灾备计划

由 IBM 服务部撰写

2019 年 1 月 30 日

提高能力，迅速响应中断事件并从中恢复

什么是灾备计划?

自然灾害

灾备计划是企业编制的正式文件，用于详细说明如何应对自然灾害、断电、网络攻击和任何其他中断事件。该计划包含有关如何最大程度降低灾害影响的策略，旨在确保企业能够持续运营，或者快速恢复关键运营。与业务连续性计划

相比，该计划目标更集中，不一定要考虑有关业务流程、资产、人力资源和业务合作伙伴的所有意外情况。

成功的灾备计划通常可以应对所有类型的运营中断，而不只是造成某个地点不可用的重大自然或人为灾难。中断类型包括断电、电话系统中断、由于炸弹威胁暂时无法进入某个设施、“火灾隐患”或影响较小的非破坏性火灾、洪水或其他事件。灾备计划应按照灾难类型和发生地点进行规划。它必须包含任何人都可以实施的脚本（指令）。

观看视频 — 灾备计划的发展历程

20 世纪 70 年代之前，大多数企业只需要关心如何复制纸质记录。到 20 世纪 70 年代，随着企业逐渐依靠计算机开展运营，灾备计划开始受到重视。当时，大多数系统都是面向批处理的大型机。在等待主运营地点恢复期间，可以通过备份磁带启动另一个异地大型机。

1983 年，美国政府强制要求全国银行必须制定可验证的备份计划。随着许多其他行业逐步了解到长时间中断会造成重大经济损失，它们纷纷开始效仿。

到了 21 世纪，企业对数字化在线服务的依赖度进一步提高。随着大数据、云计算、移动和社交媒体技术的出现，企业必须能够有效捕获和存储呈指数级增加的海量数据。由于必须考虑众多设备中的海量数据存储，因此灾备计划无疑变得更加复杂。20 世纪 10 年代，云计算横空出世，使企业能够将灾备计划外包出去（又叫做灾备即服务（DRaaS），这有助于缓解灾备复杂性。

网络攻击日益复杂是目前显现出的另一个趋势，这也突显了制定详细灾备计划的重要性。行业统计数据表明，许多攻击在开始后 200 多天内都未被发现。如此长时间地隐藏在网络中，攻击者有足够的时间将恶意软件植入备份集之中，导致恢复数据也被感染。攻击可以隐藏数周或数月之久，使得恶意软件能够在整个系统中传播。即使在检测到攻击之后，移除已遍布整个企业中的恶意软件也是非常困难的。

灾备计划为何非常重要?

平均而言，基础架构故障每小时的成本为 10 万美元，而关键应用故障每小时的成本可能达到 50 万到 100 万美元[1]。目前，数字业务渠道占据较大的市场份额，有力推动收入增长。除收入和生产力损失之外，客户最不能容忍的就

是宕机。如果在中断事件面前无所作为，客户会毫不犹豫地抛弃现有供应商，选择其他有竞争力的企业满足自己的需求。

企业希望制定经过检验的详细灾备计划的其他主要原因包括：

- 最大程度减少正常运营的中断。
- 限制中断和损失的范围。
- 最大程度降低中断的经济影响。
- 提前制定备用运营方案。
- 训练人员掌握应急流程。
- 支持顺畅快速地恢复服务。

观看视频 — IBM 全球信息科技服务部： 灾备即服务（DRaaS）

1. “DevOps 和宕机成本：《财富》1000 强最佳实践量化指标”，Stephen Elliot，IDC，2014 年 12 月，IDC #253155

利用咨询服务、软件和基于云的解决方案，支持业务连续性计划

许多企业都在努力地快速完善灾备计划战略，以应对当今的混合 IT 环境和复杂的业务运营。但是，在这个永续运营的世界中，企业是获得竞争优势还是丢掉市场份额，关键取决于执行灾难恢复和恢复核心业务服务的速度。

有些企业利用外部的灾备和业务连续性咨询服务来满足企业对于评估、规划和设计、实施、检验和全面管理灾备计划的需求。

还有一些主动服务，比如 IBM IT 基础架构恢复服务，**可帮助企业发现风险，确保他们时刻做好准备，能够及时检测和响应中断并从中恢复。**

随着网络攻击次数越来越多，企业纷纷从传统的人工恢复方法转向自动化的软件定义灾备方法。IBM 网络灾备服务方法使用先进技术和最佳实践，帮助评估风险，确定优先级并保护业务关键型应用和数据。这些服务还可以帮助企业在网络攻击期间或之后快速恢复 IT。

其他企业采用基于云的备份方法，比如 IBM 灾备即服务 (DRaaS)，持续复制关键应用、基础架构、数据和系统，以便在 IT 中断之后快速恢复。还可以选择使用虚拟服务器，如 IBM 云虚拟化服务器恢复，用于实时保护关键服务器。这样，就能够在 IBM 灾备中心快速恢复您的应用，以便在维护或意外宕机期间保持业务持续运营。

