



# 业务连续性： 24x7x365 业务永续运营的要求



Tech Republic 为 IBM 撰写

## 目录：

摘要.....	3
引言.....	4
为何需要业务连续性？ .....	4
计算成本 .....	6
虚拟化和复制 .....	10
合作.....	13

关于本白皮书：本文档由 IBM 委托 CBS Interactive 撰写。IBM 规定了本指南的标题和关键主题，而且可能提供了部分内容并控制内容的编辑。本白皮书只能由 IBM 全文引用和复制。

## 摘要

目前，广大客户和业务合作伙伴希望业务能够实现 24x7x365 式不间断运营。服务器和基础架构停运每分钟都可能造成数千美元的损失，当然还要计算收入和生产力的损失、对企业声誉的损害以及由于无法遵守 SLA 和法律法规所招致的罚款。许多企业对宕机采取零容忍态度。

尽管企业尽最大努力确保业务连续性，但断电、恶劣的天气、硬件问题以及人为错误仍会不时造成 IT 服务中断，而平均恢复时间需要 24 小时。业务连续性水平之所以停滞不前，主要是因为 IT 预算常年得不到增加；系统越来越复杂，相互依存度越来越高；企业采用全球分布式业务运营模式；以及移动工作人员的数量越来越多。

包括虚拟化、数据复制和云计算在内的诸多技术在不断发展，帮助企业克服这些业务连续性挑战。可以将整个服务器（甚至整个环境）转移到备用资源，实现接近实时的故障转移。在企业环境中，虚拟化和复制已经非常普及，而且云服务的采用率也在稳步增长。云端的业务连续性模式包括私有、共享、现场和非现场等选项。许多企业采用混合模式，确保最关键的业务系统实现高可用性，同时保证非关键组件能够实现经济有效的恢复。

由于云服务相对而言还是新生事物，其服务和安全参数还不是很明确，因此与专业的业务连续性服务提供商（如 IBM）密切合作就显得至关重要。IBM 可以提供全面的业务连续性和灾备服务组合以及专家咨询，能够满足任何企业的需求。通过结合数据中心、硬件、软件、技术专家和云服务的强大能力，IBM 可以帮助客户精心制定业务连续性和灾备计划，实施量身定制的解决方案，确保实现无缝的故障转移和故障恢复、数据安全性、事件修复以及合规性。更理想的是，IBM 可以管理整个解决方案，而不会增加客户内部 IT 资源的负担。

## 引言

“服务器宕机了！”这六个可怕的字眼对于不同岗位的人员有着不同的含义，但都不是好事情。对 IT 人员来说，这意味着“紧急集合”，必须确保以最快速度恢复和运行受影响的资源，必要时还要从备份中恢复数据。对于普通员工来说，这意味着数分钟乃至数小时无法工作，感到沮丧而且压力巨大。对于高管而言，这意味着巨额的经济损失，企业声誉受损，甚至可能会面临罚款（如果无法满足规定的服务级别）。

在本白皮书中，我们将讨论推动业务连续性需求的各种因素，以及宕机的潜在成本。我们将介绍目前阻碍企业实现高可用性和业务连续性的因素，探讨帮助企业快速可靠地实现 IT 资源故障转移和故障恢复的新模式。

## 为何需要业务连续性？

在过去几年，企业对宕机的容忍度明显下降。习以为常的周末服务中断维护的日子已经一去不复返。为了保持竞争力，当今企业必须以 24x7x365 方式不间断开展交易、处理业务、服务客户以及应对不断变化的情况。从最简单的层面来说，业务连续性至关重要，因为每分钟的宕机都等同于收入损失。长远来看，如果运营中断，客户就很可能转投竞争对手的“怀抱”。

### SLA

此外，许多企业需要遵守服务级别协议，如果不合规，可能会受到处罚。IT 管理顾问 Barclay Rae 在其《Guide to SLAs》（SLA 指南）一书中指出，供应商与客户、合作伙伴甚至内部部门之间都可能建立 SLA。<sup>1</sup> SLA 还可能以服务级别合同的形式正规化，具有强制性的责任和处罚条款。

