虚拟化管理

虚拟化管理

在上一个专题里，我们详细讲解了实施虚拟化需要考虑的步骤：确认候选者、容量规划、ROI计算、P2V迁移及企业管理。在接下来的运营阶段，我们应该如何管理虚拟化环境呢？虚拟机性能如何测量？VM自动化有什么好处？怎么应对虚拟化环境下的安全性挑战？在本专题中，我们将为您解答。

虚拟机

追踪虚拟机性能以精确地找到问题或得到资源消耗的报道，这是一项非常复杂的任务。那怎么测量 VM 性能呢？VM 管理自动化又有什么好处呢？

- **如何测量虚拟机性能？**
- **使用 VM 管理自动化控制虚拟化混乱**

高可用性

数据中心资源管理十分复杂。要保证虚拟机始终可用、确保快速的灾难恢复和可靠的故障恢复能力，需要很多技巧。我们先讲述虚拟机备份的过程及选择，然后进一步探讨虚拟环境下的故障恢复和集群。

- **如何进行虚拟机备份？**
- **虚拟机备份有哪些选择？**
- **如何建立故障恢复体系及配置集群**

安全性

无论你是否相信，虚拟化在安全性提升方面有很大的潜力。有了虚拟服务器，隔离不稳定或妥协的应用更容易。而且，虚拟服务器提供了更迅速的灾难恢复解决方案、强大的取证分析能力以及更廉价的入侵检测工具。

- 专家：利用虚拟化提高安全性（上）
- 专家：利用虚拟化提高安全性（下）

迁移与技能

IT 行业正在朝着 64 位计算迁移，不过迁移很慢，需要大概 10 年的时间。怎么利用虚拟化来简化这个过程呢？那管理虚拟环境的专家所需的 IT 技能与传统 IT 所需技能有什么差别？

- 使用虚拟化简化 64 位计算的迁移
- 虚拟化专家需要具备什么样的 IT 技能？

更多信息

想了解关于虚拟化安全的更多信息吗？请参见以下专题：

- 服务器虚拟化安全
- 虚拟化安全

如何测量虚拟机性能？

追踪虚拟机（VM）性能以精确地找到问题或得到资源消耗的报道，这是一项非常复杂的任务。这是由于虚拟机的行为从严格意思上来讲，与下面的主机相关联，不过也因为性能严重依赖于其他虚拟机正在做什么。

处理性能测量与报道问题对一个虚拟化采用项目至关重要。在 TechTarget 中国的特约虚拟化专家 Alessandro Perilli 的虚拟化采用系列里，已经覆盖了采纳计划里的其他关键组件，包括容量规划、RIO 计算、备份 P2V 迁移等等。

在性能领域，正如讲到的其他领域，市场目前几乎没有提供真正能满足需求和解决问题的产品。

虚拟化需求新度量

传统的测量数据中心性能的方法不能成功适用于虚拟基础架构。当然，虚拟化服务器与物理服务器相当一致还是完全不同，这是个见仁见智的问题。我们来看一下这种局面。

首先，从内部看，虚拟机提供给所有传统计数器一个性能监控器，因此，如果你仅仅在每个子操作系统安装他们的代理，现有的产品已足够好。

然而在虚拟世界，一些获得的号码几乎没有价值，而其他的根本毫无意义。

一个典型的例子是在 VMware ESX Server 环境里的内存消耗与内存分页（memory paging）。VMware 的旗舰产品 ESX 有一个叫做 ballooning 的特别功能。由于有 ballooning，为了其他的目的，ESX 能暂时使用系统管理员分配给一台虚拟机的一些存储。因此，在任何时刻，包含在 VMware Tools 里的专门驱动可以向子操作系统要求内存，就像一个气球膨胀，释放出空间并马上重新分配给其他需要的虚拟机。当发生这种情况时，操作系统被迫页出，显示出意外的、轻微的性能下降。当一切恢复正常，ESX 释放出气球并将内存归还给最初的机器。

在上述情况下，我们有一个子操作系统报道错误的内存和页文件使用，这可能导致完全错误的关于一台虚拟机如何执行的推论。

进一步说，我们可以很容易认识到那些仅与主机上发生的事相关的一些其他测量有什么意义。

一台虚拟机经常报告太高的 CPU 使用，在这种情况下，我们无法断定该对一个虚拟硬件升级，放置第二个虚拟 CPU，并对改善感到有自信。

有时，一个太高的虚拟 CPU 使用意味着虚拟机在主机级别上得到的服务不够快，这可能需要对 hypervisor 的资源管理或物理 CPU 的升级数量进行微调。这只能通过追踪主机级别的具体价值来发现。

因此，我们需要改变我们的测量方法，但我们究竟需要做些什么？

在一个高密度的虚拟数据中心，一台单一主机上有许多台虚拟机，我们有一个强制性的需要，以考虑相互依赖关系，并追踪整个系统作为一个单一的实体，而不是一个要素的总和。

自从虚拟机与主机之间的关系变得很重要，报道解决方案必须处理每个虚拟数据中心的流动性。无缝地适应在基础架构内的热或冷子操作系统迁移。

最后，也是最重要的，这些产品必须有可扩展性：当管理员必须考虑在成百部署在主机上的成千虚拟机的性能时，报道解决方案必须工作在完全自动化的模式，并提供人们仍然能读的和有意义的智能摘要。

填充一个几乎空白的部分

性能追踪与报道解决方案是现今虚拟化行业的一个空白部分。部分是由于复杂性。也因为仍然只是很小的需求。最后，许多人没意识到传统的解决方案很快变得不合适了。

很明显，虚拟化平台厂商提供加强型的报道工具（不同质量的），不过，现在，没有一家厂商提供给用户一个认真的、专用的解决方案。

现在，我们来看看第三方虚拟化性能追踪产品，不过 ISVs 仅提供了少数产品。下面是我回顾的三种：

Vizioncore 仅仅注重 VMware 的 esxcharter。这个产品提供很多图表和一个虚拟机和主机性能的追踪历史。它是一个非常好的入门级产品。Vizioncore 还提供了一个免费版，给予低预算部门一个适当的能力以了解他们的基础架构发生了什么。

Devil Mountain Software（DMS）尝试用 Clarity Suite 2006 得到更广泛的用户，它支持硬件虚拟化解决方案（VMware、微软，不过仅仅是基于 Windows 的虚拟机），同样支持应用虚拟化解决方案（Softricity 和 Altiris）。Clarity Suite 是一个托管解决方案，更多关注虚拟化工作负荷分析，使用得分系统比较性能。该解决方案在虚拟机与主机度量之间做了一些简单相关性，对容量规划和假设情景很有用，不过，它仍然离最彻底的虚拟化环境报道系统还很远。Vizioncore 和 DMS 都提供了一个 Clarity Suite 免费版本，不幸的是，这个版本在可开展的代理和未来都是非常有限的。

