Hyper-V 安全管理最佳实践

Hyper-V 安全管理最佳实践

部署虚拟化很简单，但是管理却非易事，尤其是虚拟环境的安全问题。Hyper-V 管理员你们伤不起！！！安装 Hyper-V 有陷阱，还不止一个，有木有！有木有！！网络安全很头疼，Hyper-V 管理员还得兼任网管，有木有！！还需要掌握 PowerShell 常见命令，有木有！好不容易搭建个虚拟系统，还得建立容灾系统……以下省略 N 字。

咆哮体你们伤不起！言归正传，本期 TT 虚拟化技术手册与您分享 Hyper-V 安全管理最佳实践，内容很给力，有木有？

安装安全

选择了 Hyper-V 架构后，安装时需要注意哪些方面的问题？安装过程中有哪些陷阱？应该如何避免呢？

- 安全安装 Hyper-V 的最佳实践
- 部署 Hyper-V 的五大常见错误解析

网络安全

用虚拟交换机去完全地模拟物理交换机还仅仅处于设想阶段。Hyper-V 环境中如何保证网络安全？在预算范围内购买尽可能多的网络接口卡？

- 如何改善 Hyper-V 虚拟网络环境的安全性？
- 使用 NIC 创建子网隔离 Hyper-V 的网络流量

安全工具

Hyper-V 管理员掌握一些常用命令对于管理非常便捷，一些好的工具也能提升管理的安全系数。PowerShell 使用就可以很好的弥补 Hyper-V 在管理方面的缺陷。

- Hyper-V PowerShell 中的常用命令简介
- 使用 PowerShell 进行 Hyper-V 监控与测试

容灾安全

任何一个安全的虚拟化项目部署都离不开一个完善的容灾备份计划。那么在 Hyper-V 环境如何进行规划？怎样做最省钱？容灾站点如何搭建？本部分将与您分享。

- 如何通过微软 Hyper-V 进行灾难恢复规划
- 规划最省钱的 Hyper-V 容灾备份方式
- 搭建 Hyper-V 容灾恢复站点
- 为 Hyper-V 容灾恢复站点选择服务器

安全安装 Hyper-V 的最佳实践

所有人都了解，在今天这个互联的世界里，服务器需要额外的安全保护措施。而在加入了 Microsoft Hyper-V 虚拟化之后，安全保护方面也随之需要更多的关注，因为现在我们有多个虚拟机运行于同一台物理主机操作系统之上。

可能遭受攻击的对象从多台物理主机延伸到运行了多个虚拟机的单台物理主机。因此用户不仅需要关注那些像单个主机一样运行着的虚拟机的安全标准，还需要考虑这些虚拟机所在的物理主机的安全设置。

可能很多人还在争论安装不同的虚拟化架构后，其安全特性的优缺点。而本文只针对在您选择了 Hyper-V 架构后，安装时需要注意的内容。

网络保护

首先需要考虑的就是网络问题。Hyper-V 虚拟机本质上运行在安装于主机系统的虚拟网络交换机架构上。而在所有的 Hyper-V 主机里都安装了三层虚拟网络架构：外部虚拟网络、内部虚拟网络和私有虚拟网络。这种从物理网络架构到 Hyper-V 主机设备上虚拟网络的延伸，使得用户不再可以把网络安全问题完全抛给网络管理员去考虑，而是需要综合考虑网络拓扑结构会对服务器造成的影响。

最佳实践： 您需要把所有和管理相关的功能安装到完全独立的网络上。在 VMware 主机的虚拟架构中，把管理网络安装到独立的物理网络中是常见的做法，而在 Hyper-V 主机中我们也应该这么处理。这种架构允许我们把所有管理相关的数据链路都运行于一个只有管理员才可以访问的 vLAN 上。

这非常重要，因为通过这种方式可以把对宿主机的管理放在一个单独的网络上，从而避免其曝露在虚拟机运行的网络中。

当我们在定义 Hyper-V 中服务器的角色时，可以保留一块网络适配器专用于管理操作系统。 而利用这块保留的网卡，我们可以实现对管理数据流的分离。通过运行于一个独有的 VLAN 上，可以指定具有访问权限的人员和系统，例如设定为只有 System Center Virtual Machine Manager 或其他的第三方虚拟机管理系统可以访问。

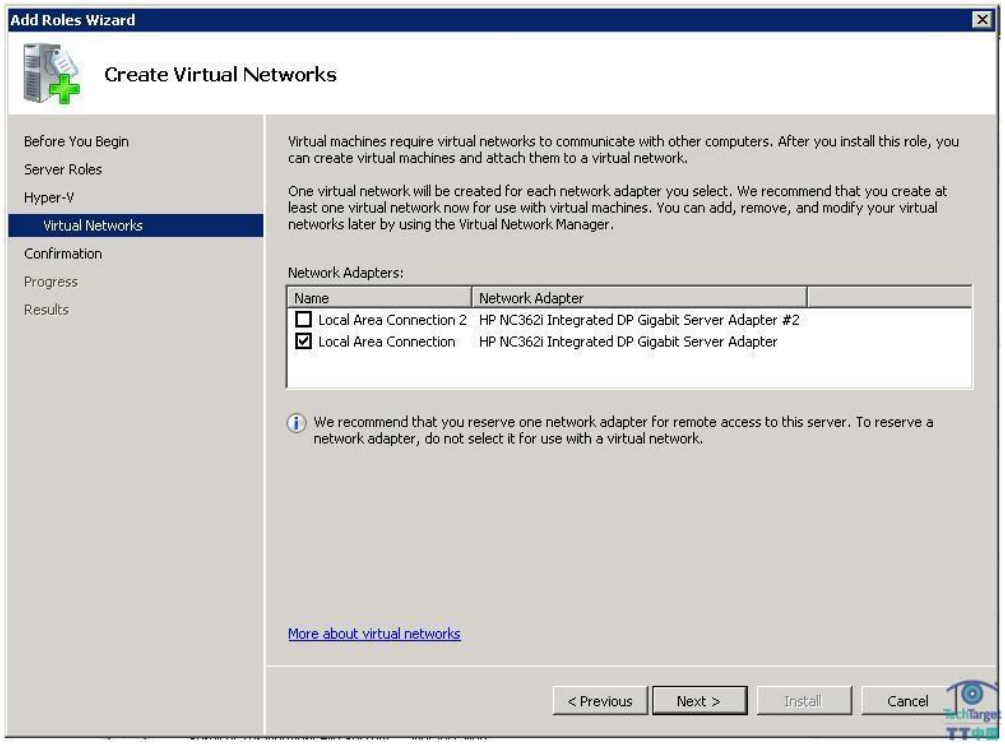


图 1，Hyper-V Add Roles Wizard （点击看大图）

如果您的物理主机是通过 VLAN 的方式实现隔离的，那么我们也可以把这种方式扩展到虚拟服务器上。例如，您可以设置一个前端网络用于生产系统服务器运行，另外设置一个独立的网络用于开发服务器使用。通过完成在虚拟机中的相关设置可以实现对 VLAN 功能的支持。

