虚拟化灾难恢复手册

虚拟化灾难恢复手册

虚拟化改变了公司对灾难恢复（DR）的规划和执行方式，它提供的高度灵活性和整合度使得灾难恢复的过程具备更高的效率和性价比。本期 TT 虚拟化技术手册主要介绍虚拟灾难恢复的优缺点与挑战、P2V 相关的备份策略、以及用 Xen 和 Hyper-V 构建 DR 系统相关信息。

了解虚拟化灾难恢复

毫无疑问，虚拟化为数据中心带来了好处，但管理便捷性不包含其中。有三大虚拟化挑战摆在许多管理员面前：虚拟灾难恢复、虚拟机备份与数据保护，以及虚拟化安全。虚拟灾难恢复有哪些优缺点？

- **虚拟化灾难恢复八问八答**
- **三大虚拟化挑战：灾难恢复、备份与安全**

虚拟化灾难恢复策略

某天，你的同事说：“告诉大家一个坏消息，我们 Exchange 服务器的容量已经达到 97%，我收到了系统的警告信息。”这时候该怎么办？灾难恢复。但其关键又是什么呢？

- **数据容量规划策略如何有助于灾难恢复？**
- **虚拟化灾难恢复方案关键：带宽和测试**

虚拟化灾难恢复方案

许多 IT 厂商都有专门的虚拟化灾难恢复解决方案，我们主要看看以下几种方案。

- 如何通过微软 Hyper-V 进行灾难恢复规划
- 技巧：使用开源 Xen 部署灾难恢复策略
- 使用 P2V 迁移进行虚拟化灾难恢复
- 基于主机备份的虚拟环境灾难恢复

虚拟化灾难恢复八问八答

虚拟化改变了公司对灾难恢复（DR）的规划和执行方式，它提供的高度灵活性和整合度使得灾难恢复的过程具备更高的效率和性价比。

虚拟化技术使得多个虚机可以运行在几台物理机上，不再依赖于硬件条件。当原始数据中心发生故障时，可以把工作负载迁移到容灾站点的其它机器上，而且无需过多关注相关的硬件平台。

以下的快问快答涉及了虚拟灾难恢复的优缺点、如何规划 P2V 相关的备份策略、以及用 VMware 和 Hyper-V 构建 DR 系统相关信息。

虚拟化对灾难恢复和数据保护策略的影响？

在规划虚拟化数据保护策略时，采用可以支持虚拟化的备份软件、重复数据删除和其它的工具很重要。虽然共享存储可以让虚拟机方便地迁移到其它服务器，但是为 DR 所作的准备工作还是必需的。确保定期向备份站点拷贝虚机，还要牢记一点：位于共享存储上的虚机通过快照进行恢复，要远比基于本地磁盘或磁带备份的恢复快得多。

通过整合服务器是如何增强灾难恢复的？

通过把多台服务器整合为单个的虚机改善了灾难恢复操作过程。借助存储于容灾站点的快照可以快速地恢复数据和整个虚拟机。其中的关键点在于虚拟机磁盘文件中包含了整个操作系统环境和容灾站点重建所需的配置文件。通过单个文件来重建工作负载意味我们可以在几个小时内完成，而不是几天。

虚拟 DR 和物理 DR 之间的区别是什么？

最主要的区别在于：虚拟 DR 关注点是虚拟机的保护而不再是物理服务器。相比物理 DR 需要基于本地客户端进行备份，虚拟机可以通过三种方式：基于 agent、镜像或者是 server-less 备份。通过复制数据，负载可以方便地实现在不同虚机之间的迁移和快速恢复，避免了物理服务器恢复时漫长的 OS 和应用重建过程。

虚拟灾难恢复有哪些缺点？

虚拟化的优点在 DR 领域可能成为其缺点。虚拟架构天生的复杂性会导致定位问题相关的物理组件变得更加困难。另外整合也是虚拟化的主要优势之一，但是这也同时意味着一个物理服务器故障的发生会对其所支持的所有虚机产生影响。请考虑使用虚拟机灾难恢复的正反两方理由。

能否借助虚拟灾难恢复技术保护物理服务器？

如果某台物理机不适合虚拟化也无需担心，可以通过 P2V 技术实现虚拟的灾难恢复过程。P2V 备份指的是可以对您不希望迁移到虚拟化平台的物理机创建虚拟的备份，这有点类似执行了虚拟化的第一步以后就不再继续了。P2V 软件可以把运行于物理机上的软件、数据和配置转化为单个的磁盘文件，这样就可以用于 DR 中的异地保存了。