新产品 Netuitive 只侧重于 VMware ESX Server（就像 Vizioncore 一样），不过它提供了创新的功能。例如，SI 解决方案自动配置虚拟机和主机性能创建行为配置文

件，使它们相互联系并用于识别古怪的行为。它们一旦出现，Netuitive SI 就反应，询问 VMware 基础架构是否配置它的资源池，因此，在任何人为干预之前，马上记录性能瓶颈。

展望未来，我认为性能报道是掌握数据中心自动化的首要方面。

关于作者：Alessandro Perilli是IT安全与虚拟化技术分析师，获得了CISSP、Check Point、Cisco、Citrix、CompTIA、Microsoft和Prosoft认证。在2006 年，获得了微软MVP。Perilli是现代虚拟化传道者，并且是著名博客virtualization.info的创立者。

(作者：Alessandro Perilli 译者：唐琼瑶 来源：TechTarget 中国)

使用 VM 管理自动化控制虚拟化混乱

很少有 IT 管理者评估数据中心管理的一个非常重要的方面：自动化的虚拟机（VM）配置。事实上一般来说，所有的 IT 组织都能从查看自动化的虚拟化管理中受益。因此，我们来看看这种能力如何迅速变成一种必需品，在未来几年驱动厂商的产品发展，并看看目前可用的产品。

本文是 TechTarget 中国的特约虚拟化专家 Alessandro Perilli 虚拟化系列“Addressing all phases of virtualization adoption”的一部分，在后面的文章中，我们将说明一些虚拟化带来的安全挑战，谈论灾难恢复、配置集群以及创建故障转移体系。

服务器蔓延到虚拟机蔓延

首先，服务器虚拟化整合物理服务器到一台主机上的能力被看作是降低新服务器不受控制而蔓延的一种实际解决方案。不幸的是，有经验的早期采用者却得到相反的结果。这是怎么发生的？

幸好他们发现在虚拟数据中心部署新服务器的成本节约是可观的，这是由于自动配置现在只需要几小时或几十分钟，而不是以前的几周或几个月。部署的唯一不足之处是物理资源分配给新虚拟机的可用性，并且如果使用 Windows，许可证的费用问题。（当大公司与微软有批量许可合同，后者的影响较小。）

IT 管理者能迅速地突然从计划移动到具体实施。是的，这样的简便通常带来了对基础设施限制的错误感知。

自从多层次架构对建设数据中心似乎降低了复杂度，IT 经理预定了新方案，诸如出于安全、性能或兼容性原因隔离应用。同样，毫不犹豫地为完成测试部署新应用。

在这种情况下，公司通常没有执行严格的政策。虚拟架构，取决于其大小，呈现出意想不到的不同挑战。

例如，比较大的公司仍然尝试了解他们成本中心的虚拟化会计方面。他们拨给部门新资源，不过基础设施管理员不能确定哪台虚拟机在使用以及日后的情况。

小一点的公司没有授权过程，允许给几个人自动配置的能力以加快执行项目，这些人甚至没有专业的虚拟化知识。因此，在短期内，想要一台新虚拟机的人几乎都能简单地组装一台虚拟机并使用它。

在这样不受控制的自动化配置环境里，一般会发生下面三件事：

1.创建和部署新虚拟机的许多人不了解大局，诸如一台物理主机实际能操作多少台虚拟机、一台单一的物理服务器计划宿主的虚拟机数量及某一位置宿主什么样的工作负载最合适。

2.每台虚拟机部署都危害着项目本身，会导致性能问题和整合计划的持续重建。

3.每台虚拟机带有一套操作系统和应用许可，在分配之前需要特别注意，不过却没有得到重视。

因此，公司在没有相关的许可、精确的任务或者甚至主人的情况下部署虚拟机。很明显，这种专门做法将影响虚拟数据中心的整体健康。

自动化的需要

当虚拟数据中心增长，IT 管理者需要新的方式执行一般操作，也需要工具帮助他们在需要时进行向上扩展。

当处理大量虚拟机时，最大的问题是它们的布局。我在这一系列文章中说过多次，正确的分配工作负载是强制性的，以使用给定的物理资源达到良好的性能。

当考虑到主机的免费资源和已经宿主的工作负载时，为一台虚拟服务器选择最佳主机不是件容易的事。这时候，容量规划工具是非常可取的。（详细请参加“虚拟化项目的容量规划怎么做？”）

在每个数据中心生命周期之间手动管理容量非常痛苦。毕竟，决定布局就需要大量的时间。同样，整个环境几乎是流动性的，为主机维护或其他原因从一台主机移动几台机器到其他主机以平衡资源使用。在这种情况下，最佳布局变成一个相对的概念。

在大型虚拟架构的另一个显著问题是定制虚拟机部署。

当虚拟化技术与诸如 Microsoft Sysprep 这样的工具联合使用，使用新参数创建克隆虚拟机和分布它们就很容易，当前的部署过程不好扩展并且只考虑到单一的操作系统。

在大型基础设施，业务单位很少需要单一的虚拟机，更多的是寻求多层次的布局。每次需要部署这些多层次基础设施，IT 管理员必须手动地布置网络拓扑结构、存取权限和服务水平协议等等。

在这种情形下，所需的虚拟机需要简单的定制 Sysprep 赞助商是不可能的：具体应用的安装、与现有远程服务的互联及部署前后脚本运行的执行等等。这是每个虚拟基础设施要执行的所有操作，将损失许多时间。

最后，大多数虚拟基础设施的部署呈现了一个典型的情形，从几个部门测试几个不同的独立项目，源项目将必须即时重新部署和创建。在任何新自动配置上，请求者与管理员都将必须记住所有层级的正确设置与定制。

一个新兴市场

考虑到如今的虚拟数据中心的风险与需求，厂商努力提供可靠的、可扩展的自动化配置工具就不惊奇了。

年轻的初创公司，如瑞士的 Dunes、奥斯汀的 Surgient 和波士顿的 VMLogix，不得不与目前虚拟化市场领导者 VMware 竞争。这是件难办的事，因为 VMware 获得了另一个年轻公司的专业技术和已经可用的产品，这家公司就是 VMware 在 2006 年夏天收购的 Akimbi。

在被收购前，Akimbi Slingshot 就被证实是个功能强大的产品，VMware 花了大量的时间改良它并把它集成到 ESX Server 和 VirtualCenter 解决方案。这种集成是一个重要卖点，因为它平衡了 VMware 客户在一个熟悉的管理环境里已经掌握的技能。

另一方面，每天，IT 经理都在查看未知产品以在混合环境里自动化虚拟机配置。Surgient 的产品（VQMS/VTMS/VMDS）VMLogix LabManager 能支持 VMware 平台，同样也支持微软，不久的将来还会支持 Xen。

