IBM 全球信息科技服务部

思想领导力白皮书

2015 年 6 月

云灾备

IBM

目录

摘要

在当今移动和社交互联的世界，用户希望随时随地能够通过多种接入平台和多个位置实现互联。在这个业务永续的世界，人们已经不能容忍任何宕机和数据丢失。在低成本的灾难恢复解决方案和高成本的复制这两个极端之间，很多企业开始选择云模型这种更为经济实惠的方式，来满足快速恢复系统和数据的要求。

不可否认，在降低成本、提高敏捷性和降低风险方面，云计算有着巨大的潜力。但如果未能对灾备进行妥善的规划和实施，就有可能无意中增加企业的整体风险。云解决方案的许多用户都假设存在某种程度的连续可用性，而并非所有云服务中均设计有这样的连续可用性。换句话说，如果只是因为可能存在改良的、更敏捷的灾备方案，这并不意味着仅仅因为工作负载迁移到了云中，其灾备便可自动获得。当涉及到灾备时，必须将云作为另一种技术领域进行查看和评估，定义、评估、测量和监控其功能性和非功能性灾备要求。

对于企业来说，要降低整体开支，并提高对云计算风险、威胁和机会的响应能力，正确的使用云计算的决策至关重要。然而，不管有多么必要，明确需求和风险，确定其优先顺序，并拨款解决这些问题，并非总是那么容易。为了做到这一点，企业需要收集和分析正确的信息，以做出与灾备风险的成本效益管理相关的价值驱动决策。

无论是将工作负载迁移到云计算平台，还是寻求“灾难恢复即服务”(DRaaS) 模型，云方案均需要在企业风险综合管理的思路上做出根本性的转变。虽然当今的大多数云方案实施中普遍缺乏灾备规划，但是较为完善的前期评估和规划可以帮助企业实现潜力巨大的云产品，从而改进灾备，使之更敏捷，并且在业务服务可用性要求和风险容忍程度之间达到恰当的平衡。

灾备临界点

在过去的几年里，用于开展日常业务的内外部系统的生态系统受到了更多的限制，而暴露的风险则要少得多。在今天的典型企业里，用户参与到同时利用内外部信息和服务的多个系统中，以开展工作。随着系统、数据和用户数量的增长，对分析的依赖性以及系统之间的相互依赖性也在增加，同时，灾备的复杂性和必要性也在不断提升。例如，当顾客进行网上下单时，交易成功与否取决于网站、电子商务应用、后台交易系统、向仓库发出订单项目和送货目的地的系统，以及刷新仓库中存货的库存系统。

如果上述任何一方面出现故障，那么，整个过程将被打乱，包括先期吸引客户购买的互动系统和洞察系统、客户跟踪交付的互动系统，以及企业跟踪客户体验和情绪的洞察系统。

您是否已经达到了云灾备的临界点？查看信息图：

维护灾备基础架构的成本和工作量让许多企业放弃了传统的灾难恢复技术，转而选择云灾备。

云解决方案拥有快速故障转移能力，即使企业的系统与用户相隔万里，云解决方案也能帮助确保接近连续的应用和数据可用性。云还可为企业灾备和快速提供新服务的能力带来前所未有的可扩展性，而且许多商业灾备和灾难恢复提供商在多年前就已经开始提供这些特性了。不同的是，云现在可以在客户的控制下提供一些这样的特性。

然而，到目前为止，很少有应用能充分利用云计算提供的灾备能力。目前，许多对于云项目的关注围绕于尽快找出目标工作负载，并将其迁移到云中。虚拟化工具和所有的云解决方案均未在灾备方面有本质上的提高。此外，出现的新的云计算服务，如经纪人业务、协调服务和服务目录系统等新的云服务均带来了关键的单点故障问题；而如果发生了此等故障，则需要停止服务，以保护数据和交易一致性。如果灾备没有被集成到最初的云应用中，企业就会在有意识或无意识的情况下承担风险。虽然一直以来，均有将云用于灾难恢复的用例，但对于怎样有效使用，包括如何有效地测试以保证基于云的灾难恢复和灾备策略以预期的方式工作，仍然缺乏充分的指导。

