VMware 灾难恢复计划&实施手册

VMware 灾难恢复计划&实施手册

之前我们做过《虚拟化灾难恢复手册》技术手册，主要介绍了虚拟灾难恢复的优缺点与挑战、P2V 相关的备份策略等等。本期的《VMware 灾难恢复计划&实施手册》具体讲解在 VMware 虚拟化环境中如何制定 VMware 灾难恢复计划以及如何开展具体实施过程。

VMware 灾难恢复计划

如何开始创建 VMware 灾难恢复计划？构建灾难恢复站点时应该考虑哪些因素？小型环境需要制定 VMware 灾难恢复计划吗？相信这些都是你迫切需要弄清楚的问题。

- 五问五答：创建 VMware 灾难恢复计划
- 中小型企业指南：快速构建虚拟化灾难恢复方案
- 制定切实可行的虚拟灾难恢复计划

VMware 灾难恢复实施

构建 VMware 虚拟化灾难恢复站点都有哪些需求？如何具体实施？VDI 架构的一大好处是易备份虚拟桌面，在发生故障时可迁移到新硬件。那为什么说 VHD 备份是 VDI 灾难恢复过程的关键？

- 构建远程 VMware 灾难恢复站点：需要做的准备
- 构建远程 VMware 灾难恢复站点：具体实施
- VMware 灾难恢复：Site Recovery Manager 之外的选择
- VDI 灾难恢复过程：VHD 备份是关键
- 虚拟桌面如何提升虚拟化灾难恢复策略

五问五答：创建 VMware 灾难恢复计划

一个坚实的 VMware 灾难恢复计划对应用发生中断后如何进行故障切换并恢复工作负载进行来了描述，对保护组织的数据和业务操作是至关重要的。通过允许虚拟机在物理服务器之间进行无缝迁移，虚拟化提供了革命性的灾难恢复计划。现在，有众多的 VMware 灾难恢复工具能够帮助虚拟机更快地上线恢复运行，但是如果 IT 管理者没有设置实际的业务目标并进行严谨的规划和彻底的测试，那么这些工具都是无效的。

让我们一起来了解一下在使用灾难恢复管理器（SRM）以及第三方灾难恢复工具创建 VMware 灾难恢复计划时经常被问及的一些问题。

如何开始创建 VMware 灾难恢复计划？

创建 VMware 灾难恢复计划的第一步也是最重要的一步就是明确组织的灾难恢复目标。众多的业务决策实际上要比构建灾难恢复基础设施的技术成分更加复杂。确定哪些虚拟机是组织中最为重要的是设置恢复点目标（RPO）的第一步，这将决定虚拟机在灾难之后启动的顺序。分析数据需要备份到灾难恢复站点的频率将决定组织的恢复时间点目标（RTO）。

构建灾难恢复站点时应该考虑哪些因素？

远程 VMware 灾难恢复站点为数据提供保护并确保了在灾难发生的情况下业务将会继续运行，但是创建灾难恢复计划可能富有挑战。做好准备整理现有基础设施的清单，明确定义 RPO 和 RTO，然后基于可用的预算做出艰难的决定。没有恰当的计划，你可能会浪费大量的时间与金钱同时将组织置于非常脆弱的境地。

小型环境需要制定 VMware 灾难恢复计划吗？

为小型环境创建灾难恢复计划是很困难的。但是即使是资源、员工有限的组织也应该花一些时间考虑灾难恢复。但是，如果你的站点只运行了少量的虚拟机，那么也不必使用专业工具为全面的 VMware 灾难恢复计划提供支持。在这种情况下，坚实的备份计划能够允许你恢复那些你的确需要的虚拟机。