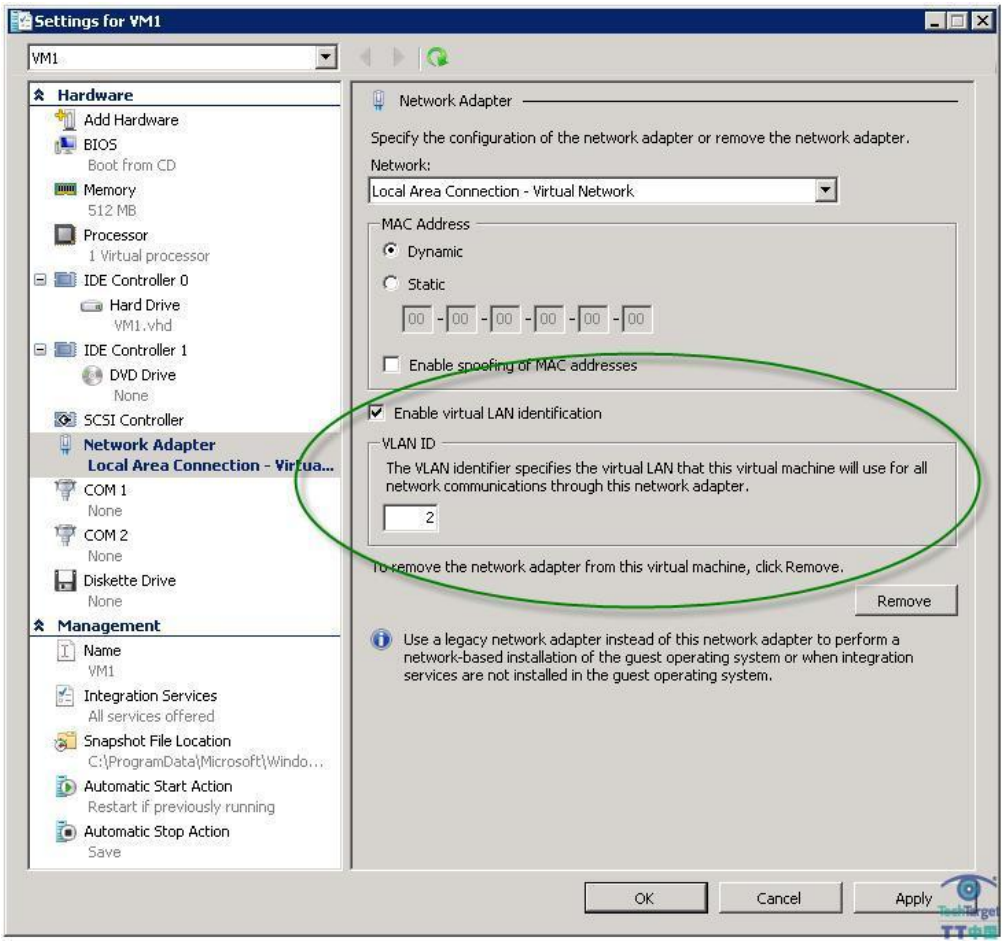


图 2，设置 VLAN 功能（点击看大图）

虚拟硬盘文件（VHD）

就像需要锁定对服务器硬盘的访问权限一样，我们也需要考虑对虚拟机硬盘文件的保护，VHD 文件需要位于主机上受保护的区域内。默认情况下，VHD 文件保存于%users%\Public\Documents\Hyper-V\Virtual Hard Disks 目录下，而对该目录的访问权限也做了相对合理的设置。而问题是，很多管理员希望把某些 VHD 文件移动到不同分区的单独目录下，从而获得更好的性能，或者是需要获得超出操作系统主分区大小的额外空间的时候。

最佳实践：无论您为 VHD 文件选择了哪个目录，请确保同时为该目录指定了正确的访问权限。

- 管理员和系统需要获得对该文件夹、子文件和文件的完全控制权。

- Creator Owner（创建者）需要获得对子文件和文件的完全控制权。
- Interactive, Service 以及 Batch 需要设置特殊权限，包括创建文件/数据写入、创建文件夹/添加数据、删除、删除子文件夹和文件、读取属性、读取扩展属性、读权限、写属性以及写扩展属性。

对虚拟机配置文件的锁定和保护也非常的重要。这些文件通常被保存在%programdata%\Microsoft\Windows\Hyper-V 目录中，对于这些都非常小的配置文件而言这是一个非常合适的地方。然而在您需要额外保存该文件的时候（例如用于简单备份使用），请一定要确保对新的文件夹指定了和如上描述的 VHD 文件相同的访问权限。

虚拟机所完成的功能？

我们在部署虚拟机时，一定要考虑虚拟机本质上所完成的功能。

考虑这个因素是为了避免把虚拟机暴露在不必要的风险之中，在同一主机上如果运行有低安全级别的虚拟机时，这种潜在风险就会存在。例如，没有人希望把后端数据服务器和最前端的防火墙服务器运行在同一台物理主机上。因为这样的话，一旦防火墙服务器被突破，整个宿主机都处于同等环境下，通过防火墙服务器上的网络可以直接连接到后端网络，甚至是物理上处于完全分离的子网络中的虚拟机，从而使整个系统都处于安全威胁中。

最佳实践：把相同风险级别或应用角色的虚拟机放到同一物理主机上，从而降低潜在的风险。

关于 Server Core 选项

安装 Server Core 对于 Hyper-V 专属环境而言是一个非常完美的选择。Server Core 是一个为远程管理而设计的，完全运行于命令行界面下的 Windows Server 2008 版本。从理论上看，这是一个非常伟大的想法，因为该版本中去掉了大量的可能受到攻击的界面接口，仅仅保留了对核心服务的安装。

因此，我们有什么理由不选择这种服务器方式呢？在很多公司，是由于管理方式的变更和所需培训投入带来的影响。Server Core 带来了一种全新的服务器管理方法，因此很多公司可能不愿意在时间和所需的培训上投入太多以支持这种新的模式。如果仅从安全角度决定，Server CoreHyper-V 主机绝对是最佳选择，当然这种是否有价值的选择需要取决于每个 IT 架构的不同。

当我们在安装 Hyper-V 系统时，从安全角度出发，有一些最重要的事情是一定要考虑到的。当然，仍然还有更多和管理员安全职责相关的问题我没有在文章中涉及，但对于初学者而言，起码要确保如上的这些最佳实践在您的 Hyper-V 安装过程中都做到了。

（作者：Eric Beehler 译者：李哲贤 来源：TechTarget 中国）

原文标题：安全安装 Hyper-V 的最佳实践

原文链接：http://www.searchvirtual.com.cn/showcontent_33815.htm

部署 Hyper-V 的五大常见错误解析

微软的 Hyper-v 使用已经非常容易了，它不需要有专门的技能，就可以设置虚拟机的启动和运行。即便有安装向导和最佳实践，但是还是有人会犯一些常识性的错误。

在本文中，TechTarget 中国的特约专家 Eric Beehler 将介绍部署 Hyper-V 时常见的五大错误，并提出解决办法。

一、忽视网络管理

当你首次添加 Hyper-V 虚拟化角色的时候，你就应该计划一块网卡专门用于管理。很多人忽视这条，觉得是在浪费网络端口。毕竟，没有专门的网络接口你仍然能够管理主机，为什么还要去浪费资源呢？