除了 Dunes，所有提及的厂商现在都把产品聚焦在自动化配置的最实际的应用：虚拟实验室管理。找到一个优先基础配置能力的承诺很容易，例如多层次部署、部署复本与物理资源调度的增强性定制。当虚拟数据中心已经达到临界物质时，这可能是所有用户在那个时刻所需要的。

在不久的将来，IT 组织将寻求更难找到的功能，像配置授权流管理或许可证管理。

在任何情况下，自治的数据中心仍然离我们很远。目前为止，只有 Dunes 和它的 Virtual Service Orchestrator（VS-O）提供了真实的框架，执行现今的虚拟数据中心的完全自动化。

（作者：Alessandro Perilli 译者：唐琼瑶 来源：TechTarget 中国）

如何进行虚拟机备份？

数据中心资源管理十分复杂。要保证虚拟机始终可用、确保快速的灾难恢复和可靠的故障恢复能力，需要很多技巧。

TechTarget 中国的特约虚拟化专家 Alessandro Perilli 的虚拟基础设施系列可以协助 IT 经理更好地进行虚拟机管理。我们谈到了虚拟化领域的一些新技术，某些领域仍然缺乏有效的解决方案。在本文的第一部分，我们将讲述虚拟机备份的过程。在第二部分，进一步探讨虚拟环境下的故障恢复和集群。

备份

虚拟数据中心的备份和传统的备份没有太大的差别。先在每个子操作系统内安装备份代理，然后在其它位置复制虚拟机的文件、分区或整个虚拟磁盘。

这个方法很管用，但是在虚拟环境下应用这个方法时有一个很大的缺点，因为每台虚拟机使用的是主机操作系统的同一 I/O 通道。所以，如果多台虚拟机同时开始备份，难免会遇到 I/O 瓶颈。

为了防止这样的阻塞，管理员应该仔细地规划好备份，使各虚拟机备份之间有一定的时间差，以防止子操作系统在操作密集期间重叠造成拥挤。

不幸的是，这个方法不具可扩展性。也就是说，当有很多虚拟机时，不可避免的会有备份重叠。因为根据应用需求，如果每个虚拟磁盘数据达到 20GB，那么每个备份可能要花好几个小时，所以难免会出现备份时间上的重叠。

子操作系统备份在恢复时，管理员还有一些事要做。首先重建一台空虚拟机，然后从裸机恢复 CD 启动虚拟机。

冒险的做法

此外，还有一个可选的方案是在主机层做子操作系统备份。

由于虚拟机是一个独立的单个文件，存储于主机操作系统的文件系统内，就跟一个电子数据表或图片文件一样，所以许多虚拟化新手可能认为备份是件非常简单的事。然而，事实绝非如此，备份要比他们想象的困难得多。

首先，虚拟机被认为是开放文件（open file），由一个进程或应用锁定（想想 Microsoft Outlook 的.PST 邮件存档文件）。这些文件只能通过特殊的方式访问——即冻结其状态镜像（我们通常称作快照），然后执行备份。

备份软件只有知道了如何处理这些开放文件，才可能执行备份任务，尽管有时主机操作系统会协助备份。例如，Windows Server 2003 有个功能叫做 VSS（卷影拷贝服务），可以借助第三方解决方案执行快照。

即使是知道如何处理这些开放文件，在执行在线备份时我们仍然还得面对另一个挑战：虚拟机不仅仅是开放文件，还是一个访问整套虚拟硬件的完整操作系统。

每次进行快照时，一切都会停止不动，包括虚拟内存和中断程序。这在虚拟领域里叫做断电，可能损坏子机文件系统结构。

有少数的厂商支持这种方法，即使有一个强大的操作系统在断电时不会造成数据损坏。Vizioncore 是一款支持这种方法的产品，很受 esxRanger 的欢迎。esxRanger 能够在 VMware ESX Server 中执行虚拟机在线备份，而且提供了相当多的自动化过程。

Massimiliano Daneri 发布了有名的 VMBK script，尽管它们不支持这种方法，但还是勇敢地尝试了这个方法，也可以为 VMware ESX Server 虚拟机执行基本的在线备份。

微软将从知名的 Service Pack 1 开始，为它的 Virtual Server 2005 提供这种支持。不过，不会允许使用标准 Microsoft Backup 做备份。

最常用的备份方法

通常被接受，而且唯一真正被虚拟商认可的虚拟机方法是挂起或关闭正在运行的虚拟机，然后执行备份和恢复或重启虚拟机。不幸的是，这个过程与具有高可用性的服务相抵触，使管理员不得不利用传统的基于代理的备份方法备份关键任务虚拟机。

当操作系统更加适应虚拟化之后，在线备份问题最终将会得到解决。不过，值得注意的是，这第二种方法也会给主机 I/O 通道带来一定的压力。

为了彻底地解决这个问题，我们必须将备份点从主机改为存储设施。在存储设施中操作虚拟机文件不会直接影响虚拟化平台。

VMware 是第一个使用这个解决方案的，不过现在它的产品 VMware Consolidated Backup（VCB）有很多值得注意的限制：只对 ESX Server 可用；只能作为第三方备份解决方案代理（使得用户不得不为不同产品配置和安装不同的脚本）；而且它不能执行恢复过程。

在存储层，还有一种不同的备份方法：利用存储区域网络（SAN）管理软件和 LUN 克隆。通常，这个方法提供的粒度（granularity）不够，因为存储设施不能识别 LUN 格式，因此不能提供单个虚拟机备份。

LUN 格式识别取决于我们购买的存储管理软件，以及支持何种文件系统。它可能识别 NTFS 格式的 LUN，允许我们备份 VMware Server 的 Windows 虚拟机。然而，它可能不支持 VMFS 格式，我们就无法备份 VMware ESX Server 虚拟机。

如果 LUN 格式无法识别，或者我们没有任何好的存储管理解决方案，我们将只能克隆整个 LUN。LUN 内包含多个虚拟机，即使只有其中一个虚拟机需要恢复，我们也只能同时恢复所有虚拟机。

（作者：Alessandro Perilli 译者：涂凡才 来源：TechTarget 中国）

虚拟机备份有哪些选择？

文件备份：一方面，我们都知道它是标准操作的一个重要组成部分。为了防止严重的数据丢失，花点时间更新恢复是值得的。然而，做备份是很繁琐、费时的，而且通常很无聊。虚拟化在某些方面很有用，而在其它方面却使问题更加复杂化。在这里我们介绍一些虚拟环境下与备份有关的选择，重点是微软产品以及解决方案。请注意，这里的大部分信息对任何虚拟平台都同样适用。

为每个工作量做文件备份的要求

由于并不是所有的虚拟机都被创建成一样的，因此不同的操作系统、应用程序和服务有不同的备份要求，确定这些要求对于管理备份是一个很好的开端。下面的表格中列举了考虑因素以及每个工作量或虚拟机的备份要求：