站点恢复管理器如何为创建 VMware 灾难恢复计划提供帮助？

在灾难发生时 SRM 帮助管理员规划并恢复 VMware 基础设施。SRM 能够减少恢复的时间，优先恢复关键业务的工作负载，甚至能够对灾难恢复进行测试。但是，

尽管 SRM 能够帮助改进灾难恢复计划，在虚拟化环境中应用 SRM 可能有些困难而且价格不菲。

除了站点恢复管理器之外，还有其他选择吗？

SRM 是众多组织所使用的一款强大的工具，但是有些 IT 主管可能会发现相对于他们的 VMware 灾难恢复计划来说，SRM 过于复杂而且价格不菲。在组织没有专职的 VMware 专家的虚拟化环境中，不选择站点恢复管理器而是考虑第三方的灾难恢复工具是有道理的。最为流行的工具包括了 Quest 软件公司的 vReplicator，Veeam 公司的备份与恢复工具以及 Zerto 公司的 BC/DR for Enterprises 工具。

vSphere Replication 将如何简化 VMware 灾难恢复计划？

VMware vSphere Replication 避免了对价格昂贵的灾难恢复存储的需求，使中小企业更加轻松地构建高效的灾难恢复计划。使用 vSphere Replication，中小企业能够将虚拟机从一种存储类型拷贝至另一个，而且这与存储厂商和协议无关。这一特性消除了灾难恢复所存在的障碍而且为组织在二级灾难恢复站点使用价格更低的存储硬件创造了条件。尽管具有上述优势，但是使用 vSphere Replication 的的确确提出了一些挑战并且带来了额外的成本。

中小型企业指南：快速构建虚拟化灾难恢复方案

虚拟化灾难恢复方案对于保护中小型企业的大部分关键数据是一个很好的解决方案。简单的备份过程并不能实现这样的功能。

当灾难彻底摧毁数据中心时，备份起到的作用非常有限。更为重要的是，在没有服务器和应用程序的情况下，数据变得不再有价值。这时，虚拟化灾难恢复方案就可以发挥很大的作用。

按照备份方式选择，使用虚拟磁盘能够更加轻易的将数据复制到备份站点。除此之外，许多基于硬盘的备份工具提供了数据的离址备份功能。这些都促成了将可行的虚拟化灾难恢复策略加入到你的备份计划当中。

虚拟化灾难恢复计划的关键因素

包含整合备份、复制和灾难恢复的解决方案能够很好的满足中小型企业的需求和开支预算。下面是开始时需要准备的东西：

基于硬盘的备份工具

寻找一个支持离场复制的产品。合适的工具还能够省去备份 windows 的工作。将不再需要每晚的备份操作，取而代之的是一个持续、稳定的虚拟硬盘区块转移计划。你需要找到一个能够在虚拟机和主机上占用很少资源就能够完成这些的恰当工具。

替代站点

以前，灾难恢复计划最大的开销之一就是维护一个完全一样的热备站点，以便在发生灾难时立即实现故障转移。但是中小型企业灾难的恢复时间是用天来计算，而不是分或秒。如果你的组织以天来计算恢复时间，复制最关键的虚拟机到云存储服务商或者出租场地的替代磁盘中是最好（最为划算的）的。

网络连接

复制过程需要网络连接。对于大部分中小企业来说，离场复制需要足够带宽的 Internet 网络连接。主地址和备份站点间的距离各不相同，但是现在致力于磁盘块操作的中小型企业备份解决方案能够最大程度地保证需要网络带宽。准确地估计网络带宽是一门艺术，但是备份工具会提供一些最为精确的预测值。

磁盘和服务器

在备份站点中，需要服务器和磁盘来存储虚拟磁盘的数据。根据你的需求，可以在这里节省一部分开支。如果你不想在灾难之后从备份站点重启虚拟机，就可以不必使用高速磁盘。

作为一种替代方案，你可以和硬件供应商协商灾难发生时的服务安排。这种方法允许你在每天的复制操作中使用低速磁盘，只在灾难恢复操作时，使用额外的资源。这一点和云服务商形成鲜明对照，当灾难发生时，他们能几乎立刻启动虚拟机，并且只是向你收取你所使用的虚拟机的那部分费用。

实施虚拟化灾难恢复方案

事实上当所有的物理设备后准备好后，灾难恢复方案的实施是一个非常简单的过程。借助于正确的备份方案，开启复制功能只需要在管理员控制台下点击几下鼠标那么容易。

开始，在备份工具中输入备份站点的网络地址，然后注意查看网络带宽的占用情况。需要注意的是，首次复制过程需要花费一些时间，所以当虚拟磁盘初始化转移完毕之后，你会看到之后需要的时间会减少很多。

还有需要了解的是每次灾难并不都是由自然灾害引起的。龙卷风、飓风、地震和其他自然灾害会被很自然地想起，但是这些灾害极少出现。更为常见的灾难包括数据库的毁坏，设备中断或者系统补丁引起的操作系统问题。这些都和典型的自然灾害没有关系，但是它们都会严重地影响用户使用。