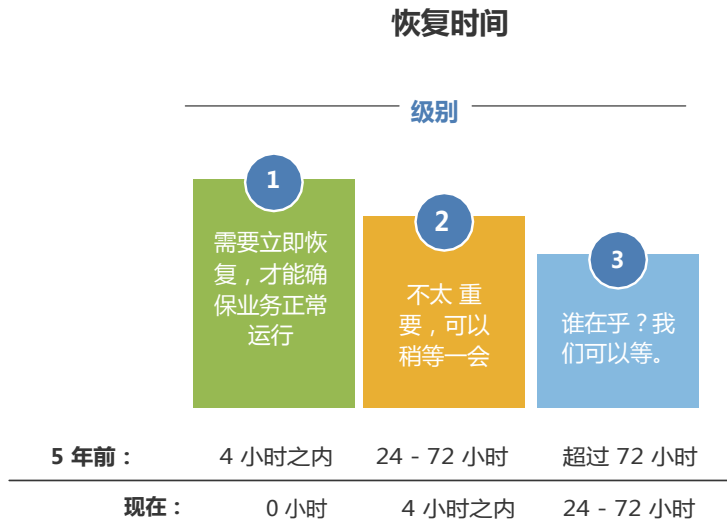
SLA 促使企业量化并思考 IT 服务运营的每个要素，包括：

- 每项服务的描述
- 用于补救问题的上报途径
- 支持小时数
- 事故解决速度
- 提供非紧急服务的速度
- 事件严重性分级
- 客户职责概述
- 特殊注意事项

每分钟的宕机等  
同于收入损失。

<sup>1</sup> Barclay Rae, 《A Guide to SLAs》, 2012 年 6 月

通过深入分析严重性级别，Rae 举了一个 SLA 例子 - 将最高优先级事故的恢复时间规定为 1 小时内，二级事故的恢复时间定为四小时内，三级事故的恢复时间定为一个工作日内。但是，正如我们将看到的，这种响应级别已经过时，而且要付出巨大的代价。



来源：Forbes Insight，“How the cloud is changing resilience in the expanding universe of digital data”，2014 年

## 合规性

除了与客户和内部利益相关方签订的服务级别协议之外，许多 IT 组织还受政府法规以及行业规定的约束，需要为关键系统和敏感数据建立备援能力，保持持续可用性。跨国企业必须在开展业务的每个国家或地区遵守相关的数据保护法律。以下是一些法规的例子：

- 巴塞尔协议 II，要求国际性的金融机构确保系统可用性
- 欧盟数据保护指令，对数据备份与可用性作了规定
- 萨班斯-奥克斯利法案，涵盖美国上市公司的财务数据
- 健康保险可移植性和责任法案 (HIPAA)，要求美国医疗保健信息实现数据可用性

这些指导方针要求企业维护备援资源以实现故障转移，并保持安全而全面的数据备份以确保信息完整性。发生违规的企业将遭受严厉的经济处罚。企业在评估潜在宕机的代价时，必须考虑这些罚款。

## 计算成本

根据 Ponemon Institute 的“2014 年数据泄露成本调研”，企业因数据事故而损失的金额必须包括直接、间接和商机成本，以便准确反映经济损失。<sup>2</sup> 这些因素包括：

- 事故检测：
- 控制事故影响
- 恢复网络、数据和/或核心系统
- 与事后调查相关的取证
- 第三方参与帮助修复问题并审计系统
- 与客户及不合规相关的法律成本
- 培训/增加帮助热线服务人员和支持人员
- 业务中断造成的收入损失
- 客户流失造成错失商机

60% 的事故都是由于人为错误和系统故障造成的。

考虑这些因素，并将其应用于由 10 个国家或地区的 314 家公司构成的调研样本，Ponemon 发现全球每条记录泄露的平均成本为 145 美元，比 2013 年增长了 9%。按国家或地区计算，平均事故总成本从 300 万美元到近 600 万美元不等。值得注意的是，这些信息泄露并不限于网络攻击。平均而言，60% 的事故是由于人为失误和系统故障（即 IT 中断）造成的。

### 代价可能有所不同

自然，并非每个企业都会付出如此高的代价。但有些企业的经济损失可能更大。根据行业不同，信息泄露和运营中断的代价可能远远高出平均水平。例如，Ponemon 发现，医疗保健行业每条记录的泄露损失平均为 359 美元。

对于许多企业部署的信用卡应用，一个小时宕机时间最高可能会损失 260 万美元，而根据 Neverfail Group 的估算，2013 年 1 月 Amazon.com 网站宕机 49 分钟的损失达到近 500 万美元。<sup>3</sup>