如果企业没有将灾备集成到其最初的云应用中，它们就会在有意识或无意识的情况下承担风险。

云灾备现状

就灾备而言，大多数企业发现，在其传统的环境中，这些问题很难回答：

- 您能对宕机一小时的成本进行可靠的量化吗？
- 您能提供准确的测试证据，从而证明您最快能在何时恢复业务运营吗？
- 您知道您的数据损坏的风险集中在哪儿吗？
- 您知道大致的影响程度吗？

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 万美元至 100 万美元。[1]

在云环境中，对上述问题可以给出可靠答案的企业少之又少。因为不断变化的业务要求，云部署的事务处理量和事务处理能力通常包括不可预测的流量模式以及偶尔的大规模波动。架构更加开放，并且拥有多个供应商、互联网服务提供商、管理系统、连接选项和技术。借助于不断变化的技术和新兴的标准，云可以显著提高复杂性以及进一步推动复杂性的波动水平。在必要时，还可以对运行的程序进行连续感知和实时监控。

对于任何云部署，无论是灾难恢复即服务模型(DRaaS)还是其他云解决方案，鉴于运行中断的复杂性和影响，都需要灾备专家谨慎地介入与监督，并且应用经过充分测试的有效方法与技术。

例如，异地数据存储和处理能力有助于降低因单个站点运行中断而产生的风险和影响的集中度。但是，在没有对灾备策略和架构进行谨慎规划和设计的情况下转移到另一个站点，这非但不能降低企业风险，还有可能导致企业风险的整体提升。即使是多站点部署的风险集中也可能造成瓶颈和单点故障。尽管云计算可以连续访问数据和计算能力，且复制起着关键的作用，但它仍然带有复制错误的风险。

多个云服务提供商和多个位置之间的系统恢复需要高水平的 IT 集成技能。

此外，企业还需要考虑它们应如何将云解决方案重新集成到遗留的生产环境中。大多数基于云的大型企业工作负载与遗留基础架构环境中运行的工作负载交互，这就意味着，在业务正常运行和中断的情况下，企业都需要考虑到这种互操作性。在新的混合环境中，需要进行艰苦的协调和安排，特别是涉及到与灾备相关的测试以及实际故障转移时，需要将各种不同的工作负载向周围转移和重新同步。

同步不仅仅是确保数据的辅助副本与主要副本相匹配，而自动化也不仅仅是编写应用重启程序的脚本。

企业必须证明自己可以利用灾备系统继续运营，这样的监管压力与日俱增。要提供证据证明灾备响应时间满足企业的需求，就需要进行测试，在其中有效地重新创建用户体验，从而证实灾备计划的有效性和价值。在过去，监管部门的主要精力放在交易性系统上。而现在，企业聚焦于客户互动系统，其业务对洞察系统的依赖性日益增强，以实现对区域营销、情绪分析和非结构化数据分析的实时处理，因而对业务永续体验充满期待。上述三方面处理的复杂性和相互依赖性需要被纳入到灾备策略和设计中。今天，每家企业的声誉都是通过客户的口碑实时建立或失去的。

云环境中的灾备测试本身也带来了一系列的挑战。例如，真正的灾难恢复测试需要将生产环境和灾备连接路径相隔离因为（您不能同时在两个地方拥有生产 IP 地址，也就是您的数据中心和您的云灾备解决方案）。这就意味着，要弄清楚怎样获得在生产环境中被屏蔽的第二组 IP 地址。这将允许在不对生产活动产生负面影响的情况下，进行综合测试。