其他需要的备份特性包含内置的故障转移和故障恢复功能。好的工具能够开启备份虚拟机，快速恢复虚拟机为用户提供服务。借助于这项功能，当故障发生时，你可以轻易地进行故障转移操作。当问题被解决之后，可以先将复制的数据移动到原始服务器上（或者新的替换位置），之后实施故障转移恢复操作。

实施总结

曾经只能应用于大型知名 IT 企业中的虚拟化灾难恢复，现在在中小型企业中，实施过程变得异常简单。虚拟化绝对是一个游戏的变革者，但是要知道你不能将关注点只集中于虚拟机上，一些备份解决方案同样可以备份和复制物理服务器上的内容。

加令人振奋的是，备份厂商已经研究支持这些特性的产品许多年了。虚拟化备份产品已经成熟，并且有很多选择方案。可争辩的、最困难的就是选择哪种备份方案用于灾难恢复最为恰当。

制定切实可行的虚拟灾难恢复计划

许多组织编写灾难恢复计划只是为了满足审计的需要。当灾难来临时，计划往往被放在一旁，恢复成为一次临时的演练。但是新的虚拟化技术已经使落实灾难恢复变计划得更加灵活、有效，而且切实可行。

最近几年，业务及管理的要求一直在推动着全面的灾难恢复计划的制订。不幸的是，这一趋势却导致了制定的灾难恢复计划只符合审计的需要，并不符合实际工作的要求。从本质上讲，灾难恢复计划仅仅变成了你需要检查的另一个盒子而已。

事实是，多年以来一直有很多因素在困扰着灾难恢复的效能，这些因素导致了灾难恢复计划的创建与执行之间的脱节。一个主要的问题就是需要将工作负载从一台物理服务器迁移至另一台物理服务器。对服务器 A 上的 Windows Server 2008 虚拟机进行的备份仅仅适用于硬件完全相同的服务器 B。这意味着每次购买一台服务器后，你还需要另外再购买一台相同的服务器用于灾难恢复，这并不划算。

与灾难恢复相关的工作通常涉及在灾难恢复服务器上手动重新安装操作系统和应用程序，然后从备份恢复应用数据到这台服务器上。这一过程很耗费时间而且容易出错，效率也很低。但是不必担心，因为有一种更好的方法：虚拟灾难恢复计划。

虚拟灾难恢复计划

虚拟化已经打破了连接操作系统与特定硬件的链条。操作系统经过了封装而且灵活性非常高，这消除了一个高效、切实可行的灾难恢复计划所面临的最大的障碍之一。

当取代了在 72 小时内还没有完成测试的物理灾难恢复计划后，我亲眼看到了虚拟灾难恢复计划与普通的灾难恢复计划的不同。在使用虚拟灾难恢复计划后，在 24 小时以内就执行完成并进行了验证。而且虚拟灾难恢复计划在价格方面也更胜一筹。

在那次经历之后，我痴迷于虚拟灾难恢复计划的诸多优势之中。即使生产工作负载没有以虚拟机的形式运行，你也可以使用各种 P2V 转换工具创建物理服务器的虚拟副本。不管你的生产工作负载有多少被虚拟化了，P2V 工具已经全面打开了虚拟灾难恢复计划的大门。

渡过数据恢复难关

即使是使用高效的虚拟灾难恢复计划，在进行数据恢复时很多项目还是会卡壳。磁带速度太慢，而替换存储可能很复杂，成本也很高。对于要求低 RTO 和 RPO 的灾难恢复计划来说，存储复制最为关键。

然而，制约因素却是众多的存储复制产品需要存储阵列彼此匹配，要么就是复制设备价格昂贵。如果你还要求低 RTO 和 RPO 的话，那么你可能没有任何选择。但是如果你可以接受较高的 RPO 的话，那么有一些新的复制产品能够弥合进行数据恢复时所存在的差距。

VMware Site Recovery Manager 5 以及 Zerto Virtual Replication 都能够在两个 VMware 基础设施之间进行存储复制，并不需要存储阵列或复制设备之间的匹配。事实上，这些产品能够复制本地磁盘的数据，我们甚至不必使用磁盘阵列。