<sup>2</sup> Ponemon Institute, “2014 年数据泄露成本调研”，2014 年 5 月

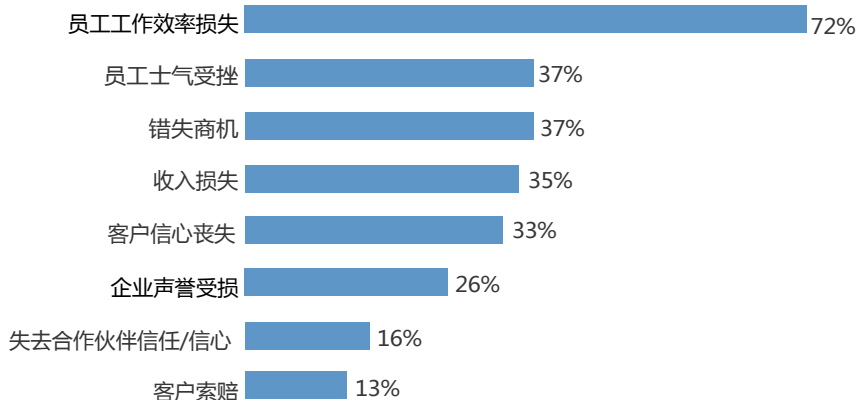
<sup>3</sup> Neverfail Group, “Downtime Report: Top Ten Outages in 2013”，2013 年 12 月



## 灾难恢复计划的更新需要改变

“作为贵公司最严重中断的结果，以下哪些方面会造成最严重的影响？”

(请按 1 - 3 级评分)



样本：全球 66 位灾难恢复决策者以及声称遇到灾难或重大业务中断的影响者

(可选择多项)

来源：Forrester Research, “The State of Business Technology Resiliency, Q2 2014”, 2014 年 5 月

在 Continuity Software 去年进行的一项调研中，43% 的受访者表示每小时宕机会造成 10 万美元或更多的损失，12% 的受访者表示每小时宕机所造成的损失超过 100 万美元。绝大多数受访者 (90%) 认为服务可用性对客户而言至关重要。此外，接受 Continuity 调研的 73 位受访者表示自己的可用性目标高于 99.91%，换句话说，每年意外宕机时间不能超过 8 小时。与 2013 年的 68% 相比，这个数字呈上升趋势。<sup>4</sup>

宕机造成的损失因公司而异，但是在过去四年中，各行业的宕机损失不断攀升，因此计算成本是理解和沟通业务连续性指标要求的一种好方法。

## 当前趋势

有趣的是，尽管我们讨论了面临的所有压力，然而，近几年来，许多企业的业务连续性工作仍然相对停滞不前。

Forrester Research 的报告 “State of Business Technology Resiliency, Q2 2014” (2014 年第二季度业务技术连续性状况) 表明，业务方面对快速恢复时间目标 (RTO) 的要求有所上升，但 2013 年的实际恢复时间平均约为 24 小时，与 2010 年的 18.5 小时相比还有所延长。事实上，在 2013 年的 Forrester 调研中，仅有 2% 的受访者表示他们能够在 1 小时内恢复。<sup>5</sup>

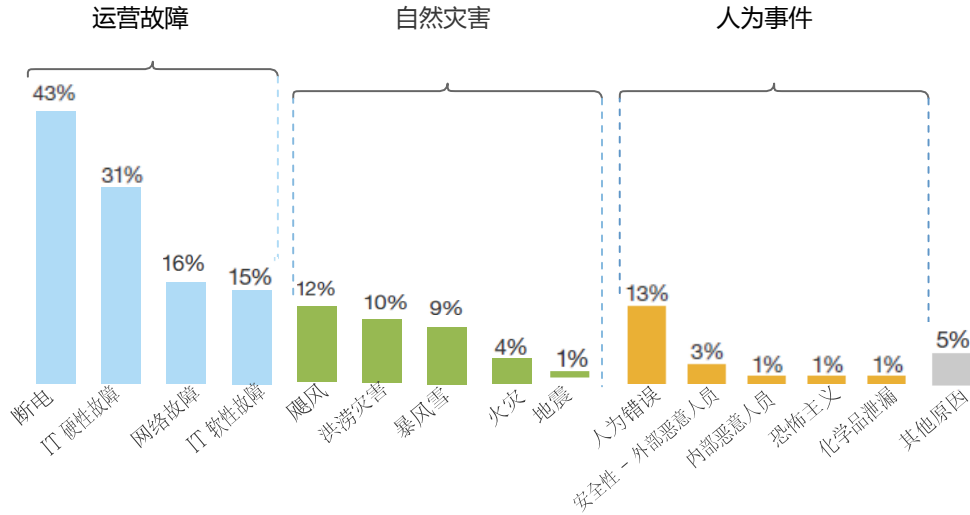
与此同时，宕机的原因还是那些“常客”。据 Forrester 报告显示，即使大规模的灾难 (比如飓风桑迪) 会抢占新闻头条，但断电、IT 故障和认为错误仍是最常见的业务宕机原因。