这里，我们应该去考虑安全问题。主机，从 Hyper-V 的架构来看，它是父分区，用于宿主几台虚拟机，拥有自己的工作负载和数据。当你能够访问主机的时候，也就意味着你可以直接访问这些虚拟机和虚拟机硬盘。你是否愿意让你的 DMZ 和内部网络工作在同一个子网呢？当然不愿意，这会有很大的安全风险。

考虑到主机相对于虚拟机拥有不同的安全级别，父分区只能在专用于管理员能访问的独立网络接口上进行管理。如果不这样的话，就面临着潜在风险。

二、使用错误的磁盘类型

当你设置一个全新的虚拟机时，你也该设置虚拟磁盘。动态扩展盘是主机硬盘上的一个文件，你可以随意更改它的大小。这是一个很好的选项，因为它一开始就是一个很小的文件，会随着你的需要而缓慢增长。就算你指定一个 250G 的硬盘，它只会使用所需的空间。这意味着你最终获得的是一个真实的 VHD 文件大小，通常都是比较小的。

但这样的方便是有代价的，因为动态扩展磁盘会影响性能。不仅在需要的时候扩展文件，在使用压缩功能添加和移出大量数据时也需要额外的维护。

如果你不保持追踪配置并用光磁盘空间的话，也会存在一个问题。固定大小磁盘通过创建合适大小的 VHD 文件，预留了空间，你的性能与硬件大致一致，并且避免了用光磁盘空间的可能。如果你已经拥有动态磁盘，你可以使用 Convert 操作将其转换成物理磁盘。

三、快照配置不正确

系统管理员使用微软 Hyper-V 虚拟化的最佳理由在于快照功能。这是用来恢复自己不小心对虚拟机的一些误操作的一个简单方法。不过，使用快照仍然存在几个问题。

首先，快照并不是一个备份，这看起来不合理，因为快照的魔力使其想一个完美的备份，但是它不会给你文件级别的恢复，也不会让你远离 Hyper-V 主机上的安全风险。它只是一个系统状态备份，因此某些应用，如 Microsoft Exchange Server 在运行数据或链接时会碰到问题。

其次，快照在默认情况下作为 VHD 文件存储在同个位置，因此快照文件会加剧磁盘磁盘有限的可用空间的窘境。你第一个倾向可能是使用 Hyper-V Manager 删除不需要的快照文件。这实际上不能摆脱这些快照文件。这仅仅在合并到主要 VHD 的时候作了标记。下次你关闭虚拟机时，合并就会发生，因此如果你有多个快照，这会需要大量时间。因此，没有任何快捷的方式缓解磁盘空间问题，确保合适地规划你的快照，并腾出时间来维护，避免问题出现。

四、过多的 CPU

目前多核很常见，主流的服务器基本都是 8 核。大多数人认为多核等于高性能，微软的 hyper-V 最大允许你分配 4 个 CPU（在 Hyper-V R2 里分配 32 个 CPU）给虚拟机。

虽然这种方式很灵活，但在单个虚拟机上使用多核是有代价的。你不应该给一个虚拟机分配多个虚拟机 CPU，最好按照 1：2 的比例来划分。以四核服务器为例，出于性能原因，你不应该分配超过 8 个虚拟的 CPU。此外你不应该分配 4 个 CPU 给一台虚拟机，因为虚拟机的处理器映射不到一个特定的物理核心上。相反，而是分配给所有的物理处理器去完成。因此，你要有适当理由为虚拟机配置多个核

心，像 CPU 密集型服务器，如数据库服务器就可以这样配置。如果你使用的是 WSUS 服务器，它多数时间是空闲的，分配多的核心就是浪费资源。

五、没有考虑使用虚拟交换机

虚拟交换机是网络技术的扩展。网络管理员设置虚拟 LAN（即 VLAN），并使用 802.1Q 集群，使网络更高效、更易于管理。

当我们插入交换机端口时，我们仍然将主机认为是该网络连接的终结点，其实不是。如果您在网络中使用 VLAN 和集群，可以将该功能扩展到您的虚拟机主机。让网络管理员给你交换机配置与设置的概要。为每个子网配置专用的网卡，在保存网络端口时，你能发现能宿主不同网络的各种虚拟机。当你只有有限的 NIC 端口时，这样尤其有用。

不需要广泛的专门培训，微软 Hyper-V 就可以在 Windows 管理员帮助下实现虚拟化。它很容易配置并不意味着选项不复杂。这些选项带来了许多积极方面，使人忘记了它们可能会在生产环境产生消极影响。要避免这些，需要提前做好决策，就可以安心使用功能完整的 Hyper-V 环境了。

(作者：Eric Beehler 译者：唐琼瑶 来源：TechTarget 中国)

原文标题：部署 Hyper-V 的五大常见错误解析

原文链接：http://www.searchsv.com.cn/showcontent_33415.htm

如何改善 Hyper-V 虚拟网络环境的安全性？

当人们提及虚拟交换机的时候，首先在您脑海出现的是否是一个放置于服务器机架顶端的，有 1U 或 2U 高，外观为黑色或深绿色的盒子？传统交换机厂商 Cisco, 3Com 或 Juniper 提供这种用于完成 IT 系统内部连接的网络架构产品。在这些网络设备的硬件内集成有成熟的网络处理操作系统（Internetwork Operating System），用于完成用户生产环境中所需的复杂路由、交换和访问控制等功能。

在现有的任何一种技术下，用虚拟交换机去完全地模拟物理交换机还仅仅处于设想阶段。而虚拟化平台内部的虚拟机交换机已经和物理交换机功能非常的相似，只是现在它还仅能作为物理服务器连接子网的一部分提供补充功能。本文中将要涉及的是在 Microsoft Hyper-V 环境中这种技术可能面临的一些问题。

简言之，虚拟网络并不等同于物理网络，我们需要对虚拟网络安全性保障方面给予更多的关注。首先，Hyper-V 的虚拟机交换机是“Learning Layer 2”设备，这指的是它们只能对基于介质访问控制地址（Media Access Control addresses）的数据包做路由。这也意味着 Hyper-V 的虚拟交换机不能识别和处理，基于更先进的 IP 地址方式的路由和数据访问控制功能，而这种方式在现在的 Layer 3 物理交换机上已经非常的普遍。从原理上看是因为在现有技术下，访问控制列表（ACL access control list）还无法被应用于 Hyper-V 内部的虚拟交换机上。

Hyper-V 的虚拟交换机还有一些其它功能限制，这是由于它缺乏对第三方监控和虚拟网络流量管理功能的支持而导致的。一旦数据流从物理网络进入到 Hyper-V 的内部虚拟网络中，它就失去了所有来自外部的入侵防护和流量检测功能。

因此，Hyper-V 网络环境需要通过一些配置技巧来复制那些在物理服务器中所具有的高级安全功能。首先，用于限制到 Hyper-V 宿主机端口流量的访问控制列表（ACLs）需要重新设置，使其仅支持来自物理网络架构中的数据访问。而位于同一台主机上的虚拟机之间的会话则不会受到那些基于网络的访问控制列表的限制。如果在安全法规中有要求的话，还需要为每台虚拟机单独安装操作系统层防火墙和流量监测软件。

