虚拟化安全综述

虚拟化安全指南

虚拟化是数据中心的流行技术,它起源于 20 世纪 60 年代。它是把昂贵的计算机资源的利用最大化的方式。典型的服务器运行至少 40%利用率，虚拟化可以更有效地利用技术资源，并节约固定费用。虚拟化的最大优势是，它允许管理员从中央区域为个人电脑和客户设备提供软件。虚拟化不需要管理员对一般任务进行分别考虑。服务器的关机可以带动多用户的关机。

虚拟化安全基础

虚拟化是数据中心的流行技术，而且很有道理。典型的服务器运行至少 40%利用率，虚拟化可以更有效地利用技术资源，并节约固定费用。如果有了 EMC 公司的 Vmware 辅助技术的扩展和一些其他的虚拟化平台，很明显，虚拟化这项技术会迅速发展。

- 了解虚拟化安全
- 虚拟化挑战传统安全概念
- 虚拟化安全未知问题
- 虚拟化安全软件能否保证虚拟化安全?
- 虚拟环境的安全威胁已由理论变为现实

虚拟化和企业风险

虚拟化不是新概念，对它的使用当然也不断有人感兴趣。虚拟化的 IT 架构可以增加系统的实用性和灵活性，而且它对资源的有效利用可以降低所有权成本。例如，Dell 使用的服务器机房运行虚拟软件，在不到 100 个物理服务器上提供超过 1000 个的测试和开发的环境。这就大大减少了设置测试环境的时间。那么虚拟化的使用会增加企业的风险吗？

- 桌面虚拟化是否是企业的现实选择？
- 企业中的虚拟机会增加风险吗？
- 使用虚拟软件会增加企业风险吗？

虚拟化和恶意软件

如果使用得当，虚拟化技术和产品可以很好的防御恶意软件对主机和子机的攻击，本部分中将具体介绍如何使用 VMware 和英特尔虚拟化技术防御恶意软件。

- 利用虚拟技术防御恶意软件
- 使用 Vmware 分析恶意软件
- 使用英特尔虚拟化技术分析恶意软件

虚拟机（VM）安全

虚拟化不给在“客户”机上运行的软件添加任何额外的保护。如果在真实的操作系统中，软件存在漏洞，那么在虚拟机上漏洞也同样存在。这是因为虚拟技术的目标就是为了制造一个和真实系统行为一样的虚拟机器。因此，你必须像对待真正的操作系统一样，加固“客户”机器，给程序打补丁升级。而目前，虚拟化能实现部分隔离功能。

- 虚拟机操作安全问题
- 虚拟机具有什么样的额外安全保护措施？
- 如何确保虚拟服务器环境的安全
- 如何整合物理机和虚拟机的安全

虚拟化利弊分析

由于虚拟机是在独立和隔离的环境中创建的，所以系统管理员能够很容易用各种方法进行配置。虚拟化通常被用来执行备份和灾难恢复。通过虚拟化，跨多种操作系统分配工作负载变得更为简单。而虚拟化的风险存在于如何在一个单独物理计算机上安装各种不同的工作负载。虚拟化不具有兼容性，所以虚拟化的全面部署将会迫使对那些经检验证实可靠的安全控制重新进行修改----这项工作将给 IT 部门和公司员工造成混乱。

- 虚拟化安全利弊分析
- 深入剖析虚拟化之安全利弊
- 虚拟桌面安全软件保障远程客户端安全

了解虚拟化安全

虚拟化是数据中心的流行技术，而且很有道理。典型的服务器运行至少 40%利用率，虚拟化可以更有效地利用技术资源，并节约固定费用。如果有了 EMC 公司的 Vmware 辅助技术的扩展和一些其他的虚拟化平台，很明显，虚拟化这项技术会迅速发展。

通常，安全是事后才要考虑的事情，而且还是一件大事。虚拟化改变了服务器和数据中心的定义。因为反对把明显的物理服务器和网络（推测以被保护或监控的）连接，一个虚拟环境就是一个独立的，设备齐全的“盒子里的数据中心”，当所有过去在网络上发生的程序对程序通信（process-to-process communications），现在可能发生在独立的 IT 场地内部，毫无疑问，安全衍生物将会意义重大。