<sup>4</sup> Channel Insider, “Helping Combat Downtime, On-Premise and in the Cloud”, 2014 年 6 月

<sup>5</sup> Forrester Research, “The State of Business Technology Resiliency, Q2 2014”, 2014 年 5 月

## 宕机的主要原因是日常事件，而不是灾难

“您所遭遇的最严重的灾难或重大业务中断的原因是什么？”



样本：全球 94 位灾难恢复决策者和影响者  
(不包括回答“不了解”的样本；可以回答多个选项)

来源：Forrester Research, “The State of Business Technology Resiliency, Q2 2014”, 2014 年 5 月

其他分析公司也表示赞同该观点。在上述 Continuity Software 调研中，87% 的受访者在接受调研前的 3 个月内经历了宕机事件，最常见的原因是硬件故障、设备升级、人为错误和断电。

同样，毕马威 (KPMG) 的“2013-2014 Continuity Insight” (2013 - 2014 年业务连续性洞察) 报告指出，恶劣的天气和断电是宕机的前两大原因，与 IT 相关的错误位列第三。<sup>6</sup>

因此，如果已经充分了解了宕机的原因，那么为什么恢复时间和成本却会一年不如一年呢？

### 不断变化的形势

答案就是，企业为了紧跟全球竞争的步伐，IT 环境变得越来越复杂，越来越分散。世界各地越来越多的移动和远程工作人员需要随时通过多种设备访问关键业务系统，正如我们所讨论的，任何中断所造成的经济损失会像雪球那样越滚越大。

Forrester 将这种趋势称为“目前时代”。在以上引用的报告中，分析师 Stephanie Balaouras 解释道，通信应用已成为每个企业运营的任务关键型要素，客户的期望值始终居高不下，而且应用之间的相互依赖性（例如，销售工具通过业务流程管理框架依赖于特定数据库）使得环境中的关键组件比以往任何时候都要多。

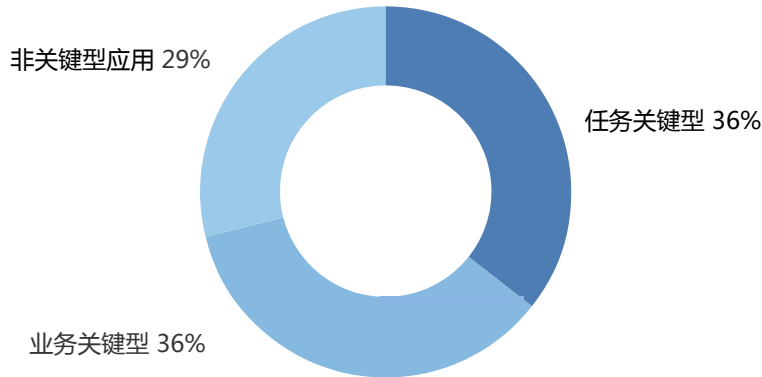
<sup>6</sup> 毕马威，“The 2013-2014 Continuity Insights” 和 “毕马威会计师事务所全球业务连续性管理 (BCM) 计划基准调研”，2014 年 4 月

断电、IT 故障和人为错误是业务中断最常见的原因。



## 任务关键层和业务关键层不断增加

“您的应用和数据占以下各层的百分比为多少？”



样本：全球 94 位灾难恢复决策者和影响者  
(不包括回答“不了解”的样本；由于四舍五入，百分比总和不等于 100)

来源：Forrester Research, “The State of Business Technology Resiliency, Q2 2014”, 2014 年 5 月