在云中，IP 地址的管理和隔离比以往都更为关键。当互联网成为您的生产加工和灾备测试环境的一部分时，如果发生问题，企业就会处于巨大的风险中。

总之，传统、狭窄的 IT 的验证和恢复范围早已不足以满足企业需求。灾备环境的运行也不再与生产环境运行相同。

云灾备需要一定的技能和经验，以确保正确的设计、架构、安排、管理、监控、报告和治理已经到位，使系统正常工作。要在云中维持灾难恢复环境可能比较简单，但就关键的交易性系统、互动系统和洞察系统的恢复而言，需要做的工作就会更多，以提供证据证明在发生中断的情况下，企业可以继续运营业务。

正确的云灾备方法

云灾备的现实是，如果您没有对它进行设计、实施和维护，您就无法实现云灾备。但企业应该怎样确保其从一开始做的就是正确的呢？根据最佳实践，正确的方式是采用一种结构化的方法，使企业能：

- 了解目标云工作负载支持的业务负载、对应的业务和 IT 灾备要求，以及云/遗留应用/数据依赖性的重要性
- 确定相关风险和所对应的处理方法
- 制定能满足业务灾备需求的最佳云策略
- 记录云和遗留环境之间的联系、相互依赖性和同步点
- 制定、实施、测试和维持相应的业务和技术灾备计划和程序
- 创建云计算特定的/集成云环境/遗留灾备系统的验证和测试计划
- 制定云灾备过渡路线图

进行灾备云基础架构的设计和规划已经是一项十分艰巨的任务，更不用说实施和管理了。但企业可采取一些关键的策略和步骤，对云灾备进行规划和管理。图 1 列出了 IBM 弹性企业框架(Resilient Enterprise Blueprint) 方法的四个步骤，该方法对云灾备从评估到管理进行了考量。

图 1. IBM Resilient Enterprise Blueprint 方法的四个步骤。

步骤 1 - 评估和评价

几乎没有企业有能力让其整个 IT 环境“永续”。相反，灾备应与业务价值相联系。结构化方法可以帮助企业谨慎地从灾备角度来确定业务要求，这可推动灾备目标和指标（例如，关键业绩指标和关键风险指标）。您可以先确定和记录灾备等级，并且与您的业务用户就每一等级的恢复时间和恢复点目标以及每一级别对应的业务功能达成一致。

这将为您提供一些衡量标准，用于评估不同的云方案的特性和功能。

有了这些信息，企业需要能够理解服务和基础架构之间的相互依赖性及其对这些业务目标达成的影响，同时希望他们能够转移。在您理解这些风险后，

您可以制定不仅能满足业务需求，还能让您能进行验证的适当的灾备策略和架构。这个过程中的主要活动包括：

- 收集目标云工作负载的关键业务灾备要求
- 分析包含相关基础架构组件和数据、治理政策、灾备策略和计划的现存应用链
- 就灾备要求和能力对目标云工作负载进行评估
- 记录云和遗留 IT 环境中运行的应用工作负载之间的联系、相互依赖性和处理/数据同步点

企业没有能力让其整个 IT 环境“永续”。灾备应与商业价值相联系。

步骤 2 – 规划和设计

设计阶段必须包括完全集成的方式，企业通过这种方式“运营业务”，包括服务依赖关系。然而，云较高的抽象程度可能为确定和记录服务依赖关系蓝图带来挑战。云计算参考架构(Cloud Computing Reference Architecture) 正好可以在这些方面为包括配置、复制、自动化、监控和报告等在内的管理工具集提供帮助。