应对管理程序单点故障的最佳办法是什么？

定期执行虚拟机备份，因为一个单点故障会导致该服务器上所有虚机失效。例如，微软就要求在开始 Hyper-V 安装前必须首先执行硬件 DEP（data-execution prevention）操作，这样可以提高恢复速度。另外分离 Hyper-V 主机和虚拟机所在的网络也可以改善安全性，请记住一点：某个管理程序的单点故障会影响到所有的虚拟化平台上。

在微软 Hyper-V 平台下，如何创建包含主站点和备份站点在内的虚拟灾难恢复计划，而且不会耗尽所有资源？

Windows Failover Clustering 可以支持多站点的灾难恢复部署。首先，确保容灾站点的存储设备可以承载主站点的所有虚拟机负载。另外，站点间的网络架构环境也很重要。Hyper-V 集群需要双向复制网络来支持重建过程可以顺利进行。还有一点需要考虑的是您需要的 Hyper-V 容灾级别以及部署所需的费用。

如何学习 VMware 环境相关的灾难恢复策略？

VMware 公司及其合作伙伴提供了很多关于这方面的在线资源，从备份和复制软件到自动化灾难恢复无所不包。还有指南和播客提供了关于 VMware 平台企业级业务连续性和虚拟恢复计划等内容。VMware SRM、Double-Take Software Inc.的复制软件以及 EMC Corp.的 RecoverPoint 可以实现虚拟的灾难恢复计划。您还可以通过发起 VMware 灾难恢复评估调查来学习如何成功部署以及哪些方面可以进行改进。

（来源：TechTarget 中国）

三大虚拟化挑战：灾难恢复、备份与安全

毫无疑问，虚拟化为数据中心带来了好处，但管理便捷性不包含其中。有三大虚拟化挑战摆在许多管理员面前：虚拟灾难恢复、虚拟机备份与数据保护，以及虚拟化安全。

虚拟化抽象层从底层硬件分离应用，所以比起传统未虚拟环境需要更高级别的系统规划与管理。幸好，有方法克服这些虚拟化难题，更好控制环境。

虚拟灾难恢复

每个组织必须拥有虚拟灾难恢复计划预防突发事件，虽然灾难的类型与范围取决于公司的位置有所不同。

虚拟化技术本身并不是灾难恢复解决方案，但相对传统的非虚拟环境，虚拟化为灾难恢复带来了更多的选择。出于我们的目的，虚拟灾难恢复主要包括数据到外部地点的移动。

谈及虚拟灾难恢复，正确的规划是主要的虚拟化挑战之一。

管理员需要谨慎考虑数据在 LAN 或跨 WAN 如何移动数据到远程地点。虚拟灾难恢复的这个组成部分通常包括对连通性和带宽的详细评估。

在 LAN 架构中也包括更改，即从 NAS 或 SAN 对数据的优化。经常测试很重要，这能确保数据能恢复到主要的数据中心，或从远程站点（如 DR 站点）直接可用。因此，广泛的测试是虚拟灾难恢复计划的重要构成部分。

虚拟机备份与数据保护

数据保护在大多数据中心处于优先权位置，但这只是虚拟化挑战的另一方面。它能支持单个文件的实时恢复，也能在业务连续性方面发挥重要作用，能遵守法规遵从的要求。

在这里，管理员的最大问题在于如何部署适用于软件与硬件的备份工具，使得虚拟数据备份与虚拟机备份更方便。“人们假定（备份）与在物理环境一样，”Evolve Technologies LLC 公司的 CEO Dave Sobel 说，“多数备份软件期望能访问物理硬件。但在虚拟环境不是如此。”

对于虚拟机备份，管理员通常使用快照工具和持续的数据复制来捕获虚拟机状态存到 SAN，然后使用复制工具复制数据到站外存储。

涉及到虚拟环境中的数据保护与虚拟机备份，恢复也体现出一些虚拟化挑战。从虚拟机快照里来的数据颗粒恢复如果缺少合适的软件工具，就会出现问题。并不是所有备份软件都能从虚拟机里提供颗粒恢复，这迫使管理员首先恢复虚拟机，可能恢复到实验室服务器，然后提取所需的文件。至少，虚拟化能促进先前备份与恢复过程的改变。