与此同时，根据研究公司 Corporate Executive Board 的研究，自 2008 年金融危机以来，IT 预算几乎没有增长过，直到 2015 年才见起色。<sup>7</sup> 这意味着企业无法对资源投资，因此无从谈起对业务连续性战略进行升级或简化。

此外，移动正在改变人员的工作方式。早在 2012 年，IDC 就预测，到 2015 年，移动工作人员的数量将达到 13 亿，占全球员工总数的 37%。<sup>8</sup> 最近，Gartner 发布了一项预测，表示截止 2016 年，38% 的雇主会要求其员工使用自己的移动设备开展工作，到 2017 年，这一数字将接近 50%。<sup>9</sup>

所有这些因素都对传统的业务连续性设置带来了压力，这涉及备援硬件（维护成本高）和磁带备份（恢复时极为耗时）。由于必须仔细准确地确定设备依赖关系和网络路径，因此还可能产生多个潜在的故障点；故障转移期间的任何错误都可能会使整个基础架构瘫痪。

在快速发展和日益互联互通的业务形势下，企业必须找到智慧的业务连续性解决方案，保护自己的基础架构、数据、运营以及工作人员。

<sup>7</sup> Corporate Executive Board, “IT Budget Benchmark Key Findings 2014-2015”, 2014 年

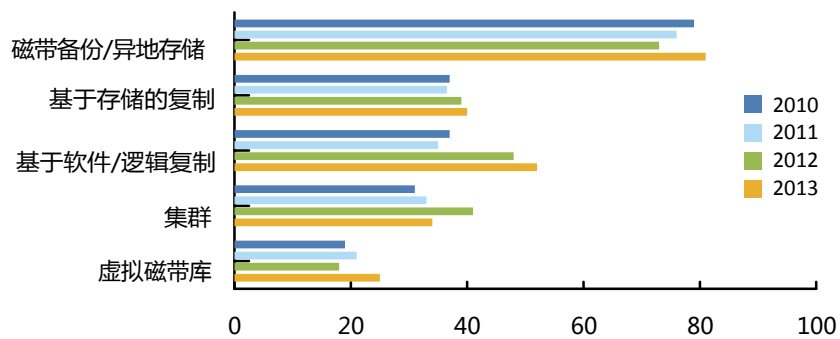
<sup>8</sup> 路透社, “Mobile Worker Population to Reach 1.3 Billion by 2015, According to IDC”, 2012 年 1 月

<sup>9</sup> Gartner, “Bring Your Own Device: The Facts and the Future”, 2013 年 5 月

## 虚拟化和复制

由于虚拟化可以从硬件中抽象出服务器、网络和应用工作负载，因此对各行各业各种规模的企业来说，业务连续性成为了更容易实现的目标。只需极短的宕机时间，即可将整个服务器乃至整个环境都移植到备用硬件中，许多企业还实时复制所有的业务活动，因此备用环境可以随时准备好进行接近实时的故障转移。

数据保护技术：2010 年至 2013 年



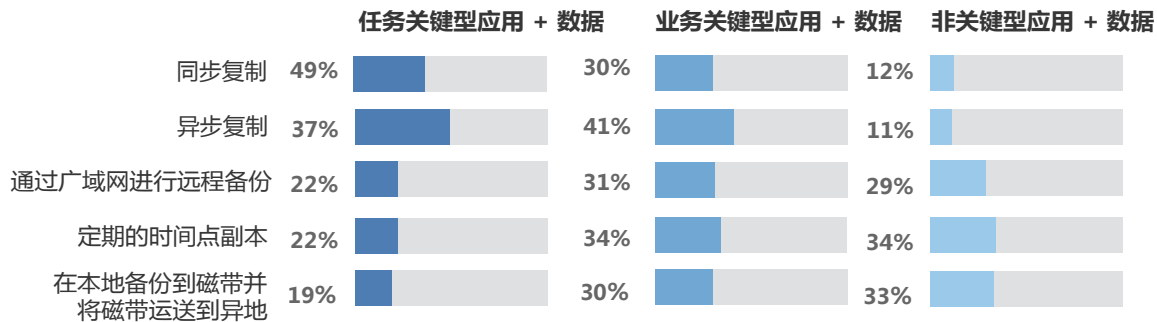
来源：Vision Solutions，“State of Resilience 2013”，2014 年 1 月