在微软的 Hyper-V 安全指南中也强烈建议用户保留独立的网卡设备，用于宿主机主分区（primary partition,即管理操作系统所在的分区）到网络的连接。通过这种方式，可以使位于主分区上操作系统的网络流量和子虚拟机的网络流量接口层相分离。从安全的角度考虑，我们认为子虚拟机访问流量的安全级别往往比主分区的要低，因为必须首先保证主分区的安全才能使其上的子虚拟机保持正常运行。那

些对安全级别要求较高的环境中可能会更加严格，对于主分区网络流量不仅仅要限制在自有的网卡接口上，而且要位于独有的受保护的子网中。

微软在 Windows Server 2008 R2 版本中，引入了一项新的虚拟机交换机管理设置，从而加强了 Hyper-V 的安全性。在 R2 版本的 Hyper-V Virtual Network Manager 中加入了一个新的复选框“Allow management operating system to share this network adapter（允许管理操作系统共享该网络适配器）”。通过这个选项进一步确保管理操作系统流量和虚拟机流量的分离。在不勾选该项的情况下，主操作系统分区就无法访问创建的虚拟网络。

在需要实现高可用的 Hyper-V 环境中，还需要在集群节点间实现一定形式的存储共享。在很多情况下，都是通过安装基于 iSCSI 接口的存储区域网络（SAN）架构以满足 Hyper-V 虚拟机的存储需求。那么，最佳的做法就是始终保持 iSCSI 网络流量和生产环境网络流量的分离。同时，iSCSI 流量通常还应该位于一个独立的子网中，以防止在网络拥挤时出现拒绝服务的情况，而且也便于将来把各种不同类型的网络流量相互分离。

很多用户尝试通过网络接口间的聚合（teaming）来提高系统可用性。在这方面，微软本身并不提供用于实现高可用的网卡聚合功能。而这一点也是众多媒体经常批判的，关于生产环境中应用 Hyper-V 架构所具有的重大缺陷之一。但是，我们需要注意到微软从未对端口聚合做支持，包括在物理环境中。而在这点上，像 Dell 和 HP 这样的供应商多年来一直在坚持开发自己的支持负载均衡的网卡聚合驱动程序，而这些驱动有很多也可以用于 Hyper-V 环境中。很明显，作为用户我们需要去区分各 OEM 供应商所能提供的这类驱动的支持级别。

简言之，当我们的 Hyper-V 宿主机拥有足够多的物理网卡接口时，迁移到 Hyper-V 虚拟机环境的工作就会变得很简单。我们也可以看到一些公司采用了带有 10 个网卡接口的 Hyper-V 宿主机，除了现在通用的主板自带的两个网卡接口之外，加入两块四端口的物理网卡实现总计 10 个物理端口。拥有这么多的物理网卡接口可以确保满足冗余的生产网络、存储网络和管理网络分离的需求，另外还有部分预留的接口可以做很多“有趣的”网络设置，从而满足将来可能增长的需求。

网络具有潜在的风险，而在托管的虚拟机如何适应 Hyper-V 宿主机上也存在潜在的风险。尤其在为满足故障切换和负载均衡需求而设置的，可以支持虚拟机在线迁移的集群环境中，虚拟机的托管带来的安全性以及和 IT 架构的兼容性问题都是需要特别关注的。请关注这一系列文章的下一篇，您将了解到更多相关内容。

（作者：Greg Shields 译者：李哲贤 来源：TechTarget 中国）

原文标题：如何改善 Hyper-V 虚拟网络环境的安全性？
原文链接：http://www.searchvirtual.com.cn/showcontent_33810.htm

使用 NIC 创建子网隔离 Hyper-V 的网络流量

当来咨询的客户表达他们对 Hyper-V 的兴趣时，我建议在他们预算范围内购买尽可能多的网络接口卡（NIC）。一般地，如果是出于通过光纤通道存储区域网络集中存储的目的，我建议为每台服务器至少配备四个 NIC。如果客户端使用 iSCSI SAN，我建议至少使用六个 NIC。不过为每台服务器配备 10 个 NIC 也是很平常的。

原因在于许多 Hyper-V 服务器管理员需要进行由额外 NIC 造成的网络隔离。管理员也喜欢能在存储和生产网络连接之间进行连接聚合。不过虽然 Hyper-V 能支持虚拟局域网（VLAN）聚合，这是种支持多个拥有一个以上交换机的 VLAN 的方式，这种设置的挑战更多在于政治上，而不是技术上。

一般来说，当 VLAN 聚合到 Hyper-V 服务器，网络管理责任就落在虚拟化管理员身上了。网络管理员忽视了这种责任是常见的，安全经历很担心，因为一组“非专家”（例如虚拟管理员）现在对他们不太精通的环境负有责任。

此外，当多个 VLAN 聚合在一起，潜在的管理错误会增加。随着更多服务器管理员尝试整合多个子网，因此，安全区域问题会上升。

另外，使用子网隔离网络流量，不仅按照微软的建议指南分配 NIC 到不同的子网，也能预防半途而废。微软的故障转移集群服务对于频率延迟尤其苛刻，当服务器不能及时发送或响应集群频率，或导致资源或集群故障。通过使用集群本身的链接隔离集群频率，就能避免这种情况。

为了证明我的观点，下面是如何正确隔离网络连接的实例。我的一位客户购买了两台 Hyper-V 服务器，跨三个子网部署虚拟机：

- 子网 A 是生产网络，包括传统的办公室服务器，如 Exchange、SQL 和文件服务器；
- 子网 B 是一个运营网络，用于业务线服务器，业务关键组需要少量额外的网络保护；
- 子网 C 包括测试和开发者的分段沙盒。

要正确连接子网，需要以下六个 NIC：

- 一个 NIC 专用于到 Hyper-V 服务器的管理流量。热迁移流量也通过这个接口。

- 一个接口卡用于集群的频率连接。这个连接宿主在本身的子网里，并且确保网络堵塞不会导致集群故障。
- 两个 NIC 通过多路径 I/O 设置连到 iSCSI SAN。
- 两个网络卡作为绑定连接，进行物理连接，并在逻辑上配置到网络 IOS，以通过 VLAN 流量到子网 A、B 和 C。

这是种可接受的配置，因为在其区域里隔离了每个通信类型。例如，iSCSI 流量通过使用隔离的路径通过存储网络。这种设置确保生产网络连接不会影响到服务器硬盘驱动的访问。

为管理流量创建隔离的连接，另一方面完成了两件事情。第一，从物理上隔离了来自 Hyper-V 管理流量的虚拟机流量，这样更安全。同时，防止虚拟机过度消耗网络连接，阻碍服务器管理。

最后两个 NIC 旨在网络聚集。这种配置在 IT 博客里进行广泛深入地讨论，。我在这系列文章的第一部分“Hyper-V NIC 聚合”中已经解释过。注意，微软虚拟网络交换机协议可能阻止一些 NIC 聚合驱动启用。在尝试 Hyper-V NIC 聚合之前检查服务器厂商支持表。

我这个客户聚合了这三种生产 VLAN 到相同的成对接口。尽管流量低，Hyper-V 主机服务器的数量相对较小，系统管理员通过独立的接口隔离每个 VLAN 流量，而不是聚合它们。