因素	要求	备注
可接受的数据丢失量	备份频率	细节将影响存储空间的要求
可接受的宕机时间	恢复数据的最大化窗口	有助决定是否需要进行完整VM备份，或者在坏的情况下是否有时间重新安装子机OS
数据量	保留备份的存储空间	总数据量将基于是否子机OS将包括在备份文件内
备份保持期	保留备份的存储空间	越长的保持期将需要额外的存储。异地存储将需要可移动介质
自动故障转移	确认子机O，主机OS，以及/或者对集群或其他高可用性选择的虚拟平台支持	基于工作量的细节，有可能需要高可用性特性的多种类型
预算	最大化存储资源利用的同时，最小化硬件和存储空间利用的需求	将对每一个工作量限制备份可选的类型

在这些原则中一定要包含商业代理和应用程序用户，以确保满足要求。它通常是一种像这样的协商过程：“你确定测试/开发虚拟机需要 99.999%的运行时间吗？这是成本。现在 99.99%看起来更好，对吧？”

子机和主机备份

虚拟机备份主要有两种方法：为每台虚拟机分别备份或在虚拟主机服务器层备份。要在子机层备份，就要在每个支持的子机 OS 安装备份代理，然后选择需要保护的数据。如果这样备份，虚拟机与物理机就基本上是一样的。你可以只备份必要的数据以降低对存储空间的要求，但是你的备份方法必须支持子操作系统。

主机层备份包括复制整个虚拟硬盘（VHD）的文件以获取 VM 的所有内容。这个方法提供了恢复 VM 的最简单的途径（一般你只需要把 VM 重新附到机能主机服务器），但是

这样很费存储空间。记住，你将自动存储子机操作系统和它包含的一切内容。VM 在使用时 VHD 文件被锁定为独占读/写。因此，有一个备份的办法是关掉或终止 VM，然后复制必要的文件，重启 VM。但是这样需要关开机。

自动备份操作

微软虚拟服务器提供了一个简单的日常备份操作方法，只需要几行代码（用 VBScript，VB.NET 或 C#）就可以使备份过程自动完成。一般你的 VM 关开机的时间会只有几分钟（复制 VM 相关必要文件到本地或网络所需要的时间）。这样备份每天就只需要几分钟，但是不是所有的应用程序都支持这段关开机时间。

微软系统中心数据管理员（DPM）

该产品的名称叫起来并不顺口，但 DPM 支持微软虚拟服务器 2005R2 SP1。它使用一种叫做持续数据保护（CDP）的方法进行频繁的基于快照的文件备份。为了保护 VHD 文件，DPM 用微软的 Volume Shadow Copy Services（VSS）获得整个虚拟机的备份。这不需要任何关开机时间，并且把影响了降到最低。它通过检测数据块间的差异从而最大限度地降低存储空间要求。这个方法让你可以更频繁的备份而不用担心使用过多的存储空间。如果需要的话，你可以返回到任何一个特定的时间点。DPM 管理工具让批量主机和虚拟机的管理变得简单。该产品不是免费的，但它可以简化备份过程，物有所值。

总结

文件备份在 IT 领域是一个不可避免的苦恼，执行和支持文件备份可能是非常痛苦的事，而且 VM 的使用并不总是会使事情简单化。值得庆幸的是对于确定何时及如何备份文件我们有多种选择。很可能你会结合使用子机层备份、主机层自动备份和像微软系统中心数据保护管理员这样的附加产品来达到你的目的。当然，最重要的是为每台 VM 确定业务要求。根据经验，做文件备份宜早不宜迟，不要等到关键数据丢失了才备份。

（作者：Anil Desai 译者：涂凡才 来源：TechTarget 中国）

如何建立故障恢复体系及配置集群

虚拟数据中心的高可用性（HA）是一个多层次的任务，它涉及到在线备份（live backup）、故障恢复功能或集群等等。在本系列的上部分中，我们已经谈到了虚拟机备份。在本文中，TechTarget 中国的特约虚拟化专家 Alessandro Perilli 将探讨如何在虚拟环境下配置集群（cluster），建立故障恢复体系（failover structure）。

虚拟化的高可用性有两个层面。我们既可以在子机层操作，依赖 OS 和应用灾难恢复能力；也可以在主机层操作，从而面对一系列新的问题。

在子机层执行 HA 配置的过程几乎与在物理机环境下一样，需要解决一些技术问题。例如，为每个虚拟网络接口设置静态 MAC 地址。此外，还需要突破一些限制因素，这些限制因素取决于所选的虚拟化平台和 HA 软件。不过，虚拟集群创建基本上都是可以完成的，甚至可以创建混合式（mixed）虚拟集群。在混合式虚拟集群中，有一个或多个节点是虚拟机，其它节点则均为物理机。

主机的高可用性更有必要性，不过也更加复杂。在这样的情况下，以故障恢复为例，运行于主机中的虚拟机必须被复制到另一台主机，而且要保持持续性同步，复制虚拟磁盘和虚拟内存修改。这个操作与在线备份有同样的问题，而且还更加复杂，需要尽可能快、尽可能多地重复进行此操作。

这样，Vizioncore 再一次成为了主角。它有 esxReplicator，能够将正在运行的虚拟机从一台 VMware Server 复制到另一台 VMware Server，而且不需要集中存储设备。不幸的是，这款产品不能处理网络修改（network modification），而执行故障恢复时需要用到网络修改，所以我们只能手动切换出错主机和冷备份（cold standby）主机。

VMware 自身也提供了一个更加强大的解决方案，推出了 ESX Server 3 和 VirtualCenter 2，这是一个基于 VMotion 的故障恢复选项。VMware HA 不像 Vizioncore esxReplicator，它可以自动重启出错主机中的虚拟机。不过很遗憾，VMware HA 在配置方面非常费力。它必须要有 VirtualCenter 和 VMotion，而且虚拟机必须存储于光纤通道 SAN 环境，否则它就无法工作。

其它高可用性方法

另一方面，P2V 迁移工具可以帮助我们执行 P2V 迁移。因此，我们可以配置 P2V 迁移工具，以便复制虚拟机到其它主机。

在这种情况下，PlateSpin 是一个比较好的选择。它提供了 Windows 操作系统的动态迁移功能（live migration）。此外，还可以利用这个技术进行灾难恢复。然而不幸的

是，PlateSpin 跟 Vizioncore 一样，也不能处理故障恢复的每个方面，所以我们还得手动干预。

使用故障恢复固然是个不错的方法，但是最可取的 HA 配置方法毫无疑问当属集群。在集群中，多台主机担当共享虚拟机的一个执行前端。如果其中一个主机出错，不会造成服务中断。因为还有其它主机可以正常工作，虚拟机总是可用。

利用虚拟化平台的自身功能或第三方解决方案，我们可以在主机层执行集群。

例如，在 Microsoft Virtual Server 中，Windows 是主机操作系统，微软允许通过 Cluster Service 执行虚拟化物理节点集群。