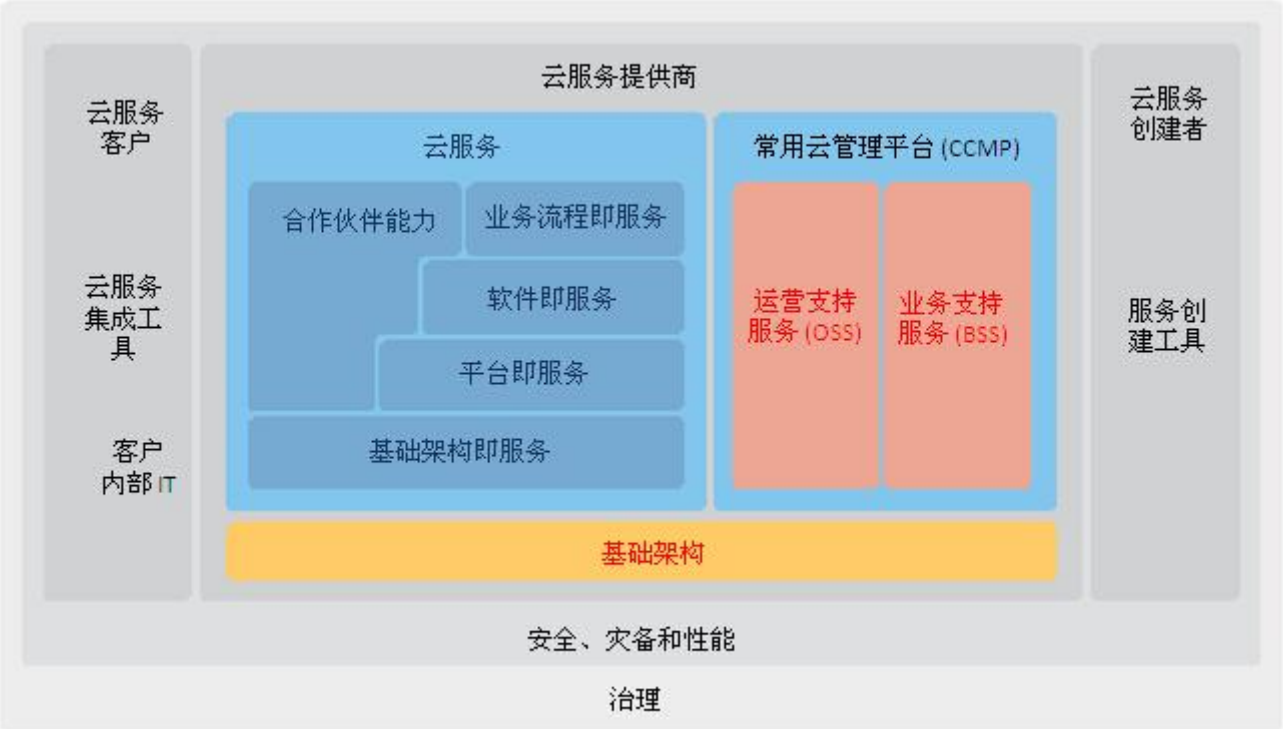

图 2. 云计算参考架构(Cloud Computing Reference Architecture) 有助于确定相互依赖性。

为了能有效地利用这些工具，您可以将参考架构与 IBM 的弹性企业框架(Resilient Enterprise Blueprint) 方法结合起来，从而对应用等级的相互依赖性、关机和重启序列，以及云和传统 IT 环境中的处理和数据同步点有一个更清晰的认识。还应对风险集中度进行记录，不管风险是因潜在的能力瓶颈产生，还是因单点故障产生。

弹性企业框架(Resilient Enterprise Blueprint)方法可以帮助您了解您是否面临着可以接受的风险或者想要避免和减轻的风险。换句话说，您可以选择不对风险采取任何措施，也可以改进您的基础架构，以确保您可以在事件发生时对其进行处理。只有全面理解了功能性和非功能性要求（包括灾备），企业才可以进入规划和设计阶段，其中包括：

- 确定对云和工作负载关联群组以及集成云/遗留应用依赖性群组的范围内灾备要求。
- 了解配置前置时间对恢复时间和恢复点目标的影响
- 在架构和交付模型设计中，使用云灾备指导原则。
- 理顺遗留环境和混合云灾备策略，以确定满足灾备需求的最佳方案
- 制定灾备策略，进行灾备架构设计

步骤 3 - 实施和测试

以下关于云的错误看法始终存在：测试只是简单地提供您所需的内容，执行测试，并移除配置，从而回到之前的状态。正确地创建和设计测试环境，不仅仅是需要激活基础架构，或将数据副本丢到云中。

