高级虚拟数据中心技术手册之灾难恢复

高级虚拟数据中心技术手册之灾难恢复

一个牢固的灾难恢复计划能克服带宽和延迟问题，不会存在数据的丢失。在数据中心里，恢复数据和预防丢失的技术有很多种。虚拟化提供额外的好处，使你的架构更加稳定、有效和易于管理。在我们这一些列高级虚拟化手册中学习如何充分利用虚拟化技术。灾难恢复能真正从高级虚拟化技术中受益。建立远程 DR 站点并为业务连续性规划有助于确保数据和应用的安全，在发生硬件故障时仍能访问。我们将在该手册中详细阐述灾难恢复策略。

融合的灾难恢复方法

灾难恢复（DR）并不只是简单地保护数据或者重新找回数据，而是指保持业务操作的稳定性和持续性，在极端的情况下也只是允许很小（甚至没有）中断。很多公司都同时使用多种容灾恢复方案来应对性能问题。

- 虚拟数据中心的灾难恢复战略介绍
- 虚拟化在数据中心灾难恢复中的作用
- 数据中心灾难恢复需要考虑哪些因素？

网络带宽和延迟

实现灾难恢复的挑战在于不用冒数据丢失的风险，跨越更长的距离移动不断增长的企业数据。有一些因素会使这个过程进一步复杂化，比如，网络的带宽和延迟。

- 灾难恢复策略之网络带宽和延迟

重复数据删除功能

重复数据删除在容灾恢复中也扮演了重要的角色。通过删除重复的文件、数据块和字节，可以大幅减少数据节点中需要复制的数据达 50%~80%。这样的话，“变小”的数据站点就可以很快被复制到远程容灾站点。

- 灾难恢复策略之重复数据删除功能的用途
- 探讨重复数据删除后的灾难恢复

容灾管理工具

存储资源的管理，尤其是在虚拟化数据中心里尤为重要。虚拟化软件极大地淡化了管理员对上层的应用软件及底层硬件系统的关注。这意味着，在您的虚拟数据中心中，您可能无法动态地检测和调整应用程序的负载，或者在硬件发生改变时无法及时获知，这也影响了故障诊断和处理的效率。

- 灾难恢复策略之容灾管理工具软件及效率
- 使用开源复制工具来降低灾难恢复成本
- 数据中心灾难恢复需要外包还是自己解决？
- 灾难恢复规划工具：是否物有所值？

案例分析

本部分提供关于灾难恢复的案例和分析。

- 灾难恢复需要多少个数据中心？
- 您的灾难恢复规划过期了吗？

虚拟数据中心的灾难恢复战略介绍

灾难恢复（DR：Disaster Recovery）并不只是简单地保护数据或者重新找回数据，而是指保持业务操作的稳定性和持续性，在极端的情况下也只是允许很小（甚至没有）中断。但是这样的话就把 IT 管理人员带到了一个两难的境地：管理员必须了解大量工业界情况和公司的特定数据保护和恢复需求，然后才可以确定并且实施强有力的解决方案。

在了解 DR 的这些基本概念之后，就必须检查当前的方案，并且清楚地明白在虚拟数据中心中可能影响到 DR 策略的主要因素。IT 管理员需要掌握各种各样的技术方案来应对企业的 DR 规划，其中最重要的就是虚拟化技术。虚拟服务器将会需要储存空间保存主机以及每一台虚拟机的“黄金”镜像和即时备份（定期快照）。也可以虚拟化存储设备，使所存储的数据可以在不同物理站点之间便捷迁移。

“EMC 的 V-Max 和 NetApp 的 VSeries 可以在虚拟机之上虚拟化存储空间”，Long View Systems 的数据中心实施总监 Pierre Dorion 说。Long View Systems 是一家 IT 解决方案和服务公司，总部设在 Denver。

桌面平台虚拟化的使用率也在不断上升，并且允许公司在数据中心服务器上宿主每一台主机而不是在个人桌面的 PC 机上。这样的解决方案可以提供一个较高层面的安全和控制，每一个桌面平台实例匹配用户的特定配置、用户的应用程序以及用户的数据——需要必须得到保护的额外存储空间。

现在存储区域网络（SAN：Storage Area Network）是虚拟数据中心的主干线，并且支持在两个或者更多物理站点之间的常规性数据复制——这是很多 DR 实施方案中的关键技术。当前的 SAN 可能使用传统的光纤线路（FC：Fibre Channel）或者 iSCSI 架构，这取决于公司的规模以及其存储性能需求。NAS 系统也支持虚拟化。

从一个站点往另外一个站点拷贝数据并非完全是技术性问题，但是传输的性能因素可能建立或者中断 DR 配置。尽管带宽费用在不断下降，但同时公司必须移动更大量的数据卷并且需要保证移动时数据不丢失。

融合的 DR 解决方案

很多公司都同时使用多种容灾恢复方案来应对性能问题。例如，首先在本地存储系统使用快照，可以实现快速备份并且不会有延迟问题。把本地拷贝异步复制到远程 DR 站点，允许长距离传输，而不用太关注带宽和延迟问题。尽管存储需求成倍增加，但是该方案可以在两个支持数据拷贝中实施而不是只有一个。

该方案一个变化就是把数据同步复制到近距离的 DR 站点，然后再把这些数据异步复制到远距离 DR 站点。

使用这个融合的 DR 方案，可以根据公司需求中保护的数据类型而采用不同的复制优先级。同步复制和异步复制两者的选择是一个非此即彼的命题，例如一家公司的重要业务数据库可以接收到 DR 站点的同步复制——实时保持两端数据的同步。异步复制足以能够保护每天的业务数据，但是需要一定的数据分级知识以及对特定数据重要性的把握。然而，这样做可以优化 DR 复制的效率，并且需要很少或者不需要任何额外费用。

IT 管理员使用各种各样的技术手段进一步应对同步方案的性能问题，以减少所有的数据集和增强 WAN 性能。

部署桌面平台虚拟化的单位同时使用多种终端虚拟化技术。企业并不是在虚拟桌面平台基础架构（VDI： Virtual Desktop Infrastructure）和应用程序虚拟化之间选择，而是把关键应用程序部署在 VDI 实例中。该方案提供严格的 VDI 中心化控制，不会增加对主要应用程序的备份。同时也可以在很大程度上减少每一个桌面平台实例的存储空间、加速 DR 复制。