VMware Site Recovery Manager 5 以及 Zerto Virtual Replication 能提供的 RPO 在 15 分钟之内，大多数组织可能能够接受这一时间范围。但是一些金融机构要求数据是同步或者近似于同步进行复制的。仍然有基于软件的复制产品以合理的价格提供了更高级别的简单性与灵活性。

正是由于采用了虚拟化，灾难恢复计划才比以往更加成熟。而且有上述工具可以使用，便没有理由不采用能够进行轻松、准确测试的综合性虚拟灾难恢复计划了。

构建远程 VMware 灾难恢复站点：需要做的准备

虽然虚拟化解决方案在灾难恢复方面具有诸多优势，但将所有服务器整合于一个 vSphere 平台，并且如果不维护一个远程灾难恢复站点，仍然会给你的系统带来隐患。

每个企业都需要灾难恢复计划，但是研究显示，只有不到 50%的企业有相关计划。随着虚拟化使工作负载在不同物理服务器间更加容易地迁移，在第二数据中心需要灾难恢复计划，无论是物理环境还是虚拟环境都是必要的。

幸运的是，虚拟化灾难恢复正变得越来越易于操作。下面我们看看构建 VMware 虚拟化灾难恢复站点的需求。

为什么虚拟化灾难恢复比以往更加容易？

服务器采用以下措施来简化灾难恢复：

服务器的操作系统和应用不再和特定的物理服务器硬件绑定。

虚拟机具有可迁移性，你可以在任何 vSphere 服务器上运行它们。

依靠虚拟化特性，你可以完成虚拟机的克隆、快照和移动。

VMware 高可用性和分布式资源调度这些高级特性能够帮助机构尽快地从灾难中恢复，借助于资源分配避免系统缓慢和中断。

从公司开始实施虚拟化以来，已经有众多特性让灾难恢复变得更加容易。比如，vStorage APIs for Data Protection 中的 CBT(change block tracking)特性，允许备份灾难恢复工具轻易地找出虚拟机磁盘文件中发生过改变的块，之后这些发生改变的块通过广域网复制到远程 VMware 灾难恢复站点。除此之外，基于软件的灾难恢复解决方案，取代了硬件工具，高可用性使得所有规模的公司都能够更轻易地负担复制虚拟机的开销。

规划远程 VMware 灾难恢复站点

在构建一个远程 VMware 灾难恢复站点之前，有许多问题需要考虑。毕竟，恰当的灾难恢复计划能够避免浪费大量的资金在本不需要的设备和设计上。

让我们来看在进行远程 VMware 灾难恢复站点规划时需要考虑的方面：

清查现有的基础设施，在彻底理清一个主要数据中心的资产之前，你不能对它开始复制。RVTools 和 Veeaminc.Reporter（免费版）是两个不错的用于 vSphere 基础设施免费工具。

了解应用程序和它们的依存关系。当你对应用程序如何工作和它们的依存关系有初步的了解之后，你将会知道哪些应用程序需要抵抗灾难的能力。如果你的灾难恢复计划只能够在一部分服务器上实现故障转移，那么那些依靠多个服务器的应用程序可能会受到影响。要考虑到（主站点和备份站点）存储和网络架构之间任何潜在的差异，确保程序即使在不同的环境下，也能够按照预期实现把故障转移到备份站点。

不要忘记你的客户。因为你运行维护所有的服务器和应用程序，并不意味着终端用户就能够访问他们。怎样替换他们的桌面和应用程序？他们怎样进行远程访问？

应用程序区分优先级处理。如果你的远程 VMware 灾难恢复站点不能提供和生产环境数据中心同样的容量，处理的优先级是什么？哪些应用程序需要优先进行恢复？

建立恢复点目标（PRO）和恢复时间目标(PTO)

你的公司需要在多长时间内将虚拟机（包括它运行的应用程序）恢复上线，24 小时的 PTO 意味着业务能够在缺少虚拟机 24 小时的情况下继续工作。

你能够接受多少数据的丢失？如果数据每小时复制到第二数据中心，当灾难发生时，有可能最多丢失之间 59 分 59 秒的数据。如果这样是可接受的，不会严重地影响业务，那你的 PTO 可以设定为一个小时。