事实是，没人知道虚拟化将在多大的程度上颠覆过去 15 年中，该行业为建立系统和应用程序防护方面的努力。为了掌握这种局势，理解安全在虚拟世界的不同功能非常重要。

不可能明确地说清楚意义重大的虚拟化安全的机遇是什么，但是有些关键点需要考虑。

- 网路防护无意义----大部分的网络防护都是发生在可见流量上的，数据包与行为和恶意行为相比，然后采取措施。如果流量不可见，就需要在虚拟服务其内部实行基于网络的办法。也就是说，在虚拟机内部或在跨越多个物理机的虚拟架构之间，监控进程间通信。

在虚拟世界中“网络”定义有很大的差异，也需要不同的防护。Blue Lane Technologies 公司和 Reflex Security 公司是两家已经着手解决这个问题的产商，不管结果是什么。

- 管理程序庞大（对于攻击来说）---每个人都在说操作系统是如何地不安全。是的，所有的操作系统都不安全，但是复杂一点的说（朋友之间的复杂）意味着在潜在的不确定的另外的操作系统，也就是管理程序，上堆积整个混乱的潜在的不安全的操作系统。

对于不熟悉虚拟化术语的人来说，管理程序是无遮蔽金属和在上面运行的操作系统实力之间的软件提取层。这是软件，和大部分我们知道的软件的情况一样，它很容易受到攻击。问题是到底有多容易？桩子很高，如果下伏系统受到攻击，可能所有在它上面运行的虚拟机都会受到影响。

如果结果是管理系统可能会受到攻击，那就好像在流沙上面建造摩天大楼。你不需要成为建筑工程师就可以发现这是如何产生的。

- Steroids 上的 结构管理----当每个物理服务器上有 5，10 或者 100 个虚拟设备时，大部分的负担是放在已经存在的结构管理架构上的。给 5000 个虚拟图像打补丁，运行多个不同的操作系统几乎是不可能的。今天的结构管理提供品都必须包含在虚拟世界操作所需的可测量性（和效率）的因素。
- 商业的连贯性是一项挑战---很多的企业都运行备份的服务器，和复制技术，只是以防万一。对于 mission-critical 应用程序，这事做地非常适合，因为停工期费用非常昂贵。但是如果这些关键的应用程序是在虚拟空间中运行的，你的商业连贯性计划需要把这些因素包括进去。

在“过去的又变成时新的”类别中，这是个已经解决的问题。由大型机操作系统解决问题的时代已经过去了。只因为我们以前已经看到了，并且可以找到类似的情况，这并不是说，在这种新情况下，这个问题已经不需要解决了。

- 软件商业模式必须改变----很多软件，特别是管理软件 是按照每个管理设备定价的，但是在虚拟世纪，什么是管理设备呢？制造出的每一个虚拟图像都需要付费吗？图像改变的时候，要发布信贷吗？我没有答案，但是我可以说的是，价格现状是不够的。

我们会看多虚拟化会产生软件间隔模式的出现。

这些问题的答案可能早了些。我知道，有很多聪明的人指出了这些问题，并在市场上推出了新的产品来解决这些问题。

（作者：ike Rothman　译者：Tina Guo 来源：TechTarget 中国）

虚拟化挑战传统安全概念

毫无疑问你会听到有人怀疑传统的安全控制在虚拟环境中的作用。尽管不确定是否有相关的新技术，还是有很多改善安全的方法，可以使攻击者窃取敏感数据变得更困难。

虚拟化向 IT 行业提供对传统安全概念和更有价值的保护业务架构的有力挑战的机会。这些安全方面的好处可以从 IT 行业对于应用环境配置、漏洞管理的更简单的程序以及把原始的应用图像向企业的所有端点的快速传送等的更强大的控制上实现。