（作者：STEPHEN J. BIGELOW 译者：王越 来源：TechTarget 中国）

原文标题：虚拟数据中心的灾难恢复战略介绍

原文链接：http://www.searchvirtual.com.cn/showcontent_30723.htm

虚拟化在数据中心灾难恢复中的作用

现在，许多公司都在它们环境的某处使用虚拟化技术。但是，他们可能不知道如何使用虚拟化技术来进行数据中心灾难恢复规划。学习如何应用虚拟化到灾难恢复很有用，也会受到很多技术上的限制。

在商业服务器领域，虚拟化技术有如野火般迅速蔓延。通过将旧服务器整合到多核多处理器的新服务器可以获得非常诱人的投资回报率（ROI），但很多 IT 企业虚拟化服务器的速度都还不够快。

在世界各地的研讨会和大型会议上，我与很多 IT 经理、主管和 CIO 都探讨过业务持续和灾难恢复的话题。在与他们讨论的同时，我还针对商业服务器虚拟化的应用做了民意调查，发现了一些很有趣的现象。和我讨论的这些人当中，大约 75%的人在他们的环境中应用了虚拟化技术，包括测试、开发和生产。大约 33%的人表示在生产系统中应用了虚拟化技术，其中，几乎 100%的人都是为了获得服务器整合的效益才应用这个方案的。令人吃惊的是，很少有人（不到 5%，甚至有的听众中一个都没有）使用高级软件，如 VMware 的 DRS（分布式资源调度程序）或 Vmotion。

每次，听众中都不到 10%的人应用高可用性集群保护虚拟机基础设施，这让我感到很震惊。同样，很少有人积极地利用虚拟机技术进行灾难恢复（DR）。很多人表示他们倒是愿意看看如何借助虚拟化进行灾难恢复，但是目前还没有执行过。

尽管一些 IT 公司都一致宣誓要做好灾难恢复，但它们很少有人利用高级虚拟化软件进行灾难恢复。那么，虚拟化在灾难恢复时有什么了不起的作用呢？下面，我们一起来看看：

硬件独立：基于物理系统的灾难恢复解决方案都需要将相同的硬件保留到恢复站点，或必须经过很多复杂耗时的步骤在新的或不同的硬件上重建服务器操作系统。有时候碰巧恢复服务器就是同一个硬件模型，但是包含了最新硬盘控制器固件，会导致服务器镜像延迟。虚拟化使硬件从操作系统中抽象化，而且使操作系统中使用的设备驱动器统一化，不管是何种底层硬件模型，所有虚拟机都使用一个共同的驱动集。这样，在新服务器上安装服务器镜像时就省了很多设备驱动对应的麻烦，大大减少了恢复时间和配置错误的风险。

虚拟机磁盘格式文件：虚拟机将其子操作系统、应用、存储和配置（如 IP 地址）存放在一个文件里。这个文件——虚拟机磁盘格式（VMDK）或虚拟硬盘（VHD）文件，包含了整个操作系统环境以便能进行简单的虚拟机装载和保存。这个文件不仅包含了操作系统镜像和应用编码，还描述了虚拟机所需的配置，其中包括虚拟处理器、内存和设备。这个简单的可移动文件包含了组成服务器所需的一切信息、服务器环境描述、实际码和数据。从虚拟机磁盘文件启动虚拟机时系统会自动迅速设置所有参数。在灾难恢复站点进行恢复会变得很简单，只需启动 VMHD 或 VHD。

物理工具到虚拟工具：虚拟机解决方案需要利用管理工具来创建、启动、停止和保存虚拟机镜像。为了方便创建虚拟机，有很多工具可以帮助分析物理服务器和从服务器创建 VMDK 或 VHD。从物理系统创建的 VMDK 或 VHD 文件可以很快地部署到恢复站点。

硬件再利用：恢复站点的虚拟机硬件不必闲置在那里等着灾难发生，它也可以用作开发、测试或其它用途。当发生灾难时，关闭用于测试或开发的虚拟机，然后启动生产虚拟机，这个过程只需几秒钟即可完成。

基于虚拟化技术的灾难恢复解决方案看起来很似乎很不错，不过一定也有其不足之处，不是吗？这些解决方案对大部分工作有效，但并不是全部都管用。有些要求苛刻的应用，如高 I/O 数据库，可能会由于额外的虚拟化管理费用而限制了它们的性能。目前，大多数数据库厂商的产品还不支持虚拟化环境（但这即将会改变，所以请关注市场动态）。另外，有些应用或服务需要专门的硬件设备，在虚拟环境中可能不支持它们所需的那些设备。在这些特殊情况下，你就只能用统一物理硬件的方法来建立灾难恢复解决方案，忍受更加繁琐的恢复过程了。

（作者：Richard Jones　译者：涂凡才　来源：TechTarget 中国）

原文标题：虚拟化在数据中心灾难恢复中的作用

原文链接：http://www.searchdatacenter.com.cn/showcontent_11424.htm

数据中心灾难恢复需要考虑哪些因素？

回忆一下我作为 IT 主管和顾问所积累的数据中心灾难恢复经验，我见到过许多处于灾难恢复标准制定、技术研发、设备部署及改进的企业。灾难恢复策略和基础架构本身就很复杂，对于大型企业来说更是这样。在这个过程中存在许多可变因素：需要确定许多标准和流程，需要对人力资源进行组织，需要对技术进行整合，需要辨别不同应用间的差异并为其排定优先次序。加上内部与灾难相关的一些不确定因素，无论发生何种事件，整个在哪恢复的过程都会变得异常复杂。

对于一些基本的事件做一定的假设并将内外部因素都考虑进去显得很关键。这使人们可以认识到在灾难恢复流程研发过程中对这些小问题进行处理的意义所在。如果不这样做，等待你的只能是严重的后果。

关于这方面我已经多次在“DR 预期差距”的演示中做过阐述，其中讲到了企业的可恢复性设想往往与实际的 IT 技能不符。事实上，如果这些假设因素没有得到明确的界定和处理，你昨日的灾难恢复功臣就有可能变成明日的替罪羊。

当然了，在这些假定因素中，创建灾难恢复的 RTO 和 RPO 等级是最关键的，而在制定灾难恢复规划的过程中还有其它许多因素需要考虑和权衡。以下列出的是一些很实际的规划条目，这些因素对于灾难恢复方案的设计和规划而言很有意义：

员工：在执行灾难恢复计划过程中，IT 员工是否都能参与？他们如何到达备用的灾难恢复站点？是否已为他们准备了短期的住所？在灾难发生后，一部分员工要待在总部，而不是立即就参与到数据中心恢复中去。

基础设施：完成灾难恢复计划需要有哪些通信和交通运输设施的支持？如果飞机不能起飞、手机无法使用或道路受到封堵该怎么办？

位置：要考虑灾备中心与总部的距离因素，以及灾备中心所能承受的灾难等级是多少？看看许多最佳措施的做法，他们的灾备中心距离都很远，为的是避免受到同一灾难的影响——而你的呢？