相反，VMwareESX Server 没有这样的功能。不过，它有一些外部解决方案可以完成这个任务，如 Symantec Veritas Cluster Service。最近 EMC 公司发布了 Rainfinity，这让我们看到了希望，有一天 RainWall 技术终将可以用于执行 ESX 集群。

目前，虚拟化集群解决方案还远不够成熟，在采用之前一定要进行严格的测试。

更多难点

故障恢复和集群配置的结构也十分复杂。虚拟机在主机之间迁移时，它们可能有不同生产厂家的 CPU 服务，这些 CPU 可能比较相似，但并不相同。而且，现有的虚拟化平台仍然无法实时处理动态迁移过程中的这些差异。

同样，如果各个可用主机的配置不同，虚拟机的虚拟磁盘分配（例如，一台虚拟机有 4 个虚拟 CPU）可能无法得到满足，从而无法执行迁移。

这种情况不久还可能变得更糟糕，这取决于生产商如何支持准虚拟化（paravirtualization）。这种方法需要新一代的 CPU 才能运行主操作系统。如果虚拟化平台不能同时运行普通的二进制译码（binary translation）和准虚拟化，或者不能准确地在两者之间进行切换，那么我们就不能混合使用新老物理服务器。换句话说，我们每次购买新配件后就必须翻新全部硬件基础设施，或者谨慎地考虑如何集合主机，从而获取高可用性。

最后一点也很重要，我们必须允许可信存储设施访问，这显然是最关键的一步。这一步通常是由称作多路径（multipathing）的软件完成的。当主机有两个或更多 HBA（主机总线适配器）以访问多个 SAN 时，存储管理软件能够动态选择可用连接，而不会选择出错连接。

在驱动层安装软件有一定的局限性。根据你所选的虚拟化平台不同，你可能不能安装驱动。例如，VMware ESX Server 现有的架构就不允许存储商安装它们自己的驱动，而 VMware 自己提供的驱动又不支持动态多路径。

在选择托管解决方案（hosted solution）时，如 VMware Server 或 Microsoft Virtual Server，你的判断依据是操作系统，而不是是否支持 OEM（原始设备制造商）的驱动，因为 OEM 的驱动始终是被支持的。

（作者：Alessandro Perilli 译者：涂凡才 来源：TechTarget 中国）

专家：利用虚拟化提高安全性（上）

关于服务器虚拟化是否能够降低维护成本，引发了许多议论。它减少了服务器蔓延、降低了购买的软硬件数量、节约耗能以及减少了维护工作。但是，这些都不是用户和厂商对虚拟化技术感兴趣的唯一原因。

无论你是否相信，虚拟化在安全性提升方面有很大的潜力。有了虚拟服务器，隔离不稳定或妥协的应用更容易。而且，虚拟服务器提供了更迅速的灾难恢复解决方案，强大的取证分析（forensic analysis）能力，以及更廉价的入侵检测工具。

下面，TechTarget 中国的特约虚拟化专家 Alessandro Perilli 将探究所有这些虚拟化的应用，看看虚拟化变革在今后将如何影响安全性的提升。在第一部分中，我们会涵盖沙箱（sandbox）、灾难恢复、高可用性以及取证分析等方面的虚拟化应用。在第二部分中，将进一步探讨一种叫做蜜罐（honey potting）的技术，以及虚拟化的未来。

沙箱

虚拟化对安全性提升最简单的应用即是应用隔离。

在虚拟机中移动一个任务或一组应用对 IT 经理来说很管用，可以帮助他们控制两类问题：应用不稳定性和应用妥协（application compromising）。其中，应用不稳定性可能导致严重的资源浪费，最坏的情况可以导致整个系统崩溃。应用妥协则可能导致本地权限扩张和未经认证的系统占用。

VMware 公司作为现代虚拟化技术的先锋，提出了避免以上两种问题的最佳解决方案。同时，作为“虚拟化设备（virtual appliance）”概念的首批推崇者之一，VMware 公司还发布了浏览器设备。这个浏览器设备在虚拟机中的作用相当于操作系统，处理一些因特网相关的任务，如冲浪、邮件阅读、聊天、P2P 网络资源下载等。所有这些动作都非常关键，万一有漏洞，攻击者将可以在 VMware 浏览器设备中与底层主机操作系统进行交互，访问重要的用户信息或访问公司网络。

有了虚拟化，恢复妥协系统（compromised system）也更加容易。用户即使没有相关技术，也可以轻松地重启虚拟机，返回到起始点，几秒钟就可以恢复一个崭新的系统。

这些年，许多安全分析师都对虚拟化表示怀疑：利用虚拟层真的可以安全隔离虚拟机与虚拟机、以及虚拟机与主机操作系统吗？他们的质疑是有道理的，因为虚拟机监控器（VMM）总是处理虚拟机的 I/O 请求，有问题的请求可能会导致缓冲区溢出，进一步导致 VMM 所在的主机操作系统妥协。不过到目前为止，还没有报告记录有成功攻击 VMM 的案例，所以时间会告诉我们，当黑客们利用这个漏洞时会有什么后果。

灾难恢复和高可用性

在任何公司环境下，IT 部门最急迫需要的就是数据保护和服务可用性。

目前，我们要进行数据保护的办法就是在受保护服务器内的文件级进行备份。这个方法有两个大的缺点：数据恢复需要大量时间；公司需要最初的硬件（或是拷贝）才能恢复业务，以免并发其它问题。

虚拟化大大地减少了灾难恢复所需的时间和成本。主机级的备份解决方案不是保存文件，而是复制整台虚拟机，即使虚拟机正在运行也可复制。这种备份得到的是一个非常大的文件，在用它执行恢复时远远要比重新安装操作系统和恢复数据节省时间。

也许你觉得这听起来不错但革命性不够。请你注意，你可以在任何主机操作系统、任何满足供电需求的硬件上恢复保存的虚拟机。甚至，你不用太多停机时间就完成恢复物理出错。

如果停机时间完全超出承受能力，我们有两个选择：高可用性配置和热待机（hot standby）配置。在高可用性配置中，多个集群节点分担、平衡通信负荷。在热待机配置中，有一个或多个第二节点随时准备顶替出错的主要节点。这两个解决方案都依赖于两个或更多物理服务器的可用性。你必须为所有需要保护的服务增加很多服务器。不过虚拟化可以帮助提供一些服务器能力，并且价格较便宜。

每天都有越来越多的公司在部署混合式集群服务，即第二节点是虚拟的。这意味着它们在物理硬件中安装主要节点，而第二节点在虚拟机中，随时准备顶替出错节点。由于备用节点不消耗资源，所以单主机的物理机可以储存多个备用节点，在故障恢复时为虚拟节点动态提供足够的物理资源。