虚拟环境还将面临攻击，但是这些攻击将不只简单地存在于应用环境中，还将在渗透入企业环境中存在更大的困难。在本质上，业务应用的攻击界面充分地降低到了虚拟机——操作系统、可执行应用和配置轮廓——所管理的。

挑战传统的安全方法的第一步是认识到所有的计算机系统都总是处于被恶意攻击的风险之中。没有任何适当的安全技术可以保证技术架构的完全安全。虚拟系统对化妆成授权软件来窃取数据或者修改配置中端业务的攻击比非虚拟系统并不具有更大的免疫力。虚拟化厂商在保护管理程序、执行 VM 的完整性检查的证明以及检测新型攻击方面的友好表示是使这个架构尽可能安全方面正在付出的很重要的努力。IT 行业的机会是利用虚拟化改变商业上的交付应用的方式，以及改变保护商业的方式。

下面是 IT 企业利用虚拟化提供更安全的商业环境的例子：

- 一家主要的金融企业正在参与到保护可以被远程电脑获取的客户数据。采用的解决方案是使数据中心的敏感应用虚拟化。因为在这这种虚拟的解决方案中，机密数据从来不离开安全的数据中心，公司就不用太担心数据泄露。企业没有采用严格的端点安全软件，而是使用了虚拟化来避免客户数据被远程收集的问题。
- 一个地区的能源公共事业需要保证控制系统的持续的正常运行时间。这种公共事业利用虚拟架构有规律的在数据中心轮换控制系统，每天更新关键的虚拟机

（VM）。这种简单方法在安全方面的好处之一是对 VM 的成功攻击的时间不会超过 VM 更新的周期——当 VM 终止的时候攻击也会终止。其他的好处是公共事业可以有效地进行灾难恢复，来减轻对控制系统攻击的影响。

- ✧ 国家服务机构已经使用虚拟化更好地进行远程应用的漏洞管理。机构已经认识到通过在向远程站点发送之前在采用软件更新、补丁、配置管理和对数据中心中的虚拟机的安全扫描收到的管理精力上的节约。IT 提高了应用环境的控制，并可以迅速把新版发送的整个企业。

存在挑战的方面是 IT 必须考虑虚拟架构如何在提高应用能力的同时帮助避免常见的安全问题。虽然安全和虚拟厂商继续生产对攻击弹力更大的产品，但是 IT 也可以使用虚拟化大幅改变攻击表面，使商业受益。

（作者：ric Ogren　译者：Tina Guo 来源：TechTarget 中国）

虚拟化安全未知问题

虚拟化技术正在数据中心这一领域风靡，有其必然原因。典型的服务器其利用率不足40%，虚拟化技术有助于更高效的利用技术资源，并可大幅度降低费用。从 EMC 公司的 VMware 业务和其他一些虚拟化平台业务的扩展来看，这一技术很显然正处于快速发展阶段。

通常情况下，安全性问题只是满足需求之后才考虑的问题，这存在很大的问题。虚拟化技术改变了服务器和数据中心的定义。与物理上独立的、通过网络联接的服务（可以认为这些服务器是安全的，且可以监测的）相比，虚拟环境是一个“装在盒子中”的隔离的、自成体系的数据中心，以往通过网络进行的进程间的通信现在只发生在一个 IT 部件中，毫无疑问，安全问题的影响是非常重要的。

实际上，虚拟化技术会在多大程度上影响工业界在过去 15 年为系统和应用构筑的安全措施还不清楚。为了把握这些情况，了解虚拟化世界中安全功能的特别之处很重要。

更明确的说，还不可能准确地描述出虚拟化技术所面临的最重要的安全性挑战是什么，但是可以从以下几个关键点进行考虑。

- 网络防御变得不再具有实际意义。大多数网络安全防御技术都基于监测数据流，将数据包或其行为与已知的恶意数据包进行比较，然后采取行动。如果不能监测数据流，则需要在虚拟服务器内实现一种基于网络的防御方法。换句话说，监测进程间的通信，这些进程间的通信发生在虚拟机中或是发生在不同物理设备上的虚拟设施之间。