企业应能维持严格的 IP 地址管理、数据副本管辖边界，以及能证明其不仅能执行测试，还能产生预期的实际结果的证据线索。

在实施和测试之前，您要考虑到最终的结果：实际测试，以及在面临重大服务中断的情况下，在备用环境中“运行业务”的能力。利用这条信息，您便可通过以下步骤，制定相应的业务和技术灾备计划和程序：

- 使用方法和工具配置目标灾备环境，将虚拟或物理服务器自动化，以实现连续性，并为灾备测试配置云工作负载
- 创建云环境特定的/集成云环境/遗留灾备系统的验证和测试计划（可包括定期推出计划内故障，以测试实时组件/服务灾备）
- 测试云灾备策略，并获得客户认可
- 为审计和报告而保留测试范围和结果的证据

部分或组件级别的测试，以及问题会在中断时“自己解决”这样的盲目观点已经不再为人们所接受。

步骤 4 - 管理和维护

云的速度和灵活性可以为用户带来极大的敏捷性，但通常也会带来较高程度的波动。强大的治理、管理和控制流程都是必需的，以使灾备能力与生产环境同步。监控和报告是关键，因为灾备不是一个“一蹴而就”的项目。相反，它是一个运营流程，管理人员需要知道企业在任何时候的实时状态，尤其是在计划外运行中断的情况下。管理和维护灾备能力的步骤包括：

- 设计/更新灾备方案框架、监控、治理和灾备风险报告，以将云纳入其中
- 制定云灾备过渡路线图
- 为 IT/云灾备的利益相关者制定云教育方案
- 过渡到稳定状态的综合灾备方案管理和报告
- 保持持适当的制衡：
  - 保障（包括第三方）和认证
  - 应用就绪
  - 流程就绪，供应商的稳定性和声誉，迁移到另一个位置/供应商的灵活性
  - 连续性要求
  - 网络
  - 数据 - 位置、防护、隔离
  - 治理、风险和合规性 (GRC)

结论

在业务永续的世界里，运行中断的复杂性和影响极大，因此需要更加注意灾备解决方案的设计和管理。在复杂的多提供商系统中，基于服务的灾备意味着，您需要采取不同的思维模式。

云的发展带来了对灾难恢复的高效性和经济性的预期，然而这样的预期基本未实现。如今，适当设计、实施和测试的云灾备解决方案仍然相对较少。

现实情况是，传统与云 IT 环境之间的结合并不会很快消失，而假定的云“内置”灾难恢复能力也不会将灾备简化，事实上，它们让灾备变得更加复杂。企业在无灾备专家介入和监督，以及未应用经过充分测试的有效方法和技术的情况下获得并部署云解决方案，这会大大增加企业风险。

从创新云服务到全面的计算、数据和应用灾备解决方案，IBM 已经具备了公认的专业技能、知识和技术，能够帮助您的企业在面临来自企业各层面以及任何 IT 环境（包括公共云、私有云或混合云）的威胁和机会时，实现内置（而非附加）的灾备。

进一步了解四步走企业灾备蓝图方法如何用于使用云来开发持续可用性：

“业务永续”的历程分为四个步骤

我们坚定地致力于了解不断变化的业务需求，因此，我们的企业灾备服务和久经考验的解决方案可以帮助您规划和设计云灾备的实施和管理。

更多信息

欲了解有关 IBM 灾备服务的更多信息，请联系您的 IBM 代表或 IBM 业务合作伙伴，或访问以下网站：http://www-935.ibm.com/services/cn/zh/it-services/businesscontinuity/

观迎参加云灾备需求度调查，填写调查表，你即有机会预约一对一专家咨询（名额有限）

http://www-31.ibm.com/ibm/cn/gts_cloud_resiliency/

IBM Global Technology Services
Route 100
Somers, NY 10589

美国印刷
2015 年 6 月

[1] IDC，“DevOps 和宕机成本：最佳实践量化指标财富 1000 强”。Stephen Elliot．2014 年 12 月，IDC #253155。

BUW03048-CNZH-00