虚拟化安全问题

虚拟化安全的最大问题在于熟知任务，如日常扫描和打补丁应该及时执行。例如，如果你有 500 个系统，对于管理员来说，验证这 500 个系统都运行的是最新的应用和操作系统很困难。

由于虚拟化安全呈现的抽象状态经常让任务管理变得混淆。管理员很容易丢失对主机操作系统与虚拟机正确更新的追踪，每个工作负载的转移让情况更加复杂，会丢失工作负载的位置。忘记打补丁或者缺乏扫描会让虚拟机或主机易受攻击。

虽然有工具能让每天的虚拟化安全任务自动化，缺乏使用经验却能让好工具失去意义。因此，专家强调精细化管理的重要性。

(来源：TechTarget 中国)

原文标题：三大虚拟化挑战：灾难恢复、备份与安全

原文链接：http://www.searchvirtual.com.cn/showcontent_45323.htm

数据容量规划策略如何有助于灾难恢复？

想想看下述场景是否在你的 IT 部门出现过？

系统管理员 Joe 把他的头探进办公室说，“告诉大家一个坏消息，我们 Exchange 服务器的容量已经达到 97%，我收到了系统的警告信息。”

如果发生这种情况，那就说明过去所做的容量规划工作失败了。此时不用再做无谓的努力了，即已经处在失败的情形了。极有可能的情况就是申请更多原来根本没有预算的费用。在这样的一个经济时代，可能永远无法知道这样糟糕的状态到底会是什么情况。

虽然说时光不能倒转，但是仍然可以改变未来。如下是一个推荐的方法，可以用来开发容量规划策略以帮助用户摆脱这样的噩梦，并且类似情况防止再次发生：

- 第一阶段：合适的时间解决合适的问题
- 第二阶段：短期执行
- 第三阶段：长期规划

第一阶段：合适的时间解决合适的问题

通常我们看这个世界都会有一定的视野局限性。首先提出一个问题，再解决这个特定的问题，然后再向前发展。

遗憾的是，如果无法打开视野的话，处理一个这样的问题往往就是忽略一个瓶颈问题的同时暴露另外一个问题。很多容量管理问题都是非常复杂，也会有若干种解决方案。在这些场景中，容量管理就不再是一个问题了。这是我的亲身体会得到的……

几年前，有一个客户让我每个月输出一份数据库性能报告。在这项工作持续几个月以后，他发现性能有所下降，这就迫使他给予过多地关注，并且他也丝毫不隐瞒对这种情况的关心。他下意识地反映就是表示对数据库性能的关注。

实地演习就开始了，并且逐一开始解决，从更换服务器到升级内存都考虑过。最终的调查结果表明，问题不在于数据库变得慢了，而是报告的输出频率不够，导致的结果就是很小的性能波动都会给整个报告带来非正常影响。我们通过提高报告输出频度来解决“容量”问题。

底线：回顾所出现的问题，标识出所有的因素，然后再开始着手使用合理的解决发难解决问题。

第二阶段：短期执行

在标识出问题原因之后，就可以开始规划紧急救援。在文章开头我提出的那个 Exchange 危机中，我们最终使用 Microsoft EXBPA 工具分析 Exchange 服务器，并且迅速查明有几个用户的收件箱太大。

底线：分析这些事实，弄清楚短期规划的优势所在以及这些规划如何可以辅助摆脱危机模式。

第三阶段：长期规划

通常情况都是我们完成短期执行阶段后就回到日常工作中，并且很快就忘记并没有真正的解决这个问题。无可非议，我们把 Exchange 的利用率从容量的 97%降低到了 85%，但这只是一个短期解决方案。

在这个案例中，我们需要长期战略。例如邮箱规模的限制、归档离职员工的数据、对邮件服务器的定期升级（依据企业自身的规定）以及报告容量度量的系统以防止再次超过 90%的占用率。

底线：除非长期规划得到很好的实施，否则最终仍然会回到最初的问题。

还需要注意的是：除了上述这些方法，还有很多工具也可以辅助完成容量规划工作——但具体的工具和方法取决于具体情况。微软提供了几种工具，如 EXBPA 和 Microsoft 系统中心。但是即使同样的工具就算可以帮助用户摆脱麻烦，但通常也会使用户无法摆脱危机。

（作者：Brian Madden 译者：张冀川 来源：TechTarget 中国）

原文标题：数据容量规划策略如何有助于灾难恢复？
原文链接：http://www.searchvirtual.com.cn/showcontent_31708.htm