在虚拟化的世界中，网络的定义有很大的不同，且需要不同的防御措施。不管这一问题结果如何，Blue Lane Technologies 公司和 Reflex Security 公司这两家厂商已着手研究这一问题。

- 管理程序对于防御攻击来讲太重要了。每个人都在议论操作系统是多么的不安全。的确，所有的操作系统都是不安全的，一组可能有潜在安全问题的操作系统运行在一个有潜在安全问题的管理程序之上，会使这一安全问题变得更为复杂。

对于不熟悉虚拟化技术的人来讲，管理程序可以理解为计算机硬件与运行在其上的操作系统之间的一个软件抽象层。它是一个软件，和其他我们知道的大部分软件一样，它非常易受攻击。问题是：易受攻击的程度如何？它的栈很高；如果处于底层的管理程序受到威胁，很可能也会威胁到运行在它上面的所有虚拟机。

如果管理程序确实易受攻击，那就如同浮沙之上筑高楼。普通人，不必是结构工程师，也能说出这将导致什么样的后果。

- 配置管理的困难。当每个物理服务器上安装了 5 个、10 个或 100 个虚拟设备时，就会给现有的配置管理设施增加许多的压力。例如，管理 5000 个运行不同操作系统的虚拟镜像几乎是不可能的。当今的配置管理提供的功能在规模（和有效性）方面必须增加一个量级才能适用于虚拟环境。
- 保持业务连续是一个挑战。许多机构使用独立的服务器，并在必要情况下切换到备份系统中。关键任务中的应用，由于工作中断代价非常高，这种做法是合适的。但如果这些关键的应用部署在虚拟空间中，则应改进为保持业务的连续性所做的规划，将虚拟环境这一因素考虑在内。

正如“what’s old is now again”（过去场面再次出现）所述，这是一个已经解决了的问题。大型主机操作系统在过去遇到过这个问题。但是，仅仅是人们过去遇到过这个问题并可以找到一个参考，并不意味着这一问题在新的环境中已经接近解决。

软件的商业模式必须改变。很多种软件，特别是管理软件，以被管理的设备数目为标准收取费用，但在虚拟世界中，被管理的设备又如何定义呢？是不是建立每一个虚拟镜像都要付费？当删除一个镜像时是不是也要留下记录？我不知如何回答这些问题，但我可以说的是现有的定价模式是不够的。

我们将会看到，由于虚拟技术的推广会出现新的软件定价模式。

也许会有解决这些问题的初步方案。我知道有很多的聪明人士提出一些想法，并将新的产品推向市场以解决这些问题。

但是，在列举出所有的关键问题之前，与公司中管理数据中心的员工合作提出具体环境中的虚拟设备的安全规划是非常重要的。通向虚拟化的道路非常有趣--这种感觉有点像刚刚走下过山车之后的眩晕感。

（作者：Mike Rothman　译者：陈志辉 来源：TechTarget 中国）

虚拟化安全软件能否保证虚拟化安全?

安全厂商使用 Vmware 公司刚刚发布的应用程序界面（application program interfaces ，APIs)技术生产软件仍然早了点儿。但是新兴的虚拟化安全市场崭露头脚，面对解决和这项技术有关的风险。

最近进入虚拟化市场的是 Altor 网络公司（Altor Networks Inc），上周该公司发行了一种虚拟安全分析器，可以接入虚拟化交换流量，就是系统管理程序上层。这家公司还计划在今年下半年，发布一款虚拟化网络防火墙。

Altor 网络公司的高级主管 Poornima Debolle 说，当 IT 管理员称许虚拟系统的性能和降低成本带来的收益的时候，人们仍然被它的复杂性所困惑。他说，IT 专家们意识到传统的防火墙和 IDS/IPS 是针对静态的，以边界为基础的物理网络而设计的。

“虚拟化数据中心的开发结合了大量的服务器和流量环境，以前这是和管理以及网络前景完全分离的。” Debolle 说 “虽然很多服务器都有安全措施，但是超过 50%的服务器没有安全防护。我们把它称为虚拟网络的盲点。”