原因在于他们想预防错误。

有时，Hyper-V 的 VLAN 向导很难操作。首先，你必须创建和分配正确的参数给 Virtual Network Manager 里的虚拟交换机。接下来，确保正确的物理接口连接到正确的虚拟交换机。由于 Hyper-V 的管理向导缺乏单窗口物理界面，就很容易犯错。

由于 Hyper-V 或思科的路由协议使用 VLAN 存在数据泄露问题，在 VLAN 指尖使用虚拟机的接口存在很大风险。因此，他们最多使用 10 个 NIC 通道。

在本系列最后一部分钟，我将解释创建虚拟交换机的过程。

（作者：Greg Shields 译者：唐琼瑶 来源：TechTarget 中国）

原文标题：使用 NIC 创建子网隔离 Hyper-V 的网络流量
原文链接：http://www.searchvirtual.com.cn/showcontent_29312.htm

Hyper-V PowerShell 中的常用命令简介

对于虚拟机、宿主机和任务进程而言，微软 Hyper-V 管理控制台和 SCVMM（System Center Virtual Machine Manager）都是很不错的管理工具。但是和大多数的图形界面接口（GUI）工具一样，都无法避免在客户定制化和管理权限上受到限制。但是 PowerShell 的使用可以很好的弥补 Hyper-V 在管理方面的缺陷。

SCVMM 和 Hyper-V PowerShell cmdlets 帮助虚拟机环境的管理员开启了新的管理模式。在本文中，TechTarget 中国的特约专家 Rob McShinsky 讲述一些 PowerShell cmdlets 和命令。即使您没有购买 SCVMM，依然可以使用 PowerShell 来完成大多数的任务，包括：获得基本的系统信息、创建新的虚拟机和完成在线迁移过程等。首先，下载并安装 Hyper-V PowerShell 模块。（或许某些时候您还需要更改 PowerShell 的执行模式，以保证该模块可以正确运行。在 Windows Server 2008 中它可以正常工作，但是在 Windows 7 中，您可能需要对执行模式做更改以减轻其受到的限制。这并不是最佳的办法，但是请注意有些时候我们必须减轻执行模式的限制。 ）

在完成了 Hyper-V PowerShell 模块的安装后，接下来就可以尝试一些基本的功能。在你对这些 PowerShell cmdlets 和命令足够熟悉之后，还可以组合一些命令编写成更加复杂和实用的脚本。但是这个过程并不像“Hello World”那么简单，在我们学习跑步之前先来学习走路。

Get-VM。这个 cmdlets 对于很多脚本程序而言，都是最基本的常用命令之一，而且从字面上也很容易理解。Get-VM 检索虚拟机相关的信息，然后快速呈现出某台特定主机上的虚拟机状态。我经常这样使用该命令：

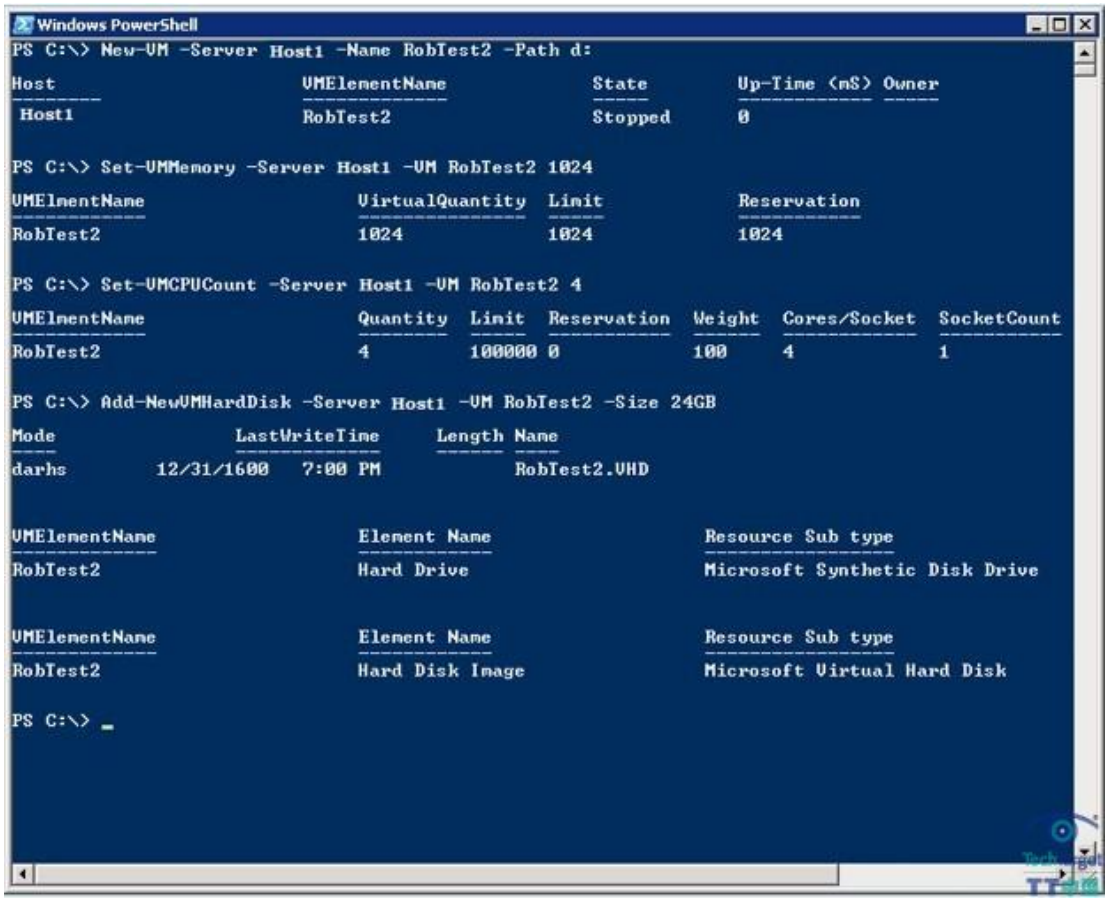
Get-VM --Server

图 1

请注意，您必须通过-Server 辅助命令来锁定某一台特殊的服务器操作，这点在使用 Hyper-V 管理控制台时也是一样的。

New-VM, Set-VMMemory, Set-VMCPUCount, Add-NewVirtualHardDisk.这一组 Hyper-V PowerShell cmdlets 用于创建新虚拟机。虽然在 Hyper-V Manager GUI 中通过配置向导来完成更加简单一些，但是在需要同时创建多个虚拟机的时候，命令行的方式会更加好用。

图 2



通过这些命令做简单调整，还可以增加或修改多台虚拟机。

```
New-VM -Server Host1 -Name RobTest2,RobTest3,RobTest4 -Path d:
Set-VMMemory -Server Host1 -VM RobTest2,RobTest3,RobTest4 1024
Set-VMCPUCount -Server Host1 -VM RobTest2,RobTest3,RobTest4 4
```

```
Add-NewVMHardDisk -Server Host1 -VM RobTest2,RobTest3,RobTest4 -Size
24GB
```