灾难通报：如何进行灾难通报？由谁来通报？RTO“计时器”何时开启？

灾备站点的运营：灾备站点需要运营多长时间？需要为其提供哪些支持？如果你是在使用第三方的灾备站点，这一点就显得更为重要。

期望性能：在灾难恢复过程中你是否期望所有应用性能都达到较高的标准？可以容忍什么样的性能等级，可以容忍多长时间？

安全：灾难恢复期间的安全要求是否要与灾难发生前保持一致？在许多特殊情况下，你对安全的要求要比平时生产期间更高。

数据保护：灾难恢复站点的数据备份和数据保护设备如何安置？记住，灾难恢复站点的数据每天都要进行备份。

站点保护：你有没有给灾难恢复站点也制定一个灾难恢复规划呢？如果没有，应该立即动手做一个，此外你还应该考虑由谁来对其负责？

规划地点：灾难恢复规划应该放在哪儿？（最好不在你自己的数据中心）。由谁来负责维护？如何与其进行沟通？

显然，为了保证灾难恢复的成功实施，还有许多因素需要考虑和解决，但仍希望本篇技巧能够帮助你走上正轨。

（作者：Bill Peldzus　译者：王霆 来源：TechTarget 中国）

原文标题：数据中心灾难恢复需要考虑哪些因素？
原文链接：http://www.searchdatacenter.com.cn/showcontent_24724.htm

灾难恢复策略之网络带宽和延迟

实现灾难恢复的挑战在于不用冒数据丢失的风险，跨越更长的距离移动不断增长的企业数据。有一些因素会使这个过程进一步复杂化，比如，网络的带宽和延迟。

带宽的一般定义是数据移动的速度(每秒的 bit 数)。延迟则代表与物理网络限制相伴而生的数据传输的延缓与滞后，以及广域网上的通讯行为：TCP/IP 信号交换、传输延迟、丢包和日期及时间戳错误。这些问题一直都是灾难恢复计划需要考虑的重要因素。虚拟化没有以任何形式减少这些因素的影响。

通过使用光纤和暗光纤可以获得更高的带宽，而且使用这些技术的成本也在不断的降低，然而，每天都要复制成百 GB 的新的(或改变了的)数据所带来的成本对大多数企业来说都极为昂贵。如何平衡成本与复制速度之间的矛盾一直都是 CIO 和 CFO 争论的焦点。

一般来说，更高的带宽会减少延迟、让数据在更长的距离上更快的传输。这也减少了同步复制的限制，依赖广域网提供商及其混用的多种广域网传输技术，可以将传统的 30 英里延长到几百英里。

尽管如此，对同步复制的需求还是会限制数据中心和灾难恢复站点之间的实际距离。比如，在地区间或许很容易实现同步复制，但是，要想在大陆之间实现同步复制依然存在很大问题。

“我们已经知道，在 1000 英里的距离上移动数据会有很大的问题。在一些案例中，我们通过使用不同的广域网提供商来解决这个问题，” Moose Logic 的总裁 Scott Gorcester 说。Moose Logic 是一家总部位于华盛顿州巴索市的专业的 IT 服务公司。

当大量数据必须复制或者到灾难恢复站点的距离太长，同步复制无法实现的时候，只要带宽和时间允许，IT 管理员必须依靠异步复制的方法拷贝数据。异步复制会迫使数据传输产生 15-30 分钟或更多的滞后。滞后的时间越长，更多数据丢失的风险就越大，这也就是为什么要求管理员在其灾难恢复计划中，必须考虑到最多允许丢多少数据。

Gorcester 注意到，一个组织对灾难恢复性能的期望值很容易超过其可以采用的技术的实际限制。“我们曾经遇到一些顾客，想跨越半个国家的距离移动有大量变化的数据集，而且，他们要求数据传输滞后的时间不能超过 15 分钟，”他说。“遗憾的是，那是一桩很棘手的事情。”

(作者：STEPHEN J. BIGELOW 译者：王越 来源：TechTarget 中国)

原文链接：http://www.searchvirtual.com.cn/showcontent_30562.htm

灾难恢复策略之重复数据删除功能的用途

重复数据删除在容灾恢复中也扮演了重要的角色。通过删除重复的文件、数据块和字节，可以大幅减少数据节点中需要复制的数据达 50%~80%。这样的话，“变小”的数据站点就可以很快被复制到远程容灾站点。

重复数据删除功能可以直接内嵌到存储子系统中，例如 IBM 的 System Storage TS7650 ProtecTIER Deduplication Appliance。重复数据删除功能也可以通过安装诸如 Symantec NetBackup PureDisk 这样的软件来实现。

最后，通过广域网加速器实现对传输协议和站点间数据交换的优化，使得生产站点和容灾站点间的链路连接更加地高效。例如来自 NetEx 公司的基于软件功能实现的 HyperIP 产品。而且市场上还有很多种可以实现广域网加速功能的产品。这种产品可以加速数据的复制并且有效地拓展同步数据复制功能的实现距离。

存储容量问题

任何的数据容灾恢复解决方案都必须仔细考虑对底层存储硬件系统的需求。例如在同步地把数据从生产站点复制到热备份容灾站点的方案中，数据量会增长一倍，从而使得对存储系统的需求也翻倍。如果我们还采用了额外的异步数据复制方案到冷备份站点，那么甚至可能使存储需求量增加两倍。

“理论上讲，我需要购买更多的存储系统，而且在容灾站点所需要部署的存储系统可能会更加地昂贵，”Gorcester 这么说，“但是我之前并不了解虚拟化技术也会使得容灾站点的存储容量需求增加。”

像重复数据删除和分层存储等技术，就可以减少对存储系统的需求。而且这需要我们跟踪每个存储站点的数据增长情况，以及部署长期的容量规划。

虚拟化并不会直接增加容灾站点对存储的需求，但是会有一些侧面的影响。服务器虚拟化技术中会创建多个不同的虚拟机，每一台虚拟机对应的都是一份或多份虚拟硬盘文件的拷贝。事实上，虚拟机的增长会增加存储容量的需求，而增加的这些数据在容灾任务中更是会翻倍增长。而在另一方面，存储虚拟化技术则可以通过创建虚拟存储池的方式，提高存储自身的利用率，从而减少物理存储的增长。这会对购买额外存储系统的需求产生潜在的影响。