Vmware 公司和思杰公司一直努力解决业界专家和 IT 安全专家所关注的安全问题。去年在 Vmworld 的大会上，行业分析师和安全专家已经看到这项技术的益处了，但是他们怀疑这项技术不易被保护。

很多的安全厂商都参与了 Vmware 的 Vmsafe 项目。赛门铁克，McAfee，IBM 的互联网安全系统部，EMC 的 RSA 安全部，以及 Check Point 软件技术公司（Check Point Software Technologies）都计划使用 Vmware 的 API，开发也可以在虚拟机上使用的软件。

Catbird 网络公司和 Reflex 安全公司是市场上销售虚拟网络的监控设备的小公司。加州的 Blue Lane 技术公司开发了一种叫做 VirtualShield 的攻击防御软件，它可以接入 Vmware 平台。这些厂商也参与了 Vmsafe 项目。

“这些公司是以传统的入侵防御系统建立以来的，传统的入侵防御系统是在孤立的应用软件上运行的。” Yankee 公司的高级分析师 Phil Hochmuth 说，“这些产品将曾经在物理网络上使用的方式复制到了虚拟网络上。”

Hochmuth 说，目前可用于虚拟环境的的安全软件是个很好的开始，但是企业应该关注 Vmsafe 的很多作伙伴开发的产品。这些产品最早可以在夏天面世。

分析师期望市场在明年可以彻底转换到虚拟化软件上。微软也参与进来了，计划发布 Hyper-V，这是基于 hypervisor 的虚拟化软件，可以在 Windows Server 2008 的各种版本上使用。很多厂商注意了微软正在推进企业采用虚拟化的进程，也看到了更多安全产品的需求。

Pund-IT Research 公司的首席分析师 charles King 在一份给消费者的报告中说,微软有机会定义市场。他说，Vmware 仍然占有优势，x86 虚拟化市场相对较小，虚拟化服务器只有大约 10%。

“Hyper-V 应该可以给微软提供向更多的人介绍和定义虚拟化利益的方式。”King 说，“如果 Hyper-V 证明确实如微软声称的那样活跃有利，那么微软在以后的几年里就会成为虚拟化的大玩家。”

(作者： Robert Westervelt 译者：Tina Guo 来源：TechTarget 中国)

虚拟环境的安全威胁已由理论变为现实

从虚拟机中逃逸，一直以来被看作类似于一种黑色操作。你不断的能听到研究人员们研究一些恶意软件样本的传言，而这些恶意软件可以从虚拟客户机逃逸到主机里。与此同时，其他研究人员也在研究一些允许攻击者从虚拟机中逃逸的漏洞。

这些有形的攻击威胁到了虚拟化项目的神圣性，而虚拟化在许多公司里相当流行，因为在服务器整合和功耗方面，它们具有很大的优势。但漏洞利用工具的数量也正在日益高涨，每一个月都会增加不少。

在 2009 年 7 月下旬的美国黑帽大会上，一些研究机构对虚拟机的这一漏洞提出了最为清楚的阐释。Immunity 是一家安全评估和渗透测试的公司，它向外界提供了一个被称为 Cloudburst 的工具软件的详细信息，该工具由高级安全研究员 Kostya Kortchinsky 开发。Cloudburst 目前能提供给装有 Immunity 的 CANVAS 测试工具的用户使用，它利用的是 VMware Workstation 6.5.1 和更早期版本的显示功能 bug，而这一 bug 同样出现在 VMware Player、服务器、Fusion、ESXi 和 ESX [见 CVE 2009-1244，以得到确切版本编号]。

Kortchinsky 在 Cloudburst 的开发中有一些创新的思维，他选择利用的是虚拟机和一些设备的依赖关系（如视频适配器、软盘控制器、IDE 控制器、键盘控制器和网络适配器），从而获得对主机的访问。在黑帽大会上，他向外界做了一次报告，解释了他如何利用 VMware 模拟视频设备的漏洞来进行攻击，他还演示了如何利用主机泄漏到客户机的内存，以及如何从客户机向主机内存中的任何位置写入任意数据。