现在您可以看到，在同时创建多个虚拟机时这样可以节省时间。

Start-VM, Stop-VM, Save-VM, Shutdown-VM. 用于完成虚拟机状态调整的命令也非常的好用。有一些操作无法通过 GUI 来实现的，我经常使用这些命令来关闭虚拟机或是保存虚拟机状态以用于故障诊断。和同时创建和调整多个虚拟机的命令相似，通过这些命令可以同时改变多台虚拟机的运行状态。

```
Start-VM -Server Host1 -VM RobTest2,RobTest3,RobTest4
Stop-VM -Server Host1 -VM RobTest2,RobTest3,RobTest4
Save-VM -Server Host1 -VM RobTest2,RobTest3,RobTest4
Shutdown-VM -Server Host1 -VM RobTest2,RobTest3,RobTest4
```

注： 如果要使用 Shutdown-VM 命令，需要安装 Hyper-V 集成组件。

Move-VM. PowerShell 还可以用于帮助完成 Hyper-V 集群的某些工作。我曾经在 Failover Cluster Administrator 无法正确工作的情况下，使用如下的命令迁移虚拟机以用于故障的诊断。当然，使用 cluster.exe 命令也可以在节点间迁移虚拟机，但是我更喜欢使用 PowerShell 命令。

```
Move-VM -Server Host1 -VM RobTest2 -Destination Host2 --force
```

当然，多台虚拟机的迁移也是可以实现的，但是需要连续地操作。

```
Move-VM -Server Host1 -VM RobTest2,RobTest3,RobTest4 -Destination Host2
--force
```

或者借助通配符，您也可以把 Host1 上的所有以 RobTest 开头的虚拟机迁移到 Host2 上。

```
Move-VM -Server Host1 -VM RobTest% -Destination Host2 --force
```

（注：为了避免出现提示信息：“WARNING: Cluster commands not loaded. Import-Module FailoverClusters and tr y again”，运行“Run, Import-Module FailoverCluster”命令完成 Failover Cluster 模块的装载，并启用 PowerShell 的集群属性。）

在您对这些 PowerShell cmdlets 和命令逐渐熟悉以后，可以尝试浏览一下 PowerShell Management Library for Hyper-V 手册。虽然手册的内容本身让人昏昏欲睡，但是我们可以一边阅读一边实践一些新的 Hyper-V PowerShell 命令，之后您可能会发现它提供了一种通用的语法模式。那么，您就可以编写脚本来借助 PowerShell 完成一些更加复杂的辅助性管理工作，相信您会慢慢发现这样做要比完全使用 Hyper-V 向导来完成虚拟机管理任务快地多。

（作者：Rob McShinsky 译者：李哲贤 来源：TechTarget 中国）

原文标题：Hyper-V PowerShell 中的常用命令简介
原文链接：http://www.searchvirtual.com.cn/showcontent_36796.htm

使用 PowerShell 进行 Hyper-V 监控与测试

对于虚拟机、宿主机和任务进程而言，微软 Hyper-V 管理控制台和 SCVMM（System Center Virtual Machine Manager）都是很不错的管理工具。但是和大多数的图形界面接口（GUI）工具一样，都无法避免在客户定制化和管理权限上受到限制。但是 PowerShell 的使用可以很好的弥补 Hyper-V 在管理方面的缺陷。

SCVMM 和 Hyper-V PowerShell cmdlets 帮助虚拟机环境的管理员开启了新的管理模式。在本文中，TechTarget 中国的特约专家 Rob McShinsky 讲述一些 PowerShell cmdlets 和命令。即使您没有购买 SCVMM，依然可以使用 PowerShell 来完成大多数的任务，包括：获得基本的系统信息、创建新的虚拟机和完成在线迁移过程等。首先，下载并安装 Hyper-V PowerShell 模块。（或许某些时候您还需要更改 PowerShell 的执行模式，以保证该模块可以正确运行。在 Windows Server 2008 中它可以正常工作，但是在 Windows 7 中，您可能需要对执行模式做更改以减轻其受到的限制。这并不是最佳的办法，但是请注意有些时候我们必须减轻执行模式的限制。 ）

在完成了 Hyper-V PowerShell 模块的安装后，接下来就可以尝试一些基本的功能。在你对这些 PowerShell cmdlets 和命令足够熟悉之后，还可以组合一些命令编写成更加复杂和实用的脚本。但是这个过程并不像“Hello World”那么简单，在我们学习跑步之前先来学习走路。

Get-VM。这个 cmdlets 对于很多脚本程序而言，都是最基本的常用命令之一，而且从字面上也很容易理解。Get-VM 检索虚拟机相关的信息，然后快速呈现出某台特定主机上的虚拟机状态。我经常这样使用该命令：

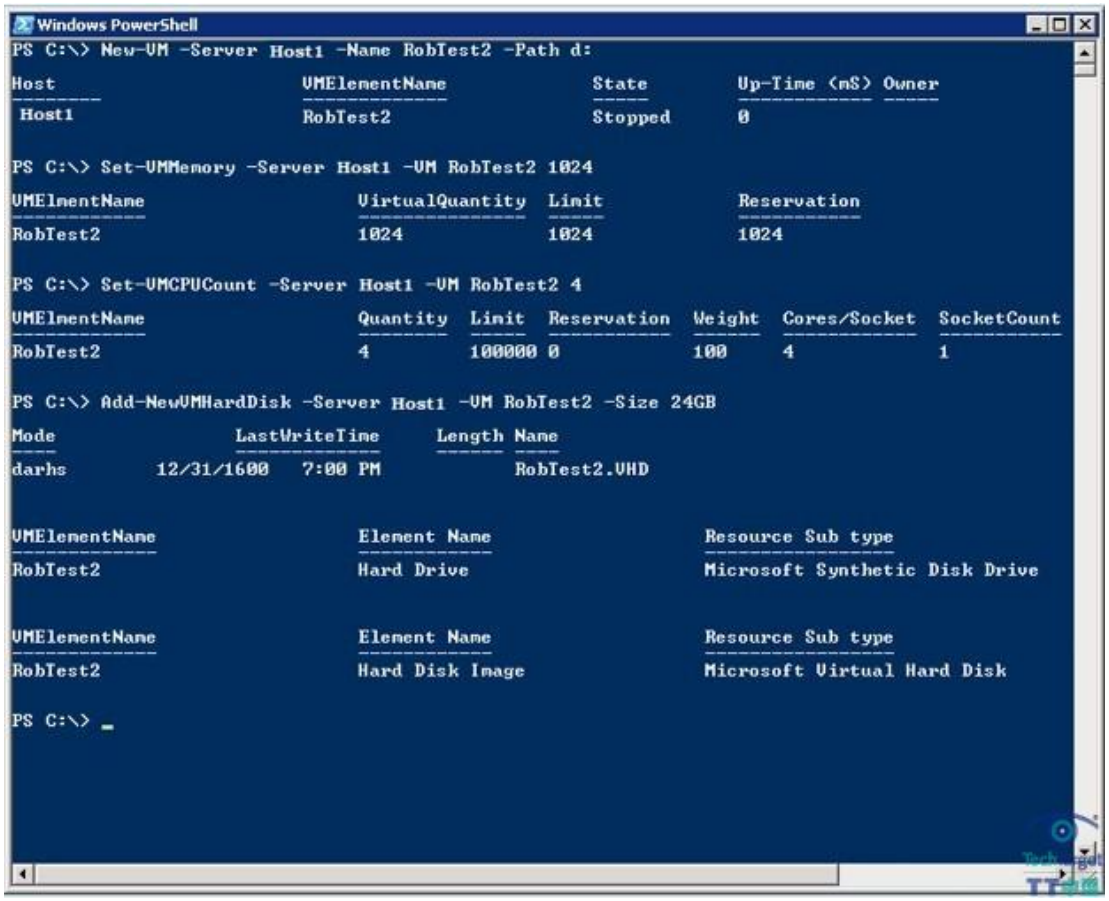
```
Get-VM --Server
```

图 1

请注意，您必须通过-Server 辅助命令来锁定某一台特殊的服务器操作，这点在使用 Hyper-V 管理控制台时也是一样的。

New-VM, Set-VMMemory, Set-VMCPUCount, Add-NewVirtualHardDisk. 这一组 Hyper-V PowerShell cmdlets 用于创建新虚拟机。虽然在 Hyper-V Manager GUI 中通过配置向导来完成更加简单一些，但是在需要同时创建多个虚拟机的时候，命令行的方式会更加好用。