现在最主要的问题就是：对于一个机构而言到底需要多少份数据备份？容灾专家的建议是：这取决于数据的重要性，以及数据保留的需求和客户所采用的数据保护方式。

通常来讲，数据中心会发现他们需要四到五份数据的拷贝：生产数据、磁盘备份数据（例如通过持续数据保护或虚拟磁带库实现的）、复制到远程容灾站点的数据备份、前一次备份的归档数据以及可能还会有一份备份到磁带的数据。

“我们每天都会对所有工作负载的数据做全镜像，”Gorceste 说，因为只有全镜像才能实现对整个系统或虚拟文件的完整备份和恢复。这种方式同时满足了对备份和容灾的需求。

（作者：STEPHEN J. BIGELOW 译者：李哲贤 来源：TechTarget 中国）

原文标题：灾难恢复策略之重复数据删除功能的用途
原文链接：http://www.searchvirtual.com.cn/showcontent_30469.htm

探讨重复数据删除后的灾难恢复

如果你是个存储专业人士，你应该熟悉“保护时间”这个概念。这个时间是指一系列操作所需的时间间隔，也就是从完成备份开始直到备份拷贝到达备份站点能够进行灾难恢复的一切操作。在磁带备份的灾难恢复场景下，这包括进行备份，准备备份站点的磁带拷贝并将它们运到备份站点的时间。

对基于磁盘的灾难恢复来说，这会是进行备份的时间和通过复制将数据转移到备份站点的时间，基于要传输的数据量和可用的带宽，这一时间将会有所变化。对次级磁盘目标进行重复数据删除的最大好处是，它能降低数据量从而允许用较低的带宽进行复制。这使得自动的数据电子化保险库变得更加省时也更便宜。

我们知道了重复数据删除有好处，那么有什么缺点呢？额外的识别并去除重复数据的过程可能会影响开始备份和开始复制之间的某个地方的性能。备份时的重复数据删除（在线，即在数据写入磁盘之前）将会影响备份的性能，而备份之后进行重复数据删除（后处理）将拖延复制。

灾难恢复实现之路

当考虑恢复的时候，数据路径上有两个点需要注意：本地保护点（local protection），生产数据在本地生成备份并可以进行运营恢复的时间；还有就是保护时间（time to protection），它代表拷贝到达远程站点并可以进行灾难恢复的时间。

具有在线重复数据删除功能的系统——比如 Data Domain、HP（StorageWorks D2D 备份系统）、IBM（Diligent）和 NEC 的产品——都鼓吹数据一抵达磁盘就可以立即进行复制的高效，这能保证非常短的保护时间。而后处理方式则有不同的观点，这些厂商，包括 ExaGrid 系统、FalconStor 软件、HP（虚拟带库 Virtual Library System）和 Sepaton 公司，都会指出，如果用全速完成到磁盘的备份，然后在备份窗口之外启动重复数据删除，可以保证备份的服务等级指标（SLAs）。复制的开始时间会有些不同，有些厂商在几分钟之内就开始，而其它厂家会有较大的延迟。

EMC 和 Quantum 横跨在线和后处理两个阵营，因为他们的产品允许管理员来决定什么时候进行重复数据删除。通过提供这种选择，可以为特定的备份组定义不同的策略。由于每种方式都有其适用的地方，这种灵活性就是件很好的事情了。

另一个需要考虑的因素是恢复时间。数据被复制到备份站点之后，从复制的灾备副本恢复数据需要多长时间呢？把数据读出来并重建到应用可以使用的状态有多快呢？有些厂家专为此目的而保留未进行重复数据删除的备份副本。这种方式有利于提供更快的恢复，但需要额外的存储容量来保存它。

这个过程能够加快吗？

对 Symantec 公司 Veritas NetBackup 6.5 的客户来说，Symentec OST（OpenStorage 开放存储）功能会有所帮助。当和支持 OST 的重复数据删除存储系统（Data Domain、FalconStor 和 Quantum 目前通过了认证）一起使用的时候，能够简化创建并管理复制的备份副本、传输备份副本到备份站点以及集中创建基于磁带的长期保留备份的过程。Veritas NetBackup 保留写入 OST 接口磁盘存储设备上的备份相关信息，并对其进行控制。它的“优化重复数据删除”技术能改进在备份站点创建复本的性能。例如，Data Domain——首个具有经认证 OST 接口的厂家——证明在 OST 环境中复制性能提高 75%甚至更多。

通过重复数据删除来优化存储容量给业务带来的益处广受赞誉。然而，重复数据删除还能给灾难恢复带来极高的效率。做重复数据删除的投资决定时，除了基于本地重复数据删除和站内运营恢复来评估产品，调查一下产品离站灾难恢复相关的功能也是个不错的主意。

（作者：Michael Keen　译者：王越 来源：TechTarget 中国）

原文标题：探讨重复数据删除后的灾难恢复
原文链接：http://www.searchstorage.com.cn/showcontent_21087.htm

灾难恢复策略之容灾管理工具软件及效率

存储资源的管理，尤其是在虚拟化数据中心里尤为重要。虚拟化软件极大地淡化了管理员对上层的应用软件及底层硬件系统的关注。这意味着，在您的虚拟数据中心中，您可能无法动态地检测和调整应用程序的负载，或者在硬件发生改变时无法及时获知，这也影响了故障诊断和处理的效率。

“对于追求新技术的虚拟化数据中心而言，首先要确保的是拥有可以有效管理虚拟化环境的工具软件。” Sierra Management Consulting LLC 公司的总裁兼 CEO Allen Zuk 这样说。这是一家坐落于 Parsippany N.J. Zuk 的公司，他们主张更多地基于硬件来实现较高的资源管理效率。

Dorion 在这方面有更进一步的解释，他认为只有仔细地选择一款存储管理工具，才可以实现更高级别的管理效率。“最终，您将接管所有存储上的数据复制任务，并使它们运行于后台进程。”他说，只有存储虚拟化技术才可以实现这些。这项技术避免了人工管理的复杂性，而且加入了管理之外的自动化和系统监控等功能。

这种自动化的实现是需要花费一定预算的。因此那些预算紧张的小公司，可能会发现实现存储虚拟化的优势，即通过自动化容灾进程管理代替手工方式，是非常痛苦的。还有一种方法就是：选择一种合适的容灾恢复托管服务。这种方式可以降低远程容灾中心在费用和后勤管理上支出。

另外的一些小型公司选择在远程站点使用小型 NAS 系统做容灾，因为 NAS 系统对实现卷复制所需的带宽费用要求要低得多，而且这种技术对 WAN 上的数据流不会产生影响。