“视频适配器处理最复杂的数据，”他说到。“它有一个特别巨大的共享内存。”

Kortchinsky 说，相同的代码模拟每个 VMware 产品上的设备。“如果有一个漏洞存在，那么每一个 VMware 的产品上都存在该漏洞，而且通过 I / O 端口或内存映射 I / O 端口可以从客户机上对其进行访问”。 Immunity 表示，Cloudburst 具有可以破坏（corrupt）内存的能力，这允许它以隧道方式在客户机帧缓冲区（frame buffer）之上建立起与主机的 MOSDEF 连接，从而与主机进行通信。MOSDEF 是 CANVAS 工具集里的漏洞利用工具，它由 Immunity 公司创始人 Dave Aitel 开发。

在今年 4 月 10 日，VMware 已经修补了这些版本的漏洞。4 天之后，Cloudburst 发布，并被加入到 CANVAS 工具集中。而正是这一点使得 Cloudburst 与众不同，它不再是一个漏洞验证性触发代码（proof of concept)，这和大多数虚拟机恶意软件不同。

文章写到这里，该安全问题技术部分的内容已经结束了，但作为一个具有购买权力和负责决策的安全经理来说，它对于你意味着什么呢？在两年前经济还没有衰退的时候，这一问题给我们的启示会更多，你会争辩说企业的支出应更多的考虑安全因素，而不是经济因素。因为安全问题可能会影响企业的 IT 环境，而这种影响是可以切身感受到的。

虚拟化的威胁一直是抽象的，理论多于实践。当然，目前还存在着一些不易察觉的、虚拟的 rootkit 技术（如 Blue Pill），但这要求黑客具有对技术的理解天赋，而把一些非常复杂的东西作为攻击的工具对黑客来说似乎是不可行的。专家同时警告说，虚拟环境里有形的威胁已经出现，但对于这些理论性的东西，你仍然不可能制定企业自身战略并购买相应的虚拟化产品。你很可能需要做的就是，跟上虚拟化的趋势，因为它能带来很大的好处，让用户垂涎欲滴。而它的安全性问题将来也会随之来临。

不过，是在未来。

针对虚拟机的攻击已从理论慢慢的变成现实。目前，已经出现了关于虚拟机逃逸的五个 CVE 警报，在 Kortchinsky、iDefense 公司的 Greg McManus 以及 Core Security 公司研究小组工作的基础上，研究人员和其他的攻击者会继续对这一问题进行分析、研究，因此以后出现更多安全漏洞几乎是必然的事情。

专家说，网络不应该依赖传统的安全措施，因为它们不能抵御每个虚拟机的威胁。到目前为止，大多数组织都在反应有关虚拟环境的安全问题，以及不断涌现的新攻击、漏洞利用程序和漏洞验证性触发代码（proof of concept)。虚拟机的安全正处于风口浪尖的境地。

两年前，安全专家、现任思科云和虚拟化解决方案的总监 Chris Hoff 曾说过：“虚拟化的安全威胁和漏洞晦涩难懂，而企业管理层对这些安全问题表现消极，他们认为在部署虚拟化技术的时候，安全问题不是考虑的重点。所以，即使尝试通过建立商业案例来考虑针对安全虚拟化环境的投资，这些努力也起不到多大的作用。”

随着 Cloudburst 被看作最近一次针对虚拟机的攻击，在这一背景下，Hoff 以及其他致力于虚拟环境安全的专家的预言似乎得到了验证。

所以，也是在两年前，Hoff 写了一篇关于某虚拟机漏洞的文章。在当时，攻击者利用该漏洞可以在 VMware 客户端操作系统上运行任意代码。在那篇文章中，他的最后一句话是："这将是针对虚拟机的第一次攻击，以后还会出现更多，这是可以肯定的... 在你必须去重新配置或为你的全球虚拟数据中心（server farms）打补丁之前...你可以开始用这样的例子与管理层讨论进行冷静、理性的讨论..."