虚拟化灾难恢复方案关键：带宽和测试

虚拟化为 CIO 们提供了灾难恢复方案设计的灵活和弹性。当然，有些基础原则是必须遵守的，正如全球咨询公司 Virtualization Practice LLC 公司的首席执行官 Edward Haletky 所言：“你必须在主站点和热备站点之间进行同样的虚拟化工作。”

通常而言，热备站点一般位于主站点的数百英里以外，以防主备站点同时遭遇地震或其他自然灾害。此外，专家认为 CIO 还需要应对一些其他事宜：比如确保有足够的带宽来进行故障恢复和对虚拟灾难恢复环境进行日常例行的测试。

带宽瓶颈

Jon Nam 是位于纽约的 Macy’s 百货集团（MMG）的技术总监，他认为“对于虚拟化方案最关键的是带宽”。Macy’s 百货将纽约和辛辛那提的两个主要数据中心之间实施灾难恢复方案，两个站点互为热备。Nam 认为：“带宽事关重大，因为一旦实施了虚拟化，将会导致巨大的数据传输量。”

Ray Lucchesi 是 Silverton Consulting Inc.公司的总裁，他认为根据如今的工作负载，带宽是一个相当严重的阻碍，如果说 32GBps 的带宽对于一个应用来说可能是足够的，那么当有很多应用需要被复制时，CIO 就应该考虑采用那些压缩或重复数据删除文件的方案以减少不必要的重复数据，从而降低数据传输对带宽的要求。

根据 IT 咨询公司 Server and StorageIO Group 创始人和高级咨询师 Greg Schulz 的看法，不是所有的数据都能进行重复数据删除。“有些情况下你不得不拥有重复的数据，重复数据删除技术是针对文本信息的，”Schulz 表示：“视频、音频和播客采访资料通常不能进行有效的重复数据删除。”压缩技术由于其 2:1 的压缩率无法和重复数据删除技术（通常达到 10:1 的压缩率）相比，但是压缩适合于视频和音频文件，因而至少可以保证这些数据能够被备份。

一些企业将其系统备份到云服务提供商处，这样可以不必构建内部的灾难恢复方案，但是 MMG 的 Nam 认为这同样需要充足的带宽：“我们从 2 到 3 个 ISP 处获取

带宽以进行备份和故障恢复。对于 Macy's 百货 7x24 小时的海外运营支持，带宽是个大问题：如何选定一天中的时间点进行这种大数据量传输的备份工作？”

测试虚拟灾难恢复方案

在必须保持 24 小时运转的环境中进行备份是很大的挑战，因为需要找到合适的时机来进行关键性测试：在云中或者热备站点上进行灾难恢复方案的验证。Lucchesi 说：“如果你拿到了设备，当然会想对虚拟化的灾难恢复方案进行验证。我知道有个用户每周做一次测试，而绝大部分用户是大概每季度进行一次。”

Visualization Practice 部门的 Haletky 认为在虚拟化环境中进行灾难恢复测试是有相当难度的：“大多数人无法对热备站点进行直接简单的操控，但是在备份复制机制上，必须进行测试，因为对于维持应用的正常运行来说，你所作的事情至关重要。”

一些新软件的出现使得测试自动化的程度大为提高。Veeam Software Corp 公司位于俄亥俄州的哥伦布市，是 Vmware 公司的备份软件提供商，其新版的备份和复制产品中包含了一个叫 SureBackup 的功能特性。位于加利福利亚州 Cupertino 的赛门铁克公司针对微软的 SQL 和 Exchange 提供专门的复制软件，Vizioncore 是 Quest Software 旗下的一家公司，专门针对小企业提供复制方案。

但是，MMG 的 Nam 认为灾难恢复方案可能只是在理论上能够完美地工作，在现实中经常会有我们无法测试到的额外系统负载 – 比如设计会议和产品发布等。

“你可以为 20 个用户进行测试，然后扩展到同类型的 100 个乃至 1000 个用户规模，”Nam 说，“但是以我的经验而言，进行负载预测的软件很难做到准确无误”。Nam 认为这样的瓶颈是非常难于定位的，如同大海捞针一样。

毫无疑问 CIO 们不情愿去推动这种测试 – 但是又无法回避它。

(来源：TechTarget 中国)

原文标题：虚拟化灾难恢复方案关键：带宽和测试
原文链接：http://www.searchcio.com.cn/showcontent_41624.htm

如何通过微软 Hyper-V 进行灾难恢复规划

任何一个参与过灾难恢复训练的人对从无到有重建一个基础设施要经历的痛苦都很熟悉。重装及修复应用程序服务器，让支助性业务重现生机以及数据损坏或者丢失的可能性，一点点的细微差别都可能导致失败。