对于越来越多的企业来说，答案是利用业务连续指挥与自动化管理，这是一种基于云的方法，采用灾备自动化以及专为混合 IT 环境设计的一系列业务连续性管理工具。例如，IBM 业务连续指挥与自动化管理服务可帮助保护应用、数据和基础架构组件之间的业务流程依赖关系。它有助于提高业务应用的可用性，企业可通过集中式仪表板访问有关 RPO、RTO 和 IT 连续性整体状况的高级或深层必要情报。

观看视频 — IBM 云业务连续指挥与自动化管理服务概述

行之有效的灾备计划的主要特性

灾备计划的目的是确保企业可以对灾难或影响信息系统的其他紧急情况快速作出响应，并最大程度降低对业务运营的影响。IBM 创建了一个模板，可用于生成基本的灾备计划。以下是模板中提供的步骤建议。如果您已准备好信息，建议将文档存储在高度安全且易于访问的异地位置。

第 1 步：主要目标 第一步是大体列出灾备计划的主要目标。

第 2 步：人员 记录数据处理人员。包括组织架构图和计划的副本。

第 3 步：应用概况 列出应用并标注是否为关键资产和固定资产。

第 4 步：库存概况 列出制造商、型号、序列号、成本以及是购置资产还是租赁资产。

第 5 步： 信息服务备份程序 包含以下信息：“日志接收器在 _____ 和 _____ 发生变更。”以及：“以下库和字典中的变更对象已保存在____。”

第 6 步：灾备程序 对于任何灾备计划来说，都应具备以下三个要素：

- 应急响应程序，用于记录对火灾、自然灾害或任何其他活动的适当应急响应措施，以便保护生命和减少损失。
- 备份运营程序，用于确保在发生中断之后，能够执行基本的数据处理运营任务。
- 恢复操作程序，用于在灾难过后快速复原数据处理系统。

第 7 步：移动站点的恢复计划 该计划包含移动站点建设计划、通信灾难计划（包括线路图）和供电示意图。

第 8 步：热站点恢复计划 备用热站点计划旨在提供备用（备份）站点。备用站点具有备份系统，可供在主站点重建期间临时使用。

第 9 步：复原整个系统 要使系统恢复到发生灾难前的状态，请使用系统管理：备份和恢复中系统完全失效后的恢复流程。

第 10 步：重建流程 管理团队必须评估损害程度，开始重建新的数据中心。

第 11 步：测试灾备计划 要实现卓有成效的应急规划，就必须定期检验和评估灾备计划。数据处理运营从本质上而言是个不断变化的过程，这就导致需要经

常更改设备、程序和文档。这些操作使得灾备计划在不断变化，必须清楚地认识到这一点。

第 12 步：灾难站点重建 这一步包括数据中心的平面设计图、当前硬件需求和可能的替代方案，以及数据中心的占地面积、用电需求和安保需求。

第 13 步：记录计划变更 让计划始终保持最新状态。持续记录配置、应用、备份安排和流程的变更。

关于灾备计划的博客

灾备：管理措施能否满足要求?

思考未曾考虑的问题

前瞻性的灾备方法

实施业务连续性计划，适应和应对风险

有关灾备计划的更多资源

使用此模板制定灾备计划

灾备计划模板

了解如何自动实施 IT 恢复管理，简化灾备流程。

IBM 云业务连续指挥与自动化管理概述

阅读这篇 Forbes 文章，了解企业高管如何应对复杂的混合 IT 环境所产生的关键应用风险。

业务连续性：转变连续性战略的时机已经到来

了解如何通过此信息图中所示的四步实现零宕机。

四步实现永续运营

阅读本白皮书，了解当前的市场趋势，以及影响永续平台需求的各种因素。

四步实现永续运营

阅读本 IDC 白皮书，了解为何当企业采用新技术时，保护战略必须与时俱进。

实现网络灾备框架的五项关键技术

阅读本分析报告，了解 IBM 为何被评为愿景完整性最出色的企业。

IBM 跻身 2017 年 Gartner 灾备即服务魔力象限领先者行列

观看这段简介视频，了解如何帮助企业发现风险，确保为检测和响应中断并从中恢复做好准备。

IBM 业务连续性及灾备服务概述

与灾备计划相关的 IBM 产品

IBM 业务连续性咨询服务

IBM 业务连续指挥与自动化管理

IBM 灾备即服务（DRaaS）

网络灾备服务

管理备份即服务

IBM IT 基础架构恢复服务

IBM 工作场所恢复服务

IBM 业务连续性咨询服务

IBM 云虚拟化服务器恢复服务