“我们在本地 NAS 系统上创建并保存镜像数据，”Gorcester 这样说，“然后把这些镜像通过多次操作复制到一台较小的 NAS 系统上，最后再将其安装到异地容灾站点。”

容灾恢复演练及成功率

即使在虚拟化环境中，经常性的容灾演练也是确保灾难发生后可以成功恢复的关键。年度性的容灾演练工作是数据中心的基本安全要求之一。同时，当发生基础架构变迁、安装部署更新、应用升级或改变以及管理人员发生变更的时候，也需要进行容灾演练。

在虚拟数据中心里，允许管理员在不影响生产环境的基础上，利用闲置的服务器实现数据备份。对于在两个热备份站点间部署了负载均衡架构的那些机构而言，容灾演练甚至可以在业务连续的基础上实现。

检验容灾策略的方式有无数种，但是我们需要牢记一些基本方面。首先，要确认需要备份的内容可以在预期的时间内被复制到指定的容灾站点。在初始化复制过程中出现的那

些问题，往往意味着容灾站点的配置，或者是两个站点之间的链接存在问题，或者是远程站点需要部署更多的存储设备。

在确认了虚拟机已经被复制以后，接下来需要确认的是我们可以通过从远程容灾站点（甚至是第三方的测试站点）向主站点复制数据的方式来实现对虚拟机的恢复。在多数情况下，使用一台单独的测试主机，用于接受单独（或成组）的虚拟机并测试它们的可操作性就足够了。在这个过程中发现的问题，可能是由于接受服务器、连通性或开始复制进程时导致的。再一次检查虚拟机复制进程，并确保所有的虚拟机文件（如 VMDK 文件）都已经被完整地复制。

您也需要密切关注恢复时间的问题。每台虚拟机需要在可接受的时间段内实现恢复，即所有的虚拟机必须在特定的时间段内恢复到所指定的服务器上。否则，将会导致无法接受的停机时间和应用恢复的延迟。

改变和适应

我们期待那些已经存在的重复数据删除和广域网优化技术可以有效地改善对数据传输要求较高应用（如容灾恢复业务）的效率。而且，事实上，网络传输的级别也在不断地发展中——尤其是在传统网络上实现更多的存储流量传输方面。

和专用于独立网络技术的传统 FC 方式所不同的是，新的技术，如 iSCSI，把存储局域网络和应用网络连接到同一个网络中。这使得机构所管理的传输方式变得更加多样化起来。FCoE（Fibre Channel over Ethernet）技术的出现将会导致更加多样化的存储和网络传输。这些都使得对网络传输的关注热点集中到网络规划和调优上，通过合理规划使得存储的数据可以在网络上高效地传输给用户。

我们也提到了管理工具的使用，它们在合理的费用消耗下，可以提供增强的自动化管理方式。Zuk 也预测道动态自动管理的加入，将会推动端到端的、服务导向型自动化服务的研发进程。这样的企业自动化管理工具可以基于服务的需求设定条件，从而实现对资源的自动分配和再分配。

（作者：STEPHEN J. BIGELOW　译者：李哲贤 来源：TechTarget 中国）

原文标题：桌面虚拟化：如何为用户提供个性化？
原文链接：http://www.searchvirtual.com.cn/showcontent_30610.htm

使用开源复制工具来降低灾难恢复成本

如今否认经济形势迫使企业减少预算。尽管灾难恢复（DR）人员在极力劝阻对这个领域预算的削减，DR 也无法躲过预算危机。那么对于 DR 站对站数据复制解决方案的创建和维护而言，有没有什么方法或工具可以降低总的成本呢？

首先，服务器虚拟化一次又一次地为各个机构的 DR 节约了时间和金钱。去年，我在 top DR budget wasters 上写了一篇技术性文章，其中分享了一个客户关于虚拟化和灾难恢复的故事。过去的几年，我和很多与次此相关的 IT 组织交谈过，大家的反应是一致的：虚拟化已经为 DR 测试带来了超过 50%的时间和近 50%的人力资源节省。

然而，在这篇文章里，我更愿意将重点放在另一方面——用开源工具进行数据复制及 Linux/Solaris 解决方案的低成本存储。通常来讲，一个企业的 Linux 系统要有将近 2500 个程序包，其中包括数百个有用的工具。然而，还有成千上万可用的相关开源工具可以帮你在更低成本的前提下完成 DR 目标。下面我们讨论一下数据复制领域的两个热门工具：rsync（remote sync 数据镜像备份工具）和分布式复制块设备（DRBD）。

什么是 rsync?

大多数企业的 Linux 系统都包括 rsync，是一个文件级的复制工具，由 Samba 提供维护。去年他们发行了 3.0 版本，增加了递归式扫描功能来提高大文件系统的复制效率。（rsync 必须对所有被复制的文件进行跟踪，运行太多文件会导致内存耗尽，新版本解决了这个问题）。

Linux 和 Solaris 管理员多年来一直使用 rsync 来复制配置文件和非核心系统数据。其最近在扩展访问控制表支持（Xattrs）和递归扫描方面的改进及多年来在生产部署上的应用使自己成为基于 Linux/Solaris 数据中心负载的高级 DR 解决方案。

什么是 DRBD?

分发复制块设备(DRBD)是一个由 Linbit 提供维护的块级开源复制技术。除 Red Hat 企业级 Linux（RHEL）外，其它所有操作系统都支持该技术的运行。然而，其 CentOS 的版本与 RHEL 是二进制兼容的，并且能被 RHEL 使用。

DRBD 通过 TCP/IP 网络在磁盘上写配置。只有主磁盘，或者活动磁盘，可以被文件系统访问。复制盘或从磁盘不能被访问，除非它被升级为主磁盘（在镜像被破坏的时候）。DRBD 可以被配置为同步或异步镜像。在同步模式下，发布写数据的文件系统无法接收到完整的写入，除非本地和远程磁盘已经都被写入了。这样做的结果是，距离和时间的延长限制了同步模式的使用。在长距离复制中异步模式效果最好。然而，如果 TCP/IP 链接的带

宽比写在主磁盘上的数据带宽小，当所有 DRBD 网络缓存都耗尽时主系统性能将受到带宽的限制。

JBODs（简单磁盘捆绑）使存储成本减少

JBOD 阵列比商业存储阵列便宜多了。很多二级或次关键系统可以很好的应用于富含串行高级技术附件（SATA）磁盘的廉价 JBOD 阵列。虽然 SATA 磁盘相比更昂贵的存储磁盘并不能提供相同的速度和带宽,但它们足以满足大多数应用需求,特别是在进行 DR 操作的时候。利用 rsync 和 DRBD 复制技术,可以在低成本前提下将一个高性能的主系统复制成一个更便宜的 JBOD 系统。此类配置前提是，在灾难恢复期间，企业可以降低对服务等级的要求。