由于虚拟化可以让您使用已经拥有的系统——在生产中运行并且正常工作的系统，因此消除了建立一个新生产系统的不确定性。

尽管 VMware 的灾难恢复工具工作得相当好，但如果您部署了 Hyper-V，并希望在灾难恢复计划中使用微软的虚拟机？

这也是可能的，如果您采取合适的步骤去实施行动计划。

了解您的灾难恢复方法

灾难恢复计划的第一步是搞清楚您的环境需求。是否您的组织有一个很短的恢复点目标（Recovery Point Objective RPO）——您的数据需要恢复到的恢复点——或者是否您上次的备份能满足 RPO 的要求？

另外，您的恢复时间目标（Recovery Time Objective RTO） ——重新上线所花费的时间 ——会影响到您对基础设备和专门软件的需求。最有可能的是，您已经将您的应用程序“分层次”为多个恢复类，例如，第一层次为处理重要任务的服务器，可有可无的则为之下的第三层、第四层。

Hyper-V 可以在所有的这些场景中得到支持，但这些场景里面的每一个以及它们的花销都是非常不同的。

非关键服务器和冷站（后备站）

让我们从最简单的服务器开始——那些被认为不重要的或者有很长 RPO 或 RTO 的服务器。同时也包含一个基于冷站场景的计划，在该场景中，您必须从头开始重建服务器和网络，并会依赖于冷站点恢复位置上的备份。

Hyper-V 服务器可以通过一个主机服务器备份或者 VM 备份来进行恢复。恢复 VM 备份，除了主机被恢复后，所有的虚拟硬盘(VHD)以及 VM 设置都会恢复到您之前备份时的样子之外，和正常的机器恢复很类似。所有的 VM 都必须使用集成服务(Integration Services)，以便可以访问卷影拷贝服务(Volume Shadow Copy Service VSS)，并使虚拟硬盘以一个一致的状态来进行恢复。特定的应用程序，如微软 Exchange，因为可能会导致数据库不一致，而不支持这种类型的备份。您可能需要使用可靠的恢复方法来处理这些应用程序。（请注意，即使是在恢复主机，您也需要重新配置您的网络，所以有良好的文件是很必要的）

您的灾难恢复计划需要有一套用于转移备份主机或者 VM 的有效脚本。确定如何去进行恢复，并在主机启动前确定其存放的位置是很重要的。做完之后才去决定只会导致混乱和恢复的失败。

关键服务器和积极的恢复目标

对于必须开启，而且要保持开启状态的应用程序，在多个地方，转为集群或者故障转移负载平衡，是对要跨地域复制存储的一个解决办法。在存储区域网络（SAN）间复制是为了进行异地存储，这种异地存储可能会成为一个完整的远程数据中心。当灾难发生时，异地存储会用于主机的恢复。

通过使用 Hyper-V 虚拟机，可以不像标准的物理服务器，使被复制后的存储区域网络中可以包含虚拟硬盘。这样就可以进行故障转移。简单地将复制后的存储区域网络上线，并以很小的数据损失，将其中的虚拟硬盘加到主机配置中。再提醒一下，操作必须要小心，因为这会让某些应用程序处于一个不稳定的状态，并可能会需要进行真正的恢复或者用别的恢复方法来进行处理。

在 Hyper-V R2 中，可以通过 GeoClusters 使用集群共享卷(Cluster Shared Volumes CSV)。这让您可以建立一个 Hyper-V 集群并让其横跨多个位置。虽然这样做的好处是可以进行自动化的故障转移，其缺点是太复杂并且需要特定的硬件。换句话说，您需要用一个服务器和存储区域网络设备匹配的温备份站点(warm site)来做故障转移。这个技术的关键是存储是跨站点复制的。可是再次提醒，微软没有为这个存储问题提供解决方案。幸运的是，SteelEye Technology、EMC 以及其它厂商的产品解决了这个问题。

未来的云选项

微软也许会作为支持无站灾难恢复形式代表的 Windows Azure，很可能是即将可用的另外一个选择之一。

虽然现在已经可以将虚拟硬盘移到 Azure 云里，其它的一些问题，例如私有网络和恢复时间仍在发展中。在未来，尽管您可能不能对整个基础设施进行复制，但时间会证明，Windows Azure 对像网站和 SQL Server 数据库这样的数据中心的特定设备是有价值的。