Continuity Software 2014 年的调研表明，72% 的受访者在其环境中使用虚拟化功能实现高可用性，与 2013 年的 63% 相比有所上升。

Vision Solution 在针对超过 3,500 名 IT 专业人员的“*The State of Resilience 2013*”（2013 年业务连续性状况）调研报告指出，从 2010 年到 2013 年，基于软件的复制部署有显著的增长。<sup>10</sup> 对比 2010 年和 2013 年，Forrester 发现了相似的趋势，即复制使用率从 35% 增长到超过 50%。该报告补充道，磁带备份仍是保护非关键型系统最流行的方法。

### 主恢复站点之间的数据

“您如何在主恢复站点之间复制数据？”



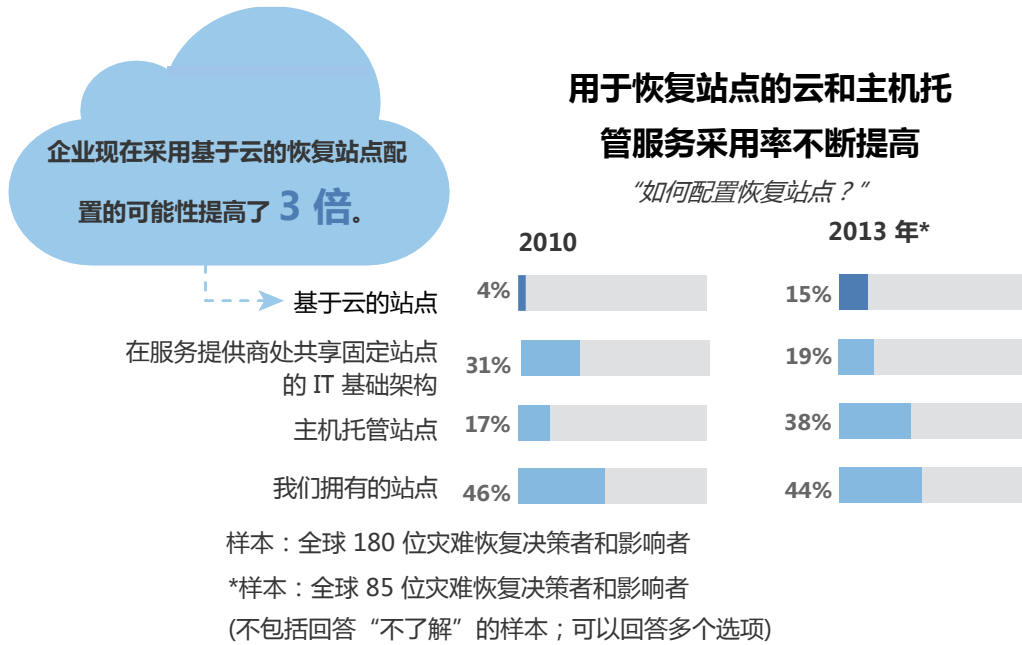
样本：全球 94 位灾难恢复决策者和影响者  
(不包括回答“不了解”的样本；可以回答多个选项)

来源：Forrester Research，“*The State of Business Technology Resiliency, Q2 2014*”，2014 年 5 月

<sup>10</sup> Vision Solutions，“*State of Resilience 2013*”，2014 年 1 月

## 进入云时代

下一代业务连续性计划的最终答案是云服务。如果能够在异地备援基础架构上托管资源，并且能够以 WAN 速度或更快的速度传输数据和虚拟化组件，就可以为希望在发生中断时确保快速恢复的企业提供多种故障转移选项。



来源：Forrester Research, “The State of Business Technology Resiliency, Q2 2014”, 2014 年 5 月