在热待机配置中经常会有一个问题，它与物理节点到虚拟的备用节点的数据复制有关。Vizioncore 等有些公司正在填补这个空缺，为大多数常用虚拟化平台提供复制服务。

取证分析

虚拟化在安全性方面的另一个久负盛名的应用就是取证分析。

VMware 的主管总喜欢提及某些往事，例如执法机构（如 FBI）早期如何采用本公司的产品，询问他们如何拷贝犯罪的硬盘内容到虚拟机，以便异地分析其内容。

如今，这种方法被称作 P2V 迁移，很大程度地实行了自动化。它可以创建一台工作的物理计算机，包括隐藏或加密的分区，而且不会改变任何数据。

在大多数情况下，这个过程很简单，能在几分钟之内通过传输所有硬盘内容（根据其大小，所需时间有所不同）。这个方法有个缺点，就目前而言，我们仍然必须关闭原来的机器。对安全性技术人员来说，这就意味着会失去非永久性存储器（compromised environment）内容。

到目前为止，主要的 P2V 解决方案提供商有 Leostream、PlateSpin 和 VMware 等公司。有些新进入的商家提供一些免费的迁移工具，也在这个领域占得一席之地。传统的影像（imaging solution）解决方案，如 Symantec LiveState 也采用了这个方法，因为最新的虚拟化产品可以在空虚拟机中输入私有格式（proprietary format）。

P2V 迁移并不是利用虚拟化做取证分析的唯一途径。简化虚拟机内测试的最好工具是快照，它也是取证分析的最佳工具。

所谓快照，其实就是虚拟化产品冻结操作系统镜像，以允许恢复妥协环境（compromised environment），尤其是测试版或不稳定的产品。执行快照时，不用管虚拟机关闭与否。如果虚拟机已关闭，虚拟硬盘的所有内容将被标记为恢复点；如果虚拟机正在运行，那么整个非永久性存储器将被保存到镜像文件。

考虑到不断进行的信息泄露（compromise），我们还面临着叫做“零日（zero-day）”工具的威胁。这些工具能够通过更新的恶意软件引擎开发新漏洞而不被发现。通过它们，黑客可以清除日志文件并删除他们使用过的工具，从而掩盖他们的踪迹。

为了减少重要信息的丢失，目前我们主要依赖于基于主机的入侵检测系统（HIDS）。它可以追踪文件、内存变更，并将它们通过网络发送到专用的日志记录设备（logging facility）。然而，这些工具不仅非常昂贵，而且很浪费受保护服务器的资源。此外，并不是每台我们想保护的服务器都有必要部署这些工具，而且入侵检测系统也可能被利用。

在这种情况下，虚拟化是一个既便宜又有效的替代方案。如果快照时间正好，可以把“零日”工具冻结在 RAM 或磁盘中，也可以冻结黑客攻击在系统日志文件中的踪迹，因为黑客还没来得及清除这些踪迹。即使是在数据中心的不同主机操作系统中，也可以在快照点重启虚拟机，这提供了前所未有的取证分析能力。

在本文的第二部分，请继续阅读关于蜜罐以及虚拟化在安全性领域的未来的内容。

（作者：Alessandro Perilli 译者：涂凡才 来源：TechTarget 中国）

专家：利用虚拟化提高安全性（下）

在第一部分中，TechTarget 中国的特约虚拟化专家 Alessandro Perilli 会涵盖沙箱（sandbox）、灾难恢复、高可用性以及取证分析等方面的虚拟化应用。在第二部分中，我们将进一步探讨一种叫做蜜罐（honey potting）的技术，以及虚拟化的未来。

蜜罐

目前，安全领域的研究人员投入了大量的时间对蜜罐（honey potting）技术进行研究。

蜜罐是一个系统，其行为看起来很像一个生产环境。这个系统部署在公司网的特殊位置，包含很多有吸引力的数据，用于引诱黑客。然而，系统内布满了日志探测器，其任务是尽可能多地发现新型黑客工具和黑客技术，尽量欺骗攻击者，以便安全管理员有足够的时间修补真正的系统，从而有效防止新型攻击。

在虚拟化技术成为主流之前，仅仅为了安全性研究而设立一台机器或整个网络（密网）几乎是不可能的，因为其高成本和管理都难以负担。而现在，我们可以借助免费的虚拟化平台，免费的流量发生器（traffic-generator）工具和虚拟实验室自动化解决方案（如 Akimbi Systems 公司或 Dunes Technology 提供的解决方案）。建虚拟密网最终成为可能，而且负担得起。企业应该评估这些系统的部署，模拟生产服务器，把密网看作强大的监测传感器（monitoring sensor）。

虚拟蜜罐对桌面模拟、防毒软件无法处理的内部威胁，以及端点安全解决方案仍需解决的内部威胁也都有很好的效果。在微软的 Honeymonkey 项目和 IBM 的 Billy Goat 中都有类似的应用。这两款产品会让虚拟桌面自动浏览网页，然后受感染，从而发现新病毒类型。

蜜罐的虚拟化应用有一个很大的缺点，就是攻击者获得访问权限后，在网络级或系统级运行的单裂（simple check）立刻可以识别虚拟机。检测到虚拟机后，攻击者会立刻离开。如果已经进入虚拟机，便会把这个环境看作一个陷阱。

我们可以从两个方面为这个缺点辩护。首先，许多攻击是自动化的，如网络蠕虫，而且恶意代码还没有如此先进到可以避免虚拟机。第二，从大型企业到中小型企业，越来越多的公司都将生产服务器转为虚拟架构。对黑客攻击者来说，虚拟机不再如以前那样可疑了，他们可能把虚拟蜜罐误看作真实目标，然后留下来开始活动。

未来

现在，虚拟化技术仍然处于早期阶段。各种虚拟化技术都在飞速发展，虚拟化应用也同样日新月异。它们将会更充分地利用计算能力和灵巧的可编程界面。

在不久的将来，从安全性角度来看，虚拟化将带来另一个好处，就是能够回收利用目前安全性软件所浪费的资源。事实上，VMware 和微软允许开放它们的虚拟硬盘格式访问之后，Symantec 和 Trend Micro 等厂商立即申请了访问权限，然后整个安全性领域都一拥而上。

知道虚拟磁盘结构就意味着公司可以从主机级操作虚拟文件系统的文件。换句话说，防毒、补丁和备份软件将不再需要从虚拟操作系统内访问数据，而可以从底层直接访问数据，从而更直接地完成安全任务。此外，要想损害安全代理将不再可能，安全系统在最前沿保护着系统。

沙箱虚拟化应用的概念不久将会更加普及。英特尔发布了新 vPro 技术，使得虚拟化的潜能更加强大。英特尔的处理器将提供两个完全隔离的箱外环境。一个寄宿传统的操作系统，负责通常的计算；另一个寄宿独立安全的环境，负责从救援到入侵检测的一切工作。