总的来说，尽管微软 Hyper-V 的灾难恢复解决方案还没有达到 VMware 的级别，但不要忘了，在 VMware 的恢复解决方案中也有相当多的脚本。灾难恢复——即使是一个低成本的计划——可以在少量的测试和对您需求很好理解的基础上开发出来。但前提是，要熟悉您可以有哪些选择，因为知道如何管理现有的 Hyper-V 环境，并基于 RTO 和 RPO 目标做出正确的规划对成功的恢复是至关重要的。

（来源：TechTarget 中国）

原文标题：如何通过微软 Hyper-V 进行灾难恢复规划
原文链接：http://www.searchsv.com.cn/showcontent_33373.htm

技巧：使用开源 Xen 部署灾难恢复策略

在使用 VMware vSphere 或 Citrix XenServer 这样的企业级虚拟化平台时，灾难恢复策略的执行是非常简单的。但是如果您运行了开源 Xen hypervisor，情况会复杂得多。

企业级平台的默认管理工具中已经包含了完整的备份和灾难恢复方案。而开源 Xen 平台下就需要自己来组合所需工具。开源方案缺少自动备份工具，管理员需要手动完成关键部分的备份。

为保障在灾难发生后可以快速重建虚拟架构，对于开源 Xen 平台有两个可以借鉴的操作实践：备份虚拟机配置文件和后端磁盘存储。通过 Linux 命令行可以协助过程的执行和故障诊断。

备份后端磁盘存储

对于灾备策略而言，备份后端磁盘存储是一个不错的开始，通常都是基于 SAN 存储进行的。

后端存储有两种不同的形式：磁盘镜像文件或裸设备。我们不需要对所有的这些虚拟机及虚拟设备做保护，只要在整个后端磁盘阵列上完成备份就可以了。但是您需要确保镜像文件是静态的，换句话说就是要先通过快照技术冻结磁盘状态，然后再对快照做备份。

通过基于 SAN 的快照技术可以创建快照。如果您把逻辑卷作为后端磁盘存储，可以使用如 Logical Volume Manager 这样的开源快照软件。只要后端存储没有被破坏，就可以在灾难发生后通过它来启动故障虚拟机。

备份配置文件

开源 Xen 平台另一个最佳实践就是：备份虚拟机配置文件。只需拷贝这个文件就可以很好地改善灾备策略。保存好拷贝的文件，在发生灾难后可以借助它们来恢复。

灾难发生后，我们需要尽快登录到受影响的虚拟机。如果磁盘文件和配置文件都没有被破坏，只需把它们拷贝出来，在新主机或容灾站点上就可以进行重建。如果配置文件跟后端存储的位置相关联，也可以对访问连接进行重新设置。

灾难恢复中的障碍

不过，开源 Xen 平台中依然会存在一些影响灾难恢复策略成功实施的因素。例如，如果配置文件丢失，我们就需要重建该文件。

Virt-manager 工具可以通过导入一个现有的虚拟机来重建配置文件。导入虚拟机的过程类似于创建一个新的 VM。区别之处在于不需要启动安装，只打开虚拟机本身就可以了。Virt-manager 还允许客户定制包括希望使用的虚拟磁盘等硬件配置信息。

当磁盘文件被破坏时恢复过程要复杂得多。这种情况下，虽然灾难恢复策略会很复杂，但通过 Linux 命令行还是可以恢复文件的。挂载磁盘文件然后把所有相关内容都拷贝到新的临时地址。在拷贝了所需信息之后，再从头开始创建虚拟机。

恢复配置文件

首先，运行 losetup-a 建立 loop 设备和希望访问的镜像文件之间的连接（-a 代表命令中涉及的参数）。这个命令是必须的，因为在 Linux 中我们无法挂载文件，只能挂载设备。该命令显示了当前所分配的所有 loop 设备。

在多数情况下，现在还看不到 loop 设备，通过/dev/loop0 来指定需要把镜像文件关联到的 loop 设备。例如，假设镜像文件的名称是 /var/lib/xen/images/vm1/disk0，使用如下的命令来创建挂载镜像文件用的 loop 文件：

```
losetup /dev/loop0 /var/lib/xen/images/vm1/disk0
```