未来已经来临。

（作者：Michael S. Mimoso 译者：Sean 来源：TechTarget 中国）

桌面虚拟化是否是企业的现实选择？

问：桌面虚拟化有什么益处？它是企业应该慎重考虑的选择吗？

答：虚拟化是把昂贵的计算机资源的利用最大化的方式，它起源于 20 世纪 60 年代。尽管如此，相对便宜的电脑的出现大幅度降低地降低了虚拟化的成本优势，作为释放 IT 资源的一种方式，这种技术也不再受人喜爱了。目前无止境的升级、不定和其他更新占据了电脑的大量时间。由于管理问题，IT 部门又重新关注虚拟化，把它作为优化 IT 资源的一种方式。

早期的桌面虚拟化完全把操作系统从个人电脑上分离出去，把它放在数据中心，只给用户留下输入和显示功能。最新的桌面虚拟化版本，充分利用虚拟化电脑的力量处理大部分进程。每个用户的桌面上都有在虚拟机上运行的完全的操作系统和应用图像。这样的设置拥有中央管理的优势，而又不需要耗费桌面电量。

桌面虚拟化的最大优势是，它允许管理员从中央区域为个人电脑和客户设备提供软件。管理员可以对多个用户配置标准的桌面图像,比如不停进出网络的活动员工，分支机构的员工和外包服务员工。不遵从法规的虚拟机可以被隔离，这些用户可以被动更新系统。桌面虚拟化降低了定点支持的成本，因为管理员可以更新服务器补丁，而当虚拟机访问应用程序的时候就会自动更新。在降低成本的同时，从中央关闭合作环境的能力也非常引人注意。

桌面虚拟化听以来有点儿像终端服务，终端服务的服务器可以运行应用程序，用户也可以远程访问。但是两者大不相同。服务器可以控制每一位详细用户的整体桌面环境。为了解决负载平衡或者失败事件，虚拟化还增加了桌面环境移动功能以及所需的应用程序。应用程序流提供了更大的灵活性：可以创建基本的操作系统图像，每个单独的应用程序图像可以在不工作的时候根据需要结合在一起。应用程序流大大减少了所需要的独特桌面图像的数量。它也提出了一个很好的主意，就是应用程序许可非常必要。

虚拟化不需要管理员对一般任务进行分别考虑。服务器的关机可以带动多用户的关机。磁盘的应用应该严密监视，因为用户也会使用相同的驱动空间。根据属性，该技术的复杂性增加了，需要新的技巧。虽然虚拟化使得关闭网络环境非常简单，但是它不能消除主机上低等级的恶意软件威胁，比如 keyloggers 和 rootkits，要明了这一点。

（作者：Michael Cobb 译者：Tina Guo 来源：TechTarget 中国）

企业中的虚拟机会增加风险吗？

问：我们公司的一些能源用户对在他们的客户设备上进行虚拟化实验很感兴趣。我们目前的安全政策指导还比较松散。允许客户端虚拟化会增加风险吗？

答：在这里，我假设你说的 “虚拟化”意思是“虚拟机”（VM），这些软件允许一个或多个来宾操作系统运行主机或者系统管理程序。这样，问题实际是你是否可以允许用户把其他的不标准的操作系统带到企业中，并在公司电脑系统上安装。当这些用户安装虚拟机环境，并把操作系统放在上面运行各种应用的时候会发生很多事情。

这不是必然的风险，可能是你不能察觉到这些用户在做什么。这种争论出现在带入企业的系统或者软件的任何奇怪的类型。

所以，这都归结于你对这些用户的信任程度和他们可能作的事情。需要小心监控他们的行为吗？虚拟机，如果以你描述的方式配置，就会被用户完全控制，而他们就成为了这种环境中隐藏的软件包。你可以和这些用户达成一种协议，减少混乱的可能性。例如，你可以选择一套操作系统作为可以支持的虚拟来宾机。然后，可以要求员工在这些来宾机安全安全包，例如杀毒软件和个人防火墙。这样就可以帮助你达到良好的平衡。