Symantec 发布了一款直接利用 vPro 中第二个独立环境的产品。公司可以用它寄宿一个监控器，当标准操作系统被攻陷后可以执行检测，并做出相应的反应，阻止访问网络资源。随着时间的推移，这将成为一个潮流。多家硬件厂商，包括网络接口和内存支持生产商，将在今后的服务器和桌面中提供这种分区功能。

然而，虚拟化辅助的安全性的未来远远不止防毒和修补能力或硬件分区。

今天的虚拟化技术可以应用到很多安全任务中，但是它仍然需要很多定制和手动操作。在今后的几年中，它会更加反应灵敏、自动化，实现真正的自我防卫数据中心。

VMware 是第一个提出将入侵检测系统（IDS）融入主机操作系统层的，这样可以更清楚地分析通信和拦截威胁。

但是，一旦安全检测器被放在主机层并能够与虚拟架构进行编程式交互，它除了会做一些本职工作以外，如像 IDS 那样警告攻击或像 IPS 那样结束恶意会话外，还会做更多其它的事。

例如，入侵检测传感器可能会在端口扫描被识别后立即要求运行虚拟机快照。根据快照时间，入侵检测传感器可能为妥协（compromised）虚拟机或受攻击内存的冻结提供安全的恢复点，然后将妥协虚拟机或受攻击内存冻结发送到安全部门做取证分析。而且，为了避免相同攻击，传感器可以从主机级开始执行透明虚拟机的补丁。

在另一种情况下，入侵检测传感器识别攻击后，可以将攻击的通信连接转向另一个虚拟网络，而这另一个虚拟网络就是设计好的专用虚拟机或蜜罐，随时准备接受攻击，并记录下任何零日工具和攻击者使用的黑客技术。

尽管大家对虚拟化技术的期望很高，但是前进的道路也不并是那么容易。其整个前景取决于两个因素：整个数据中心不得不转向虚拟化架构；虚拟机操作所需时间必须更短。

概要

服务器虚拟化不仅仅是服务器整合迫在眉睫的需要，而且将是安全管理员最重要的同盟。它将协助安全管理员简化从灾难恢复到取证分析到入侵检测和防护等大量的工作任务。

在过去大多数复杂情况下，服务器虚拟化可能需要自动化工具。但是今天，利用虚拟化的公司会收到显著的效果。明天，虚拟架构将实现自我防卫，数据中心将实行自我修复。

(作者：Alessandro Perilli 译者：涂凡才 来源：TechTarget 中国)

使用虚拟化简化 64 位计算的迁移

大家大概知道，IT 行业正在朝着 64 位计算迁移。当公司开始发布仅适合 64 位版本的重要产品时，目前这种缓慢迁移将在不久大大加速。如果你现在追赶潮流，你将有较大机会获得明显的性能提升，并走在当今可扩展性需求的前列。

不过，你需要平衡采用 64 位计算相对于迁移复杂性的好处，这意味着采用 64 位计算非常昂贵。为了简化这个过程，我们来看看下一个十年的 IT 现象：服务器虚拟化。

问题

迁移到 64 位计算是冒险的，并需要非常谨慎地计划。为什么？首先，迁移很慢。整个过程完成需要 10 年，在这期间，公司必须处理已经使用了 64 位操作系统的混合环境，不过一些关键应用仍然是 32 位操作系统。

这个过程类似于我们在一个缩小比例的情况下看见的那样：每次我们部署一个新升级的操作系统。来自新技术增强的所有好处通常是不可能达到的，因为一个业务应用或另一个在新平台不受支持。CIO 们有时必须在开始更新基础设施之前等待几年。

在同样情况下，我们在拥抱 64 位技术和它的好处之前可能需要等待几年，直到所有驱动业务的应用移植到新架构，并证明在新架构上是可靠的。这种情形下的等待比等待一个应用从 Windows NT 4.0 移植到 Windows 2000 还长，并且花费更多的钱。

第二个问题来自硬件群体。在产业转换里，提早决定采用 64 位操作系统意味着管理两个不同的架构。不过，最糟的是，这意味着一旦你从 32 位移植应用到 64 位，将拥有无用的硬件。

不可避免的事情

鉴于所有这些问题，很容易认为 64 位迁移是可以避免的，直到它成为一个业界标准。不过，即使你决定推迟，迁移是一个你可能面临的比预计来得快的步骤。

接着，最大的厂商将开始仅仅在 64 位版本提供他们的产品，因为新的架构将可能为用户提供长期需要的最大程度的可扩展性和性能。

微软是踏出这个步骤的第一家公司，宣布了它开发只用在 64 位环境的几款产品，包括流行的 Exchange 邮件服务器、新 Windows 2003 Compute Cluster 版本以及一个 Windows Longhorn 版本。你能预料到在 2010 年左右，32 位产品将完全消失。微软已经为几个重要产品提供了 32 位到 64 位的版本，诸如 Windows XP 和 2003、SQL Server 2005 和 Visual Studio 2005。

巨头软件制造商不并孤单，许多其他厂商，包括市场领导者，如苹果电脑公司、IBM、Novell、甲骨文、红帽与 Sun，都开发或提供了基于新架构的产品，声称达到十倍的性能增益。

在硬件方面，AMD 和英特尔依靠技术都能同时透明地运行 32 到 64 位代码，这两家公司都只销售 64 位处理器给服务器、台式机和笔记本。由于有这些厂商，硬件方面的采用将比软件完成得更早。

虚拟化的好处

为了简化 32 到 64 位混合基础架构的管理，在迁移过程中，服务器虚拟化确实是最佳的办法。在写这篇文章时，还没有适合新架构的虚拟化平台，不过许多平台能运行 64 位虚拟机，这是由于新的 CPU 性能。

市场领导者 VMware 能在它的所有产品里运行 64 位子操作系统，包括 ESX Server 3.0、Server 1.0 和 Workstation 5.5.1。然而，在受支持的处理器上有限制。

AMD	英特尔
皓龙修正版E或以上的版本	
速龙 64 修正版D或以上的版本	Intel EM64T
炫龙 64 修正版E或以上的版本	带VT技术的处理器
闪龙 64 修正版D或以上的版本	

注意，没有识别 AMD CPU 修正版的方法，直到测试它们时，因此，VMware 建议联系厂商以获得帮助。

Xen 3.0 也能运行混合的虚拟架构，Virtual Iron（现在基于 Xen）的 3.0 版本也能运行。

微软将在它的 Virtual Server 2005 R2 里支持 64 位主操作系统，不过，微软已经决定在运行 64 位虚拟机之前等待它的 Windows Server Virtualization。因为 Windows Server Virtualization 在两年内发布，我们能肯定微软的技术对 64 位早期采用者来说不是一个可行的解决方案。