如果您已经使用了一些 loop 设备，那么确保为新设备分配了不同的名称，例如/dev/loop1。（和其它 Linux 设备相同，命名排列是连续的。）

接下来，再运行 losetup-a，会发现 loop 设备创建完成并已经跟镜像文件关联。然后通过如下包含 loop 设备名称的命令来分析镜像文件中已经存在的分区：

```
fdisk -l /dev/loop0
```

该命令列举出文件中所包含的所有分区及其大小等相关信息。基于这些，您可以猜测根文件系统所在分区。在开始访问该文件系统前，要先确认相关的设备文件已经创建。如果您已经安装了 multipath-tools 工具包，如下命令可用于完成该任务：

```
kpartx -a /dev/loop0
```

由于镜像文件使用了 loop0 设备，所以新的设备文件将命名为 /dev/mapper/loop0p1，/dev/mapper/loop0p2 依此类推。然后借助这些文件，可以完成虚拟操作系统中文件系统的挂载。无论使用的是哪种 OS，都可以从 Linux 主机挂载虚拟分区。

现在您完全可以访问文件，而且所有的重要数据都被拷贝到了安全的地点。最后一步，通过如下命令清除所有临时设备文件：

```
umount /mnt
kpartx -d /dev/loop0
losetup -d /dev/loop0
```

使用开源 Xen 系统进行灾难恢复的最佳实践完全不同于企业级平台。数据中心通常在较小规模应用中使用 Xen，因此多数情况下，开源 Xen 平台灾难恢复策略中可能遇到的种种限制都可以解决。只要您备份了虚拟机配置文件和后端磁盘存储，该灾难恢复策略就可以帮助我们克服各种可能遭遇的意外。

（来源：TechTarget 中国）

原文标题：技巧：使用开源 Xen 部署灾难恢复策略
原文链接：http://www.searchvirtual.com.cn/showcontent_43740.htm

使用 P2V 迁移进行虚拟化灾难恢复

P2V 转换将物理服务器转换成虚拟机，但 P2V 也能在灾难恢复策略里发挥作用。

一些物理服务器不便转换成虚拟机，许多架构都保留了一些物理服务器，因为如果进行虚拟将消耗许多资源。

因此，当发生灾难后，如何恢复这些服务器？恢复虚拟机相当容易，因为其文件整合到单个虚拟磁盘文件里，很容易复制文件到另外一个地点。但物理服务器就杯具了，但你可以使用 P2V 转换来发展虚拟化灾难恢复策略。

使用 P2V 的灾难恢复

P2V 迁移不仅是转换物理机成虚拟机。你可以在物理服务器上运行 P2V 转换加强虚拟化灾难恢复策略。不是在完成 P2V 迁移后就打开虚拟复制，而是保持物理实例如常工作。然后你拥有一个物理计算机文件很好整合在虚拟磁盘里的虚拟副本，可轻松重新复制到 DR 站点。

如果在起初的站点经历了灾难，启动虚拟副本即可。而不是以前需要的“使用操作系统、层级数据启动”。

显然，开始由于性能和其他原因没有虚拟这个系统。但在虚拟化灾难恢复情形下，在恢复到完全生产前，可能数据中心负载很低。直到那时物理服务器与虚拟机功能差不多能被接受。

当运营恢复到正常，可将虚拟服务器转换回物理机。V2P 产品结合第三方 P2V 转换产品，让服务器回到最终物理测试位置。

任何时候虚拟系统时都不是先进行虚拟，你需要谨慎。不要同时开启系统。随着你发展一个虚拟化灾难恢复策略，要计划额外的资源，以便在 DR 站点供物理服务器的虚拟副本使用。

要明智管理，考虑投资一个第三方 P2V 迁移工具，让流程自动化，并能在 P2V 活动期间更新虚拟磁盘文件。（这些功能在 VMware Guided Consolidation 或 Microsoft System Center Virtual Machine Manager 中没有。）幸好很多第三方 P2V 转换工具不贵，用于日常备份还能节省时间。

（来源：TechTarget 中国）

原文标题：使用 P2V 迁移进行虚拟化灾难恢复
原文链接：http://www.searchvirtual.com.cn/showcontent_46734.htm

基于主机备份的虚拟环境灾难恢复

基于主机的备份逐步成为虚拟环境灾难恢复的最佳实践，跟基于 VM 的备份比起来也越来越流行。在虚拟灾备规划中，这种方式已经成为核心，因为它完成了宿主机上所有 VM 操作系统和应用的完整备份。相比而言，基于 VM 方式下需要针对单个 VM 的备份来完成灾难恢复。