除了传统的内部资源，还包括以下选项：

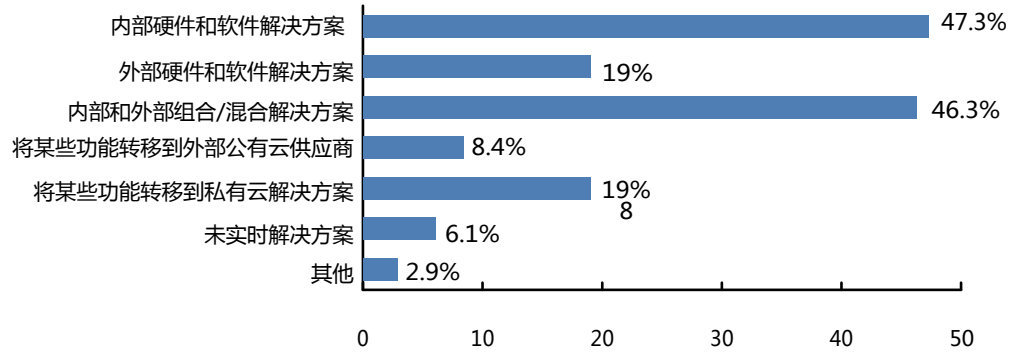
- 主机托管设施中的专用异地资源
- 在异地设施中共享基础架构
- 内部部署或托管私有云
- 公有云

72% 的受访者使用虚拟化功能实现高可用性。

许多企业所采取的战略是将这些选项中的一些组合成混合业务连续性解决方案。根据 Forrester 的报告，基于云的恢复选项的采用率从 2010 年的 4% 上升到 2013 年的 15%，同时主机托管的采用率也在上升。根据 Forrester 的调研，五分之一的受访者表示他们使用混合模式为关键系统提供快速故障转移能力，为非关键系统提供分阶段的恢复方案。

毕马威的研究发现，混合解决方案和云灾难恢复解决方案的采用率略高，接近 20% 的受访者采用私有云，仅有 8% 多一点的受访者表示他们使用公有云服务来实现某些功能。

## 企业目前的 IT 灾难恢复战略



来源：6 毕马威，“The 2013-2014 Continuity Insights”和“毕马威会计师事务所全球业务连续性管理 (BCM) 计划基准调研”，2014 年 4 月

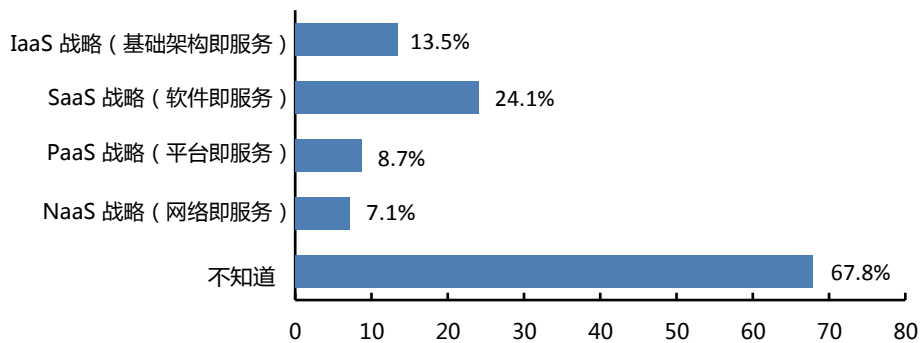
## 云端的不明确性

由于云服务相对较新，而且云计算的采用（尤其是在大型企业）通常是零星而分散的，因此关于云 SLA 的参数非常之混乱；数据安全性、所有权和位置以及发生影响云提供商的中断时的负责人员也不是很明确。

例如，在 Continuity Software 的调研中，44% 的受访者表示云服务可用性与内部系统相当。约 30% 的受访者表示云服务的可用性低于其他系统，还有 26% 的受访者表示云服务的可用性相当出色。这种趋势似乎表明，企业不一定准确地掌握内部和基于云的服务的可用性指标。

毕马威的调研结果证明了这一结论 - 高达 68% 的受访者不了解基于云的 IT 灾难恢复指标的性质。虽然恢复服务通常包括按需应变的基础架构 (IaaS) 和托管软件解决方案 (SaaS)，以及托管计算平台 (PaaS) 和网络解决方案 (NaaS)，但大多数受访者并不了解自己的云业务连续性计划包含哪些内容。

## 企业目前已在云端实施的 IT 灾难恢复计划



来源：6 毕马威，“The 2013-2014 Continuity Insights”和“毕马威会计师事务所全球业务连续性管理 (BCM) 计划基准调研”，2014 年 4 月

## 合作

---

我们已经清楚地认识到，业务连续性越来越重要，而且在很多方面以往任何时候都更难以实现，而云服务可以提供多种类型的异地资源托管，将虚拟化与复制提升到更高的水平。

然而，由于云服务存在诸多不明确性，因此与专业业务连续性服务提供商密切合作就显得至关重要，这样您就无需绞尽脑汁去理清成功的混合恢复部署所需的各种联系、SLA 以及相互依赖关系。