由于 VMware、Xen、AMD、英特尔及其他厂商的进入，我们预料到有个便宜又好用的下一代架构。

取决于你的业务需要，你能使用两个相对的策略进行迁移。

第一种由移动现有的 32 位应用到虚拟机组成，同时在新服务器上更新硬件和测试新产品。这样，当我们决定采用 64 位应用时，虚拟机将担当备用的解决方案，不需要额外的精力去维护两个不同的机组。并且拆除 32 位服务器将进行得更快。

对于那些想要尽快从新架构获益的公司来说，这个策略是最积极的，也可能是比较好的。

相反的方式是维持现有的 32 位硬件群体，并且在测试和验证新产品的虚拟机里谨慎地引进 64 位新应用。如果在某个特定时刻，公司想把应用移回到物理硬件，整个过程非常痛苦。为此，如果服务器整合是这个计划的一部分，就采用这种方式。

在许多情况下，公司将发现同时采用这两种策略是有用的，这取决于他们的部门。

无论你采用哪种策略，如今你只能选择购买安装了 32 位操作系统的 64 位物理主机。幸运的是，这没有影响，因为虚拟化厂商已经提供了 64 位解决方案，我们能改变主机操作系统和虚拟化平台，而不需要重建现有的虚拟机。

并且由于有高可用性解决方案，运营中甚至不会出现业务中断。

（作者：Alessandro Perilli 译者：唐琼瑶 来源：TechTarget 中国）

虚拟化专家需要具备什么样的 IT 技能？

虚拟化技术被采用的比率不断增加，这意味着企业需要能够设计新架构、掌握新工具和分析新结果的专业人员。本文中，TechTarget 中国的特约专家 Alessandro Perilli 将探讨传统 IT 所需技能与虚拟环境所需 IT 技能的一些差别。

许多公司没有意识到，虚拟化技术要求更专业的技能。最后，公司采用系统工程师或架构师的标准去聘用虚拟化专业人员，殊不知操作虚拟系统并非只是与操作系统和应用有关。服务器虚拟专家尤其应该有一份令人印象深刻的简历。在招聘管理虚拟基础架构的 IT 专家时，应该看重什么？本文将对此提供一些建议。

技能全面的价值

普通的系统工程师对一种或多种操作系统有深入的了解，并且具有牢固却有限的网络知识。但是虚拟环境要求更多。现在的虚拟化项目都涉及多种存储、网络和安全性等许多需要认真考虑的方面，无论是从零开始建立新的基础架构，还是迁移已有的物理架构，情况都是这样。可用的硬件更强大，虚拟机自动控制软件愈发成熟，这些方面也将更加重要。

现代的虚拟化专家需要在多方面都具有很强的能力。他们应该了解一些主要技术之间有何差别，例如在存储方面，存储区域网络（SAN）与网络附加存储（NAS）的差异，网络连接方面的 Gigabit 以太网和 InfiniBand，验证模式的 Radius 和 LDAP，还有传统的机架系统与刀片系统的比较。

对于每一个选项，虚拟化专业人员都必须清楚了解预见的实施问题和性能结果，以便能根据客户的需求和预算做出最佳的选择。

显然，这仅仅是招聘经理需要了解的候选人所需具备的最基本知识。在筛选的过程中，还要考察其它更专业的能力。

由于虚拟化还涉及到物理整合，因此企业必须谨慎设计和实行可靠的基础架构。作为一个虚拟化专家，必须要有一些高可用性的不同解决方案，而且熟知每种方案将对虚拟网络、操作系统或应用层有何影响。

同样，虚拟化专家必须掌握多种不同的备份技术，并且十分了解这些备份技术对虚拟机性能和可用性有什么样的影响，以及哪种虚拟产品可以采用哪种第三方的解决方案。

进一步而言，由于虚拟平台难免存在着漏洞，虚拟化专家必须有能力使用不同的脚本语言填补该差距，这就需要他们自己具有一整套的专业技能。

如果某个项目的目标是为数百或上千的现有用户提供一个精瘦计算环境（通常叫做虚拟桌面基础架构或 VDI），候选者就还需要有丰富的终端服务经验，以便能处理好一些复杂情况，因为一个小小的失误甚至会严重破坏业务的生产力。

性能问题

架构师和工程师的最大差别在于他们分别负责完成不同的确切使命：设计好和维护好。为了设计好一个虚拟基础架构，就必须有能力规划出一个具有扩展性、可靠和性能良好的系统。如今，性能问题大概是服务器虚拟项目中最关键的因素了。

对性能影响最大的既不是硬件也不是你选择的虚拟平台，而是部署到每台虚拟机的应用。每台虚拟机都提供一个独立的环境，但是内宿的应用会间接地影响物理资源的整体可用性。例如，有的虚拟机内寄宿着一些很占内存的程序（如 OLAP 引擎），工程师必须为虚拟机预留很大的 RAM 空间，或者有的虚拟机寄宿着许多 I/O 工作程序（如一些数据库），那么工程师就不得不为虚拟机分配专门的物理磁盘。

大体上而言，资源要求不仅要看应用的类型还要看它的设计。常见的是，一个软件解决方案从文字上看起来应该不会太占资源，实际中却相反。这可能取决于产品的内存泄露缺陷情况。

考虑到上述情况，如果没有足够的技术背景，一个虚拟化专家很可能会把多个资源消耗很大的虚拟机整合到一台宿主服务器，从而导致性能下降，而同时其它服务器的资源却未得到充分利用。之后，虚拟机以及其应用所部署的环境特性将进一步让这种操作的后果更加明显。

即使是最小的资源密集型软件，如果同时受到几千个连接访问，要满足它的资源需求也是相当困难的。因此，最好的虚拟化专家都会研究客户的环境如何工作，监控每个应用的工作高峰期，然后规划虚拟化基础架构，不在同一物理机部署相同高峰期的的产品。

由于上述这些原因，所以虚拟化架构师应该对不同厂商的各种应用有丰富的经验（从数据库到邮件服务器，从网络服务器到应用服务器）。虚拟化架构师需要清楚每个产品需要多少资源，它们在正常的环境下如何运转，哪些需要特别注意。

上面所说的这些都是在产品文档中找不到的东西，只有通过多年在数据中心的工作才可以学到。

结论

应用虚拟化的企业需要清楚，其虚拟化员工必须具备哪些技能，这些技能有什么价值。如果只是将新的虚拟化架构师和工程师与传统的系统架构师和工程师进行比较，将严重制约到企业寻找和聘用正确的专业人员。在短期和中期，如果企业的 IT 人员没有先进的技术，将会影响虚拟架构的性能和企业的执行力，从而影响企业的业务，增加昂贵的外

包服务需求。为了避免这些，公司管理层和人力资源部门应该重新考虑一下他们所需员工的条件，了解具有广泛技术背景的真正价值。

(作者：Alessandro Perilli 译者：涂凡才 来源：TechTarget 中国)