图 2



通过这些命令做简单调整，还可以增加或修改多台虚拟机。

```
New-VM -Server Host1 -Name RobTest2,RobTest3,RobTest4 -Path d:
Set-VMMemory -Server Host1 -VM RobTest2,RobTest3,RobTest4 1024
Set-VMCPUCount -Server Host1 -VM RobTest2,RobTest3,RobTest4 4
```

```
Add-NewVMHardDisk -Server Host1 -VM RobTest2,RobTest3,RobTest4 -Size
24GB
```

现在您可以看到，在同时创建多个虚拟机时这样可以节省时间。

Start-VM, Stop-VM, Save-VM, Shutdown-VM. 用于完成虚拟机状态调整的命令也非常的好用。有一些操作无法通过 GUI 来实现的，我经常使用这些命令来关闭虚拟机或是保存虚拟机状态以用于故障诊断。和同时创建和调整多个虚拟机的命令相似，通过这些命令可以同时改变多台虚拟机的运行状态。

```
Start-VM -Server Host1 -VM RobTest2,RobTest3,RobTest4
Stop-VM -Server Host1 -VM RobTest2,RobTest3,RobTest4
Save-VM -Server Host1 -VM RobTest2,RobTest3,RobTest4
Shutdown-VM -Server Host1 -VM RobTest2,RobTest3,RobTest4
```

注： 如果要使用 Shutdown-VM 命令，需要安装 Hyper-V 集成组件。

Move-VM. PowerShell 还可以用于帮助完成 Hyper-V 集群的某些工作。我曾经在 Failover Cluster Administrator 无法正确工作的情况下，使用如下的命令迁移虚拟机以用于故障的诊断。当然，使用 cluster.exe 命令也可以在节点间迁移虚拟机，但是我更喜欢使用 PowerShell 命令。

```
Move-VM -Server Host1 -VM RobTest2 -Destination Host2 --force
```

当然，多台虚拟机的迁移也是可以实现的，但是需要连续地操作。

```
Move-VM -Server Host1 -VM RobTest2,RobTest3,RobTest4 -Destination Host2
--force
```

或者借助通配符，您也可以把 Host1 上的所有以 RobTest 开头的虚拟机迁移到 Host2 上。

```
Move-VM -Server Host1 -VM RobTest% -Destination Host2 --force
```

（注：为了避免出现提示信息：“WARNING: Cluster commands not loaded. Import-Module FailoverClusters and tr y again”，运行“Run, Import-Module FailoverCluster”命令完成 Failover Cluster 模块的装载，并启用 PowerShell 的集群属性。）

在您对这些 PowerShell cmdlets 和命令逐渐熟悉以后，可以尝试浏览一下 PowerShell Management Library for Hyper-V 手册。虽然手册的内容本身让人昏昏欲睡，但是我们可以一边阅读一边实践一些新的 Hyper-V PowerShell 命令，之后您可能会发现它提供了一种通用的语法模式。那么，您就可以编写脚本来借助 PowerShell 完成一些更加复杂的辅助性管理工作，相信您会慢慢发现这样做要比完全使用 Hyper-V 向导来完成虚拟机管理任务快地多。

（作者：Rob McShinsky 译者：李哲贤 来源：TechTarget 中国）

原文标题：使用 PowerShell 进行 Hyper-V 监控与测试
原文链接：http://www.searchvirtual.com.cn/showcontent_36796.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。

（作者：Eric Beehler 译者：刘波 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

规划最省钱的 Hyper-V 容灾备份方式

将 Hyper-V 容灾备份到另外一个站点上，没有必要购买昂贵的解决方案或者部署复杂的架构。

Hyper-V 容灾恢复工具的出现使容灾恢复不再是只有 Windows 集群领域的博士才可以完成了。当前的存储区域网络可能就内置有可以用来完成主站点和备份站点之间的镜像复制技术。

早期只有大型企业才用得起的 Hyper-V 容灾恢复技术现在已经成为甚至最小工作平台中必不可少的组件。由于 Microsoft 对 Windows Server 2008 RTM 和 R2 版本中 Windows 宕机备份集群的改进，Hyper-V 容灾恢复技术现在已经非常简单，用户大概花费一个下午的时间就可以自己完成一次技术性验证测试。

规划 Hyper-V 容灾恢复

“虚拟化无处不在”这个概念的出现改进了防止故障的方案。过去备份只是可用的预防技术。在丢失一个文件、一台服务器甚至整个站点的数据之后，用户可能最经常问到的问题就是：“我曾经备份了吗”，或者是“如何才可以恢复这些数据”。

现在虚拟机的出现带来了很大的优势，归纳虚拟化的优势和属性是个非常困难的工作。当前有无数种保护虚拟机的方案，保持这种可能性本身就是一个问题。

Hyper-V 容灾恢复规划的第一步是明白容灾恢复是否确实是必须的。根据数据中心对宕机时间的容忍程度以及对恢复时间的要求，需求可能会各不相同。考虑使用如下这些方案来保护虚拟机，下面列出的这四项能力可能会增加实施成本。

- **恢复**：恢复技术可以使虚拟机从一个时间点和磁盘或者磁带重新回到在线状态。由于简单的服务器恢复技术是一项花费相当便宜的方案，但是恢复虚拟机所使用的时间也最长。根据备份解决方案的不同，解决方案的控制粒度也不同：在恢复过程中，不用知道精确的恢复点。例如，如果每天晚上都备份虚拟数据，则恢复点就可能是“过去某天的某个时间”。这些技术在一些工作环境中非常适用，但是对其另外一个工作环境中，不知道恢复点是无法接受的。
- **高可用性**：Hyper-V 工作环境中的高可用性通过 Windows 宕机备份集群服务激活。需要注意的是高可用性和容灾恢复没有任何关系。但是高可用性却是