设定你的预算。决定你的公司愿意投入多少在灾难恢复站点上（你可能永远都不会使用它）。如果公司询问你的花费，你可能必须创建一个需求资源的列表来计算和压缩它。

至此，我们介绍完了在构建远程 VMware 灾难恢复站点之前需要做的准备工作。后续文章里，我们将继续讲解怎样具体实现构建远程 VMware 灾难恢复站点。

构建远程 VMware 灾难恢复站点：具体实施

上篇文章我们介绍了在构建远程 VMware 灾难恢复站点之前需要进行的规划，以及需要建立恢复点目标（PRO）和恢复时间目标(PTO)。这篇文章紧接着讲述构建远程 VMware 灾难恢复站点的具体实施过程。

构建远程 VMware 灾难恢复站点

如果已经明确了灾难恢复的需求和预算，你可以设定一个计划。记住，每一个公司的灾难站点都不尽相同。

举个例子，让我们思考一个具有十个关键虚拟机的数据中心。这些虚拟机有四个小时的 RTO 和一个小时的 PRO。下面是如何构建远程 VMware 灾难恢复站点的建议：

选取数据中心地址

远程恢复站点的选址在哪？它应该离主数据中心多远？是否需要到主站点的高速宽带连接？是否符合预算？我认为，一条可承担到主数据中心的高速连接是选择灾难恢复中心需要考虑的关键的几个因素之一。如果将第二数据中心定址在半个地球外的地方，可以减小单个事件影响两个地点的危险性，但是如果你不能保持数据同步，那毫无意义。大多数公司需要在两个数据中心间找到一个实现物理隔离的中间点，但是距离不会远到影响数据传输速度和在合理时间内到达两个地点。

获取、安装和准备硬件

借助于虚拟机的可迁移性，你不再需要在主和从数据中心部署相同硬件设备。我不建议在灾难恢复站点侥幸尝试集成比更高的硬件，除非你能接受应用程序效率的降低。不要侥幸尝试老旧硬件，记住，你将试图在这些主机上安置尽可能多的虚拟机。我推荐为灾难恢复服务器使用牢靠的 KVM-over-ip 系统，因为如果有任何问题，你不会想要亲自到远程 VMware 灾难恢复中心的。

安装和配置 vSphere

在灾难恢复主机上安装 ESXi 不会花费很长时间（如果你的主机数量超过 25 台，你需要自动部署）。如果可以接受，我建议在第二数据中心使用和主数据中心相同的激活码和 vCenter 服务器，你将会想要周期性的测试复制的虚拟机和故障转移过程。

选择工具

现在，许多工具包含虚拟机备份的复制功能，这些工具可能是将虚拟机转移到远程 VMware 灾难恢复站点的可行方案。这些产品的例子包括：Veeam Backup & Replication、PHD Virtual Technologies 的 Virtual Backup 和 AppAssure Software 的 Backup。或者，你也许偏好嵌入在存储区域网络或者在 ESXi 主机上直接加载的灾难恢复复制工具（比如 VMware Site Recovery Manager and Zerto Virtual Replication），这些功能能够提供更低的 RTO 和 RPO。

实施复制

初始化数据的复制将是最大规模的数据传输，随后的对发生改变的块进行复制将会小很多，但是复制数据的大小会依据应用程序中数据量改变的大小而定。复制的数据的大小也会依据复制的间隔（由 RPO 决定）而变化。

主数据中心中的硬件可能会和灾难恢复中心的有所不同，但是如果它们都运行 vSphere，你仍然可以使用同样的工具管理两个数据中心，比如 vSphere Client。

考虑灾难恢复中的云

云是最新的远程灾难恢复站点的可选项之一。具体来说，在新的灾难恢复管理软件（SRM）5 的 vSphere Relication 中，灾难恢复是作为一项服务来实现的。借助这些类型的服务，你可以不必购买 SRM 或者远程站点的硬件。你甚至不用为远程 VMware 灾难恢复站点租赁机架空间。不管现在你是否对云备份服务感兴趣，你应该确保你的备份软件在将来能够支持基于云的备份。Hosting.com 是一家能够提供这种服务的公司。

构建远程 VMware 灾难恢复站点并不容易，你的预算和 RPO/RTO 将决定这个项目的需求范围。幸运的是，所有的灾难恢复复制方法都有适用版，你可以尝试他们是否能够满足你的需求。