灾难恢复成本节约需要面对的风险

上述建议可疑被归结为是一个成本与风险间的交易。通常，预算紧缩的公司认为承担额外的风险来降低成本是可以接受的，特别是对于特定的应用和对公司风险较小的业务流程。除了改变功能系统外，将商业复制工具改为缺乏供应商支持的开源工具也会导致风险。但是，一些 IT 组织自身有能力来降低风险，或者他们可能会发现从一个 Linux 供应商处采购支持服务要比购买商业产品的成本更低，但无论任何地方出现问题都要保持平常心态。

然而，那些涉及核心业务的关键应用不应该面临太大的风险。大多数 IT 组织会花费更大的开支来将风险转移给供应商以获得服务质量，并视自己能够保持一个平常的心态。

（作者：Richard Jones　译者：喻英 来源：TechTarget 中国）

原文标题：使用开源复制工具来降低灾难恢复成本
原文链接：http://www.searchdatacenter.com.cn/showcontent_21432.htm

数据中心灾难恢复需要外包还是自己解决？

在大多数企业中，灾难恢复（DR）计划都有恢复时间目标，在选择灾难恢复站点时一般要求不能是低温场所，因此有选择的余地并不多，目前有三种方式可选：自己动手，丰衣足食；外包给 DR 提供商；与合作伙伴合作。这三种方式都可以工作得很好，但最佳的方式取决于你的需要和每个选择的需求。

我们就以前面的顺序一个一个地介绍，无论你是自己动手，还是找合作伙伴，抑或外包出去，灾难恢复站点的物理位置必须要离生产场所足够远，不能受大规模事件威胁，如飓风。

自己动手搭建 DR 站点

许多大型企业在全球各地建立有多个数据中心，这些企业通常使用现有的数据中心作为 DR 站点，基础设施和 IT 人员都是现成的。许多大型企业正在实施或已经完成了虚拟化，将以前的多个数据中心进行了资源整合，因此可以将遗留下来的设施用作 DR 中心，在另一篇文章“需要多少数据中心用于灾难恢复才足够？两个，三个或更多？”中，我讨论了全球化企业数据中心最理想的数量需要考虑 DR 的目的。

如果你有现成的数据中心设施，一定要考虑下面这些因素：

- 现有数据中心设施满足 DR 站点弹性和可靠性需要吗？
- 现有设施有足够的电力和制冷满足 DR 需要吗？
- 现有的设施距离生产场所足够远吗？能够避免区域性灾难吗？
- 在恢复站点上运行时，你的业务连续性对生产服务级别有要求吗？或者可以降低企业运营的 IT 服务水平吗？

如果这些问题的答案表明现有设施满足你的需要，那么你完全可以自己动手建立自己的 DR 站点。最后要考虑的是虚拟化整合之后现有设施的大小和成本，从多个 IT 组织那里了解到，虚拟化后电力，制冷，空间占用需求至少下降了 10 倍。

外包灾难恢复计划

目前市场上出现了大量的 DR 外包公司，如 IBM、SunGard，许多本地托管和设备代管公司提供 DR 服务，许多 DR 提供商提供增值服务帮助你建立自己的 DR 解决方案，以及帮助你测试。

许多中小型企业利用托管和/或设备代管进行 IT 运营，如果你的组织属于这一类，最好选择 DR 提供商。

如果你打算将你的 DR 解决方案外包，在考察提供商时，必须考虑以下内容：

- 它们是否可以提供你可以联系得到的现有 DR 客户清单？你的外包候选人至少需要提供 5 个成功案例，最好是同时有不同行业的案例和相同行业的案例。
- DR 外包公司应明确地进行报价，服务水平，以及违约惩罚。
- DR 企业是否愿意超额预定？有些 DR 提供商不愿意超额预定，也有的原意，所以得问清楚先。
- DR 外包企业使用虚拟化架构了吗？使用虚拟化进行灾难恢复速度更快，成本更低，因此确认外包企业是否可以提供虚拟化技术，并要求提供虚拟化成功案例，并且要求至少有 2 年的成功虚拟化经验。

在选择 DR 提供商时，你必须检查提供商的成功案例，因为我所接触的许多 IT 组织对很多著名的 DR 提供商都不满。

寻找合作伙伴

我注意到目前两个或更多企业之间合作相互共享 DR 站点的趋势越来越明显，相互合作的企业在对方的数据中心中使用额外的空间用于部署 DR 设施。

在高等教育机构，政府机构和医疗保健提供商之间这种方式变得越来越流行，这样做的直接好处是大家都节约了成本。

在寻找这样的合作伙伴之前，需要考虑下列事宜：

- 共享出来的 DR 设施要工作得很好才行。
- 合作双方必须具有几乎相同的安全和运营管理方式。
- 双方必须签订清晰的 DR 设施共享协议。
- 合作双方可能本身就是竞争关系，需要认真考虑是否能够处理得好这种关系。

最后，如果你的 DR 设施已经部署到合适的位置了，你还应该评估它是否能够满足你业务连续性要求，你可能会发现或许只需要稍作修改就可以改善服务水平，减少成本，或者二者兼得，在今天的经济环境下，要实现成本节约必须对 DR 方案仔细斟酌。

（作者：Richard Jones　译者：黄永兵 来源：TechTarget 中国）

原文标题：数据中心灾难恢复需要外包还是自己解决？
原文链接：http://www.searchdatacenter.com.cn/showcontent_26951.htm

灾难恢复规划工具：是否物有所值？

我曾和一些 IT 企业谈论有关灾难恢复（DR）规划及相关工具的话题，发现 Microsoft Office 仍是最受欢迎的工具。有些公司使用先进的以数据库为中心的 DR 规划工具，却依然会在很多时候用到 Office。因此，我们暂不讨论显而易见的问题：除了办公软件，其它软件怎么样？DR 工具能帮助规划和执行 DR 吗？是否物有所值？

在三种情况下，需要补充工具才能处理 DR 规划。这三种情况为：IT 架构的复杂度、企业规模和培训。我们依次来看一下每种情况。

DR 规划工具和 IT 复杂度

IT 复杂度直接影响 DR 规划流程、归档、测试、升级和 DR 执行的复杂度。许多大公司的 IT 系统彼此相连，形成纷繁复杂、互相依赖的网络，需要商业资产管理软件和自动系统管理软件，才能处理基础架构。不言而喻，如果你的 IT 公司包含一个或多个配置管理数据库（CMDB），你就需要同等水平的 DR 规划和管理工具、以及相关的数据库，才能正确制定和管理 DR 预案。