在主机故障后虚拟机重新恢复的辅助工具。如果虚拟机出现崩溃或者死机蓝屏，以及整个站点故障的情况，只有高可用性是不能够把虚拟机重新回退到前面某个时间点的。

- **容灾恢复**：Hyper-V 容灾恢复也需要通过 Windows 宕机备份集群服务才可以使用，但是以一种更强健的方式使用。支持容灾备份的 Hyper-V 集群可以扩展到不止一个地理站点上，另外也可以展示在站点之间复制虚拟机存储的技术。这项配置可以确保虚拟机在站点故障出现之后尽快地恢复。
- **容错**：有一些工作负载无论如何都要保持运行状态，例如一台生产型 Exchange 服务器或者承载关键任务的 SQL 数据库。如果应用程序的主实例出现故障，辅助实例就可以立刻接替处理客户的需求。该设置所使用的技术和技巧与传统的容灾恢复不同，并且需要额外的规划。

这个清单同时也分解了当前使用的技术承担的费用。例如恢复一台单独的虚拟机需要一个备份解决方案，以及可能有的磁盘或者磁带。另一方面，容错设计倾向于需要更多的硬件和应用程序层面的复制技术（这可能就需要购买了）。

规划 Hyper-V 容灾恢复显然是很宏观的一个步骤，其中需要确保精确地考虑到对工作平台有影响的各种失败可能。

（作者：Greg Shields 译者：王越 来源：TechTarget 中国）

原文标题：规划最省钱的 Hyper-V 容灾备份方式
原文链接：http://www.searchvirtual.com.cn/showcontent_34543.htm

搭建 Hyper-V 容灾恢复站点

容灾恢复规划中的一个重要错误就是分别规划主站点和辅助站点。任何高效的业务持续性战略都会把两个容灾恢复站点与其业务连接起来。

在“创建 Microsoft Hyper-V 容灾恢复站点”这一系列文章的第一部分，TechTarget 中国的特约专家 Greg Shields 介绍了各种导致虚拟化工作环境失败的情况。则接下来一步——搭建 Hyper-V 容灾恢复站点——就要求更加细致的规划。

最重要的是必须重新查看主站点的现有结构，两个站点都必须拥有正确的设备和集群配置以确保成功的宕机备份。在规划辅助站点时，考虑整合以下组件。

容灾恢复站点的存储和网络

首先在容灾恢复站点需要另外一套存储设备，设备的容量必须能够容纳所有的虚拟机及其数据。需要注意的是可能并不是工作环境中的每一台虚拟机都需要这一存储设备。针对部分虚拟机工作负载的防故障性可能不需要考虑，但是存储设备必须能够满足每一台虚拟机的额外磁盘和数据需求，诸如数据库或者库存材料。

另外，可能也需要必要的网络基础架构以实现两个站点上的集群设备能够相互通信。站点的网络技术必须提供足够好的性能以确保复制过程中不会出现大量数据排队现象。目前大多数复制解决方案提供商都能够监控虚拟工作负载的变化率，并且估计必要的带宽。在规划阶段完成这些计算是非常重要的，或者可能就会发现当前的可用带宽不足以满足复制需求。

存储复制技术倾向于涉及到两种机制中的其中一种，并且通常情况下安装在其中一个站点上。则就会有四种不同的组合，选择满足需求的一种就可以了。下面列出了对每一选择的概要介绍：

- **同步复制**：在该方案中，磁盘存储的改变必须在下一次改变发生之前向两个站点确认。但是这个过程可能降低磁盘操作速度（有时还是急剧的）。同步复制通常要求站点之间的距离比较近以及相当高的带宽，但是如果数据保存需求比较高的话，该容灾恢复方案就值得商榷了。
- **异步复制**：和同步复制不同，异步复制允许大量改变排队，并且在合适的情况下提交确认。当主站点出现故障时，该方法会导致数据丢失，但是丢失量几乎可以忽略不计。该方法的优势在于可以解决同步复制的性能和距离限制的问题。

- **安装到存储设备**：两个选择对于宿主存储复制软件的位置也都是有可能的：在存储设备自身或者在和存储设备相连的一个硬件设备上。该软件通常都已经安装在硬件之上，因此可能都不需要再安装到这些设备上了，但是需要激活。然而需要注意的是基于存储设备的技术如果没有正确地整合到每一台虚拟机的操作系统内，可能会带来虚拟机或者应用程序的崩溃。但是使用主机或者基于虚拟机代理的存储复制解决方案对于在复制期间维护应用程序数据完整性非常重要。
- **安装到主机或者虚拟机**：另外一种方案，可以把解决方案安装到 Hyper-V 主机或者其承载的虚拟机中。这些基于软件的解决方案通常可以通过内置于主机或者虚拟机的文件系统中解决复制问题。从而该软件可以捕获到主机或者虚拟机磁盘的改变，并且把这些更改封装传送到容灾恢复站点。这些数据可验证地确保数据和应用程序的完整性，但是也不能有效度量，因为牵扯到通过网络向容灾恢复站点发送数据的多台主机或者虚拟机上所承载的多个客户端。另外，取决于技术方案的不同，商家可能向复制的虚拟机要价很高而导致该方法的费用上升。

需要时刻保持注意的是 Microsoft 内置的分布式文件系统复制解决方案和 Windows 宕机备份集群并不兼容。需要一个第三方的解决方案才可以完成必要的复制工作。

（作者：Greg Shields 译者：王越 来源：TechTarget 中国）

原文标题：搭建 Hyper-V 容灾恢复站点
原文链接：http://www.searchvirtual.com.cn/showcontent_34620.htm

为 Hyper-V 容灾恢复站点选择服务器

容灾恢复规划中的一个重要错误就是分别规划主站点和辅助站点。任何高效的业务持续性战略都会把两个容灾恢复站点与其业务连接起来。

在“创建 Microsoft Hyper-V 容灾恢复站点”这一系列文章的第一部分，TechTarget 中国的特约专家 Greg Shields 介绍了各种导致虚拟化工作环境失败的情况。则接下来一步——搭建 Hyper-V 容灾恢复站点——就要求更加细致的规划。

在容灾恢复站点需要足够的服务器设备才可以应对宕机备份的虚拟机。需要记住的是：在出现故障的情况下，也可能不需要备份所有的虚拟机。因此首先考虑为容灾恢复站点规划和主站点同样多的 Hyper-V 主机。然后通过标识出在出现故障时可以放弃的虚拟机从而缩减容灾恢复站点主机的数量——但是同时需要确保考虑到后期扩展。

最后可以说是最重要的一点——记住容灾恢复站点是用来防止出现灾难性事件的。这就意味着主站点和辅助站点之间的距离必须足够远，这样才可以防止出现灾难时两个站点同时被毁坏。

因此，例如，如果一家银行为了防止龙卷风带来的灾难，则可能把其容灾恢复站点放置在城市的另外一侧。另外一个例子，希望防止飓风灾难的沿海业务就需要在更远一点的内陆找一个合适的位置。

在决定辅助容灾恢复站点位置时，把两个站点之间的网络和性能需求考虑进来。距离比较近的站点可能比那些距离比较远的站点花费较少的昂贵的网络解决方案费用。做容灾规划相当重要，但是真正需要的是一个保护虚拟机的功能性解决方案。在这些规划复付诸实践之后，就可以对 Hyper-V 容灾恢复轻松地实施 Microsoft 的解决方案——这是本系列文章中后面两篇要讨论的内容。

（作者：Greg Shields 译者：王越 来源：TechTarget 中国）

原文标题：为 Hyper-V 容灾恢复站点选择服务器
原文链接：http://www.searchvirtual.com.cn/showcontent_34621.htm