幸运的是，企业可以与业务技术解决方案领域无可争议的领导者 IBM 合作，将灾备服务从内部迁移到基于云的环境。

### IBM 业务连续性及灾备服务

IBM 可以提供全面的业务连续性和灾备服务组合以及专家咨询，能够满足任何企业的需求。通过结合数据中心、硬件、软件、技术专家和云服务的强大能力，IBM 可以帮助客户精心制定业务连续性和灾备计划，实施量身定制的解决方案，确保实现无缝的故障转移和故障恢复、数据安全性、事件修复以及合规性。更理想的是，IBM 可以管理整个解决方案，因此客户无需扩充内部 IT 资源。

IBM 业务连续性及灾备服务包括：

**业务连续性咨询服务：**凭借 IBM 数十年的成功经验，帮助您规划、设计、集成和测试整个企业的业务连续性和灾备战略，考虑企业总部和所有办公地点的应用和基础架构。

**基础架构恢复服务：**IBM 可以对您的 IT 系统进行全面充分的评估，制定数据保护和恢复战略，包括出现事故时使用的异地备份和本地恢复协助。该服务是具有合规要求以及复杂环境的企业的理想之选。

**可用性管理服务：**IBM 专家顾问帮助您分析以前的事故，制定与业务流程保持一致的战略，避免未来发生宕机。IBM 指派专门的项目经理监督项目的每个阶段，从而将您的内部 IT 资源解放出来，专注于业务运营和创新。

**管理灾备服务：**将灾备任务交给 IBM。在您指定出现中断时需要保持运行的信息和系统后，IBM 将为您提供灾备管理服务，可根据重要性定制积极主动的事件响应服务。

**云灾备服务：**IBM 的云服务包括备份、恢复和虚拟化数据管理，旨在实现灵活的访问和全面的控制。只需数分钟即可恢复服务器、应用和数据，从而降低风险，提高合规性，保持生产力。

**云虚拟化服务器恢复服务：**IBM 云恢复服务可以确保虚拟和非虚拟资源不受中断的影响，自动执行故障转移步骤，提高业务运营的可靠性。

针对恢复环境的可选监测服务有利于保证客户的合规性。该服务支持范围广泛的服务器操作系统和平台。

**云管理备份服务**：如果您在寻找一种全面而安全的备份解决方案，能够自动地执行现场和非现场复制，那么 IBM 管理备份服务就是理想之选。这些服务支持私有云、公有云和混合云模式；提供可动态扩展的解决方案，有助于降低总体拥有成本；包含加密与数据去重功能，能够实现企业级的安全性与高效率。

### IBM 的竞争优势

IBM 业务连续性及灾备服务是全球唯一能够在企业所有层面真正实现业务连续性的供应商。我们以多种方式为客户的设施提供支持：

- IBM 在全球范围运营超过 312 个云灾备中心，提供了计算和网络资源，支持技术层以及数据和应用层的复制与数据保护，并提供世界级的业务连续性咨询方法。
- 这些设施包括超过 1000 万平方英尺用于灾备和灾难恢复运营的数据中心场所，以及用于恢复工作场所运营的 41,000 多个工位。
- IBM 业务连续性及灾备服务目前为 68 个国家或地区的 6,000 家客户提供服务。
- IBM 在对宣布遭受灾难的客户履行承诺方面实现了 100% 的成功率。

欢迎与 IBM 合作，充分利用我们在数据保护和业务连续性及灾备服务方面长达五十多年的丰富经验。

有关 IBM 业务连续性及灾备服务的更多信息，请访问 [IBM Data Center Services](#)。



## 关于 IBM

IBM 是一家全球整合的技术和咨询公司，总部位于纽约州阿蒙克市。IBM 在 170 多个国家或地区开展业务，帮助企业、政府和非盈利组织解决问题，提供最前沿的产品、服务和解决方案。该公司开发和销售软件和系统硬件，以及广泛的基础架构、云计算和咨询服务。现在，IBM 专注于三项战略使命 - 通过数据实现行业与专业转型，为云时代重塑企业 IT 基础架构，以及为企业实现“互动参与系统”。