一些具有复杂 IT 的公司发现 CMDB 工具非常值得投资，同理，他们也会发现 DR 规划和维护工具物有所值。市场中大多数 DR 规划工具使用 MS SQL server 等办公软件。许多 DR 工具能从广为流行的 CMDB 系统管理工具中获得 IT 系统配置信息。

我也曾与一些公司有过交流，他们借助系统管理工具 CMDB 中可用的开发接口，开发自己的 DR 规划工具。这样，他们就可以利用现有的系统管理工具存储 DR 预案、配置信息和流程信息。这种集成方法能给用户带来好处：每天的 IT 变更管理流程能很容易地集成到 DR 规划的升级过程中，这样，DR 规划就能始终与 IT 基础架构保持同步。

企业规模

乍一看，可能会以为企业规模就是 IT 复杂度。许多情况下并没有错，但是并不绝对。一些小企业的业务可能以电子商务为主，因此 IT 基础架构非常复杂，需要自动管理工具。相反，我与一些大型的生产企业有过接触，他们的 IT 系统非常简单，无需复杂的自动系统管理工具。但是，如果公司同时拥有 DR 规划和业务连续性规划（BCP），但又无需先进的 IT 系统管理工具，最好能让 DR 规划支持总体 BCP。DR 隶属于业务连续性，用于实现 IT 灾难恢复，保证业务服务水平保持在正常水平。

业务连续性规划师建议的 DR 工具

我最近曾在一篇文章中讨论 BCP 咨询师的价值。如果你的公司决定提从 BCP 咨询师的专业意见，那么有很多 BCP 服务供应商能够提供 DR 工具，以及相关的培训课程。这种情

况下，最好是利用咨询师提供的工具，因为咨询师在培训过程中已经非常了解公司的情形。应该注意的是：DR 工具如果不能与现有系统集成，就会得不偿失。目前，一些 DR 规划工具无法与流行的系统管理架构直接集成，但是许多工具拥有开放接口，能与 Microsoft Office 集成，因而，咨询师在你的系统管理 CMDB 中集成常规功能。

灾难恢复规划工具

市场中存在许多 DR 规划工具。每种工具关注的角度不同，可能是 DR 规划、管理或执行。例如，一些工具重在帮你制定通知、危机和事故管理预案，而不仅仅是基本的 DR 预案。另一些则重在与 IT 服务目录和基于信息技术架构库（ITIL）的流程实现集成。选购的工具应该能够与企业的 ITIL 流程原则相互作用，这一点关乎 DR 工具能否取得成功。

具有事故管理功能的 DR 规划工具可以部署在第三方托管设施中，也可以部署在你的生产和 DR 设置中。大多数 DR 工具供应商在提供事故管理软件包的同时，也提供托管版本；DR 工具的托管版本在发生灾难时具有重要作用，因为当数据中心无法操作或访问时，你就需要访问 DR 工具。

DR 工具的最基本意义在于满足下列标准：

你的 IT 架构或业务连续性规划非常复杂，需要 DR 工具的帮助。

你选择的 DR 工具能够补充现有的系统管理工具、ITIL 流程和程序，并且相互作用。

DR 工具支持员工培训。

DR 工具不仅有助于规划，还有助于规划执行和事故管理。

（作者：Richard Jones 译者：周姝嫣 来源：TechTarget 中国）

原文标题：灾难恢复规划工具：是否物有所值？
原文链接：http://www.searchdatacenter.com.cn/showcontent_16480.htm

灾难恢复需要多少个数据中心？

适当的灾难恢复需要多少个数据中心？我经常在工作中遇到这样的问题。如今的经济对 IT 数据中心运营造成了两方面的压力：拥有许多数据中心的话，压力来自整合增加的效率和更低的成本。拥有一个或两个数据中心的话，注意全部集中在保证防灾准备上，尤其是在过去十年中由于自然和人为灾难带来的损坏。

关于“需要多少个数据中心”这个问题的答案决不简单。我会说“根据情况看”。因此根据什么情况呢？灾难恢复所需的数据中心数量取决于你必须做的两个最主要的决策。

第一个决策适合所有 IT 组织，取决于整个业务完成的业务影响分析（BIA）。BIA 会指示业务必须满足的恢复时间和关键目标，以便从灾难中恢复。一个常犯的人为错误是组织里的业务单位寻求激进的恢复目标，以避免如果发生灾难对他们日常工作带来的不便。这种做法不是避免了不便，而是确保组织的生存。

第二个决策适合那些本质上是占统治地位的电子商务的 IT 组织，他们必须确保他们的 Web 服务器对他们所有本地用户可用。客户端响应时间驱动了数据中心数量的需求和布局。当然不是所有 IT 组织都有这个需求，我谈论过一些有这个需求的组织，他们与 Google 相似，给他们所有的用户快速提供内容。

建立恢复时间目标

我们来看看这两个决策的更多细节。恢复目标将决定需要多余的数据中心还是在灾难恢复设备里保留一个数据中心。通常，在制造业部门的组织发现他们不需要恢复数据中心，因为关键数据已经被复制。在这些情况下，他们选择一个异地恢复提供商，万一数据中心损坏了可以恢复数据。在这些情况下，恢复时间目标通常大于 72 小时。不过，对于那些拥有 BIA 以说明更多精确的恢复时间和关键目标的 IT 组织来说，就对决定需要多少个数据中心和它们之间相隔多远有帮助了。

恢复关键目标决定设备位置

对于精确恢复需要，我已经看到两个常规架构。它们由对关键系统的恢复点目标区别。那些有 zero 恢复关键目标的（一般是金融机构），两个相隔 100 千米的可用数据中心用以同步复制是必须的。然而，在有的区域相隔 100 千米是不安全的，不能抵御诸如飓风和台风这样的自然灾害。在这些情况下，恢复目标需要定义第二级别的恢复时间和点。最常见的解决方案是把数据分配给第三方同步复制的数据中心，这些数据中心相距两公里以上，以避开飓风的影响。

一些已经决定他们的服务区域（他们的本地用户）的组织由于局部混乱也很混乱，他们能依赖包含在租用设备里的归档带提供的额外时间进行恢复。这些数据中心有更多的时

间，因为他们的客户端也从灾难的影响中恢复。对于那些没有 zero 恢复点目标的组织，两个可用的数据中心同时复制，并相隔很远。一般说来这意味着它们相隔 500 千米以上。

