桌面演练）**

18.6.3 模拟测试

- 模拟测试为灾难恢复团队成员呈现情景并要求他们**产生适当的响应措施，这种测试可能涉及中断非关键的业务活动并使用某些操作人员**

18.6.4 并行测试

- 并行测试表示下一个层次的测试，将实际人员重新部署到替换的恢复场所和实现场所启用措施，唯一的差别在于**主要设施的运营不会被中断，这个场所仍然处理组织的日常处理**

18.6.5 完全中断测试

- 完全中断测试与并行测试的操作方法类似，但是**涉及关闭主场所的运营并将其转移到恢复场所**

18.6.6 维护

- 灾难恢复计划是灵活的文档，必须对灾难恢复计划修改以符合变化的需要，灾难恢复人员**应当将组织的业务连续性计划借鉴为恢复工作的模板**