VMware 灾难恢复：Site Recovery Manager 之外的选择

最近有机会在一个 VMware 的座谈会上与一些真正的虚拟化工作者讨论 VMware 的灾难恢复工具。我发现，最受关注的是复制技术——而且许多销售商都开始转向第三方方案，而不是销售 VMware 的 Site Recovery Manager。

在讨论过程中，大多数人表示，VMware 的站点恢复管理器（SRM）对于他们的管理员和环境来说太过复杂。而且对于有限的预算有些昂贵。VMware 正在加大向小型企业销售这些产品的力度，但是在很多销售商来说，维护 SRM 产品配置过于复杂。

他们说，在许多小型环境中，不可能有一个专门的 VMware 管理员，大多数情况下只有一个统管全部 IT 环境的管理员，同时他也负责灾备。此外，对于一般的 IT 管理员来说，VMware 的灾备产品并不容易掌握。所以大家的共识是，其它厂商可以为 VMware 环境的管理提供更简单的灾难恢复工具。

此外，大多数的 VMware 环境的灾难恢复都应包含某种类型的复制机制。文件拷贝、磁带备份已经成为过去，具有即时甚至实时复制技术的先进并且不再昂贵的产品正成为主流。并且提供比以往任何时候都更完整的灾难恢复计划。

经过讨论，我将那些可能适合你的 VMware 灾难恢复工具和复制技术列举如下：

VMware DR 的第三方产品选项：

讨论中主要涉及了三个复制工具：Quest 软件公司的 vReplicator（现在已经集成到 vRanger 产品中）、Veeam Backup and Replication 以及这个领域的新军——Zerto 的 BC/DR for Enterprises。

Zerto Virtual Replication：与会者说， Quest 和 Veeam 结合了其复制软件与备份工具，相比于二者，Zerto 带来了一个完整的灾难恢复工具。我个人并没有使用过 Zerto，但许多管理员喜欢这样的组合产品，因为除了灾难恢复它还满足了备份需求。Zerto 的客户说，他们选择 Zetro 的产品作为其 VMware 灾难恢复工具是因为 Zetro 为他们提供了更多的灵活性和计划性方面的选择。

Quest 的 vRanger 和 vReplicator：自 Quest 的 vRanger 诞生以来，我就一直在使用它。在 5.3 版本中，Quest 添加了一个关键的模块，就是能够将虚拟机复制到多个目的地的复制机制。这听起来非常的振奋。对于许多管理员来说，虚拟机被

复制到多个站点有助于在分支机构建立第二个“冷”灾备站点。例如，中央数据中心的备份服务器还可以充当灾难恢复主机的角色。

Veeam Backup and Replication：Veeam 的灾难恢复工具包含了各种各样的功能，并在第 6 版中各方面都有显著的增强，包括对微软 Hyper-V 的支持以及多个数据移动器（也称为“代理服务器”）的采用。Veeam 的最新版本似乎与新版的 vRanger 不谋而合，都包括许多类似功能的变化。看来，这些灾难恢复工具主要是围绕是否能为客户提供更加丰富的功能而展开竞争。

不用说，参与讨论的每个人都有所收获，主要是关于 VMware 的灾难恢复以及如何才能使灾难恢复计划更完善。如果你不想选择 Site Recovery Manager，市场上也有很多其它的灾难恢复工具供你选择。

VDI 灾难恢复过程：VHD 备份是关键

VDI 架构的一大好处是易备份虚拟桌面，在发生故障时可迁移到新硬件。VDI 灾难恢复过程都始于 VDI 备份，但有一些不同的组件需要你存储与保护。

备份虚拟硬盘

备份虚拟桌面架构始于虚拟硬盘 VHD。如果你有实时更新的备份能轻松检索的话，那么 VDI 灾难恢复过程就会很平滑。首先，询问自己：实际的虚拟硬盘是否存储在 SAN 上或者存储在本地主机服务器上？

如果使用 SAN，可将 VHD 作为常规备份过程的一部分，或者使用快照。不过，快照与备份通常只有在 VHD 最后一次启动的时候有效，这意味着目前的或最近的信息可能会丢失。并且如果你让终端用户个性化他们的虚拟桌面，会使得 VDI 灾难恢复过程更加困难。