在主机备份方式下，单个 VM 上不需安装备份代理。取而代之的是需要捕获虚拟硬盘和配置文件的状态来确保主机层面的数据一致性，然后通过主机把数据拷贝到所选的备份介质上。当需要快速恢复时，虚拟磁盘和配置文件可以很快在现有主机或指定地点重建。

不过主机备份的灾难恢复会受到很多因素的影响，所以请关注如下类型的工作负载可能受益于该灾难恢复最佳实践。

域名解析和目录服务

虚拟灾难恢复，需要域名解析和认证资源的支持。缺少认证系统，即使是那些没有位于失效主机上的应用也可能无法工作，所以恢复时间至关重要。对于域名解析和目录服务应用，借助基于主机的备份完成虚拟磁盘和配置文件的恢复所需的时间可以缩短到 10 分钟。

微软的 AD 服务模式下，通过使用多个域控可以实现认证系统的快速恢复。借助 AD 中的命令行工具 ntdsutil 分配服务器角色，每个域中都至少有一个域控，这样可以快速启用功能。系统重建完毕后，再分配备用的虚拟域控提高认证系统的可用性。物理架构下，这个过程要花费数小时的时间。

灾难恢复的最佳实践之一就是要至少保留每个域都有一个域控位于物理服务器上。不要把所有的 AD 域控都放到虚拟架构中，除非您已经保留了至少一台未加入域的宿主机。

基于主机的备份用于 LOB 应用

LOB（line-of-business）应用，例如医疗保健、财务和库存管理应用，也可以通过基于主机的备份进行恢复。甚至是那些由于资源需求而不适用于 VM 环境的应用，都可以借助该灾难恢复最佳实践在额外的硬件设备到来之前临时恢复使用。

但是要特别注意那些基于 MAC 地址进行授权认证的软件。您需要分配静态 MAC 地址后再从厂家获取新的认证号码；或者是使用现有的许可，而把 VM 的 MAC 更改为失效的物理主机的 MAC 地址。

基于主机的备份用于数据库

即使把数据库恢复到临时地点可能也无法立刻获得完整的资源可用性，但是对于访问部分关键数据而言已经足够了。多数时候，还需要重新恢复或挂载数据库系统，然后让域名解析系统可以响应客户端的连接请求。

对于微软 Hyper-V 基于主机的备份而言，可以通过 Hyper-V VSCS（卷影镜像）writer 和 SQL writer 来调整数据库完成在线备份，但是我尝试该过程的结果依然存在数据不一致。我建议至少每天进行一次基于文件的备份，而且备份数据至少保留一天。

VDI 和终端服务器的虚拟灾难恢复

搭建虚拟桌面体系后可以轻松创建镜像，允许客户通过 VDI broker（通常是 Citrix XenDesktop 或 VMware View）访问镜像。或者，您可以让远程工作人员通过客户端连接到位于宿主机上的虚拟服务器。

运行在终端服务器上的企业应用可以通过运行于虚拟宿主机上的方式，在发生灾难后提供对应用的访问能力。为保证用户访问可以及时恢复，至少应该保留一台 VM 和用户最关键的应用保持同步，并且通过基于主机的备份方式进行保护。通过运行关键应用的终端服务器可以缩小修复物理服务器之前所需的时间窗口。

虚拟 DR 的可支持性和授权

如果您没有基于主机备份所需的软件授权，多数的厂家都可以提供测试版授权帮助客户渡过难关。需要注意的是很多时候，获得的授权跟厂商签订的协议可能会有差异。虽然多数厂家不会在停机的时候选择落井下石，但是我们也需要意识到，在这段时间要完成对最终用户授权协议的补充和扩展。

当虚拟 DR 启动后，您可能不太关注某个特殊应用是否存在于 hypervisor 供应商的兼容性列表中。此时急需的是启动临时应急功能以满足客户的需求并避免财务损失。跳出固有思维来考虑问题。虽然供应商可能不支持某个特定应用的虚拟化，但是具备短期的、高度灵活性和快速安装能力的方案也是非常重要的。

基于主机的备份可以在较短时间内重建整个服务器，从而缓解虚拟灾难恢复的压力。为保证成功实施，需要学习这个最佳实践相关的技巧。

如果您通过服务器虚拟化或基于主机的备份成功加快了灾难恢复，请在这里分享您的案例。

（来源：TechTarget 中国）

原文标题：基于主机备份的虚拟环境灾难恢复
原文链接：http://www.searchvirtual.com.cn/showcontent_43823.htm