占统治地位的电子商务着重于业务，添加了确保他们的数据和服务满足用户的需求。这要求给定区域的数据中心消除由距离和带宽要求造成的延迟。一般来说，这个问题的解决方案是在每个主要区域需要两个冗余的数据中心。北美、欧洲-中东-非洲以及亚洲-太平洋分别有一对数据中心，总共有三对。小型的缓存数据中心一般布置在主要区域里面，在这里，由于流量和带宽的限制，延迟变成了一个问题。

恢复时间目标和服务访问目标是关键

决定灾难恢复所需的数据中心的底线包括了解恢复目标和服务访问目标。这将说明所需的数据中心数量。

决定拥有恢复工具与协同定位恢复工具的区别就是钱的问题。通常，IT 组织通过并购或收购拥有多个可用的数据中心。平衡现有的财产比协同定位花费要少些。然而，现有设备的年龄或设备的缺乏可能更多的倾向协同定位。行业里的一般趋势是已经转向短期的恢复目标，这意味着恢复中心的保留已被可用的灾难恢复中心所代替。

（作者：S Richard Jones　译者：唐琼瑶 来源：TechTarget 中国）

原文标题：灾难恢复需要多少个数据中心？
原文链接：http://www.searchdatacenter.com.cn/showcontent_13953.htm

您的灾难恢复规划过期了吗？

在本文中，TechTarget 中国的特约专家 Richard Jones 将举例说明配置管理过程的灾难恢复规划、定期测试和恢复时间目标追踪。

灾难恢复规划很容易过期，从而导致它不能发挥很好的作用。有些公司经常会处于不稳定状态——状况好的时候尽力保持快速的增长，状况差的时期则削减开支。如果您的灾难恢复规划仅仅是一个事后的考虑问题，那么将很难跟得上形势。

我的一位同事曾经给我讲过他个人多年以前的一段经历，当时他在一家大型备份存储技术供应公司工作。有一次，一位客户的邮件服务器出现故障（硬件故障，磁盘丢失）。这位客户建立了一台新的服务器并从磁带备份恢复系统。但是，系统始终无法恢复正常，提示电子邮件数据库（email database）损坏。然后，他们一遍又一遍地尝试恢复，结果仍然不行。随着时间的过去，他们开始着急慌乱了，恢复时间目标和业务也受到严重的影响。这样的情形把他们快要急疯了，于是他们去找备份恢复供应商提供技术支持。经过一系列的标准化故障处理步骤后，他们决定派一名专家去帮助该客户公司解决恢复问题。客户非常肯定地认为，备份已经被损坏了，或者是在恢复过程中恢复数据被损坏了。在完成故障检修之后，技术支持组很肯定磁带中的备份数据没问题。

于是，我的这位同事被派去解决这个问题。当时，故障已经出现两天了，公司上下简直都要疯掉了。他确定磁带数据没有问题，而且恢复数据与磁带上的数据一致。显然，结论是备份过程损坏了磁盘上的数据。不过，我这位同事进一步对问题进行了深入分析。简单地说，新服务器安装的操作系统和邮件服务器补丁比原来的服务器运行的操作系统和补丁版本要新。当新服务器尝试装载电子邮件数据库时，没有预期这样一个老的数据库结构，所以就报错。然后，我这位同事仅仅是卸掉两个补丁，邮件服务器就恢复成功了，没有任何障碍或报错。

这个故事说明，许多 IT 公司在制定灾难恢复规划时忽视了一个问题。那就是它们只是制定了规划，却没有对规划进行更新。显而易见，例子中遇到电子邮件灾难的这位客户如果严格遵从最佳做法，保持更新灾难恢复规划，使之与操作系统和补丁详细版本保持一致，就不会遇到这样的灾难了。

这个问题不仅仅是那些只有一台邮件服务器和直连磁盘的小型企业会遇到，大型企业也会有类似问题。我曾经与一家五百强的企业打过交道，从它们那里我得知了另外一个故事。这家公司完成了灾难恢复规划的所有过程，制定 BIA（业务影响分析）、RTO（恢复时间目标），并且一丝不苟地执行和测试。到 2002 年为止，它们所进行的一系列灾难恢复测试证明它们的解决方案是可行的，完全满足 RTO。然后，业务也以惊人的速度持续增长。由于灾难恢复规划工作正常，测试工作逐渐就被怠慢下来，精力都转移到了一些更紧急的业务需求上。不过，与遇到邮件灾难的朋友们不一样，由于这家公司有良好的配置管理制度，所以它们一直严格地保持着配置文档记录。

在 2006 年，由于管理层的人事变动，公司来了一位新的 CIO。查看了公司的灾难恢复规划之后，这位新 CIO 询问了最后一次系统测试是什么时候。相关人员支支唔唔的回答说：“上次全面测试是在 2002 年年底，但之后系统状况一直都很好。”结果，这位 CIO 还是要求进行了测试。尽管测试没问题，但远远不能满足 RTO 要求。从 2002 年到 2006 年，数据增长幅度太大，即使是现有的最快的磁带系统也无法满足公司的 RTO 要求。它们的解决方案是采用异步复制将数据拷贝到 SAN 存储和 400 英里之外的其它系统。这家公司执行了共置的（co-located）灾难恢复热站（hot DR site）并采用磁带作为存档介质。

这些故事都可以让我们学到一些关于灾难恢复的经验和教训。

将灾难恢复融入配置管理过程

很多公司都只是把灾难恢复看作是一个事后考虑，甚至是一个独立的预算项。如果您的公司属于这一类型，请您赶快改变这种想法。灾难恢复是一个完整的过程，而且绝不是一个事后考虑和反思。如果只是把它作为一个事后考虑，在面临压力时势必会忽视灾难恢复的一些最佳做法。如果您为灾难恢复单独列出一个预算线，请马上把它消掉。灾难恢复预算应该包含在核心项目成本中，而绝不是事后预算。

定期测试灾难恢复规划

配置管理变更事件应该包括灾难恢复测试，它是任何更新测试或系统配置变更测试的一部分。配置变更需要进行人员的培训，它也应该包含灾难恢复培训在内。而且，灾难恢复培训应该一年更新一次，并作为人力资源培训要求。

观察 RTO 趋势

系统的灾难恢复测试应该一年至少进行一次。根据每次测试情况追踪 RTO 趋势是检验当前的方法和技术是否能跟得上增长和变化形式的最佳方法。不仅数据增长会延长恢复时间或高可用性故障恢复时间，日益独立化或模块化的系统也会使业务系统的 RTO 延长。

（作者：Richard Jones 译者：涂凡才 来源：TechTarget 中国）

原文标题：您的灾难恢复规划过期了吗？
原文链接：http://www.searchdatacenter.com.cn/showcontent_14714.htm