有些 VHD 只存储静态信息，如操作系统与应用，但对于个性化虚拟桌面，终端用户能在 VHD 上存储数据，修改设置、安装应用与存储书签等等。对于一个稳固的 VDI 灾难恢复计划来说，需要经常备份 VHD，还可能需要支持实时快照，以便在使用 VHD 的时候随时进行备份。

如果 VHD 存储在端点，可使用同步技术在数据中心存储副本，或者终端用户可使用镜像备份产品本地存储 VHD。那么 VDI 灾难恢复计划就降级到你所有准备的层级，那么架构中就有可用的 VDI 备份资源和能容忍的宕机时间。

保护主机服务器

备份 VHD 和与之相关的 VDI 设置只是 VDI 灾难恢复计划的一部分。管理员也需要考虑虚拟桌面运行的地点。对于大型 VDI，实际的数据进程发生在数据中心中的一台服务器上，终点只是作为一个终端而已，同步主机服务器上虚拟机的屏幕更新与用户输入活动。

也就是说 VDI 灾难恢复策略的一部分是保护主机服务器，这也就保护了宿主在服务器上的虚拟机。所以，你可使用故障恢复技术，在灾难后，虚拟会话能自动改为数据中心的另一台服务器上。不过，这需要额外的硬件和昂贵的规划才能实现。

此外，故障恢复通常列于业务连续性规划之下。如果有用于业务连续性的故障恢复功能，就不需要对 VDI 灾难恢复进行额外的支持。而且，很多 VDI 备份与管理产品本来就包括故障恢复功能，这样你就能自定义具体的实施。

虚拟桌面如何提升虚拟化灾难恢复策略

面对令人眼花缭乱的虚拟化灾难恢复工具，你可能会很快忽略灾难恢复的最终目标，那就是保持用户连接。对于一个稳固的灾难恢复策略来说，使用虚拟桌面可能是保持连通性的最佳选择。

当灾难侵袭了虚拟基础设施，数据必须被复制到另一个站点，而且受影响的服务器工作负载必须被无缝迁移。足够的连通性以及网络带宽是虚拟化灾难恢复策略真正有效的关键。虚拟桌面可以为复制及连通性提供帮助。

只有 VPN 还不够

因为对安全隐患有着很好的理解，VPN 技术备受推崇，经常被用户用来连接环境，即使是在灾难发生之后。但是针对灾难场景而专门配置的虚拟桌面可能是一个更好的选择。这是因为只要能够连接互联网，就可以在任何地方使用虚拟桌面。

更棒的是，不用部署完整虚拟桌面基础设施，你就可以在灾难恢复策略中使用虚拟桌面。在生产环境中，通常需要全冗余的 VDI 部署、管理并维护虚拟桌面，还要加上简化桌面部署的其他技术，用户到桌面协调，远程访问以及用户状态管理。

通常 VDI 还需要实现桌面的个性化。然而，个性化程度最小时虚拟桌面才有意义，这在灾难恢复策略中意义重大。

尽管个性化在日常工作中是必须的，但是当灾难发生时一切就全变了。灾难发生时，大多数公司发现他们自己只关注确保核心业务可用。在紧密结合，易于理解的桌面之上交付业务应用是保持所有企业重要形象的一种方式。

空闲的架构与受宠的桌面

虚拟桌面能够支持公司的虚拟化灾难恢复，其中一种方式是通过分布式虚拟化，或者是在最终用户的设备上交付只读的虚拟桌面。

分布式虚拟化需要 hypervisor 能够展现在每个用户的桌面上，虚拟机也需要分布。所有这些活动在给用户交付正确的数据时需要做出一些努力，但是结果是以更低的成本实现与集中式 VDI 相同的凝聚力。

对于虚拟化灾难恢复来说，分布式方式允许用户继续使用原有的硬件以及操作系统。同时，虚拟桌面提供了在灾难期间所需要的连接以及安全的门户服务。使用

单独的虚拟桌面对生产环境中所使用的桌面进行灾难恢复同样能够减少培训工作和恢复的时间。

不论你如何发展虚拟桌面灾难恢复策略，一定要确保不要忽略或忘记最终用户的体验。对许多用户来说，只需要使用一个虚拟桌面并被告知“这就是你所有的应用及数据”将更加简单—立刻行动吧。