（作者：Ed Skoudis 译者：Tina Guo 来源：TechTarget 中国）

使用虚拟软件会增加企业风险吗？

问：虚拟环境和在一个服务器上创建多个应用的系统的安全方面的缺陷是什么？

答：虚拟化不是新概念，对它的使用当然也不断有人感兴趣。虚拟化的 IT 架构可以增加系统的实用性和灵活性，而且它对资源的有效利用可以降低所有权成本。例如，Dell 使用的服务器机房运行虚拟软件，在不到 100 个物理服务器上提供超过 1000 个的测试和开发的环境。这就大大减少了设置测试环境的时间。

经常提到的虚拟化的一个优势是这种技术在企业中简化操作和巩固服务器和计算机数量的能力。但是，管理员将息需要学习如何配置和维护虚拟 IT 环境。不仅需要理解大量的专业术语，而且大部分的虚拟化产品也要求另外的硬件或者软件。这要求里很大量的系统管理程序和硬件，以及每一个应该如何恰当地配置。

一旦创建了虚拟环境，法规和审计就必须也进化到可以处理物理和虚拟系统。这就是说找到一种方法衡量资源的使用和共享架构中的应用的成本分配，因为序列号和物理位置在虚拟世界中都没有意义。记住，如果不能确定虚拟系统上有什么，就不能从它上面获得最大的利益。还有除非使用了谨慎的镜像分类，“image sprawl”和孤立镜像就会造成延迟并打倒 IT 员工。所有这些，不要提可能的 rootkit 管理程序的威胁，都增加了保护虚拟系统安全性的负担。

虚拟化软件可以造成不可预知的错误，而主机是它上面的所有实例失败的可能单点。另外，很多软件应用都提供了有限的虚拟化支持。将来，管理员将需要创建在这样的软件许可中保护现有投入的环境。这个长期过程的另一个挑战是支持虚拟化的认识到许可证模式的优势。为了最大程度上节省，需要全面理解合约和厂商许可权。

尽管存在这些缺陷，虚拟化的优势使这项技术值得考虑。有了虚拟化，IT 管理员可与巩固他们的物理架构，保护在现在有操作系统和应用上的投入，并对硬件投入中获得更多。随着虚拟环境的增长，对商业连续性和生产量管理策略上还会产生一些优势。

（作者：Michael Cobb　译者：Tina Guo 来源：TechTarget 中国）

利用虚拟技术防御恶意软件

问：虚拟产品在防御恶意软件方面有什么作用？

答：如果使用得当，他们可以产生很好的效果。使用现在的攻击技术，只要主机和客户机经过了仔细地修补和强化，受感染的客户机不可能感染基本的主机操作系统和其它客户机。

因此，举例来说，如果需要调查某个特定的恶意软件样本或者浏览某个可能不可信的网站时，可能就会想要使用客户机。首先，在原始的客户机操作系统上设置一个恢复点（也称之为还原点）。然后，再上网或者运行恶意软件进行分析。这样，病毒感染基本系统的可能性很小。运行完恶意软件之后，可以单击虚拟化产品中的恢复按钮，并且恢复到原始系统。为了完成所有这些操作，你甚至可以使用运行免费 VMware Player 产品的 VMware 公司的免费虚拟浏览器应用。然而，限制相当大。要再次恢复到原始的客户机，可以使用 VMware Player，并且只要从原像中导入到客户机应用中即可。

但是这个方法并非万无一失。越来越多的恶意软件都在设法检测其是否在虚拟机中运行。如果精明的恶意软件认出所处在这样的环境中，它就会改变功能，并且隐藏或者改变一些最引人注意的功能。因此，如果你喜欢分析恶意软件，那么可能想要确认恶意软件是否在检测虚拟机。欲了解关于这个问题的更多信息，请查阅我和同事 Tom Liston 共同编写的相关文章（pdf 格式）。在本文中，我们介绍了一些技术，可以缓解对 Vmware 的检测。

要关注的另外一点是也许有一天，恶意代码会跳离虚拟机，从一台客户机转入另一台，甚至进入主机本身。这些攻击很难实现，而且到本文为止，还没有公布可以进行此类攻击的代码。虽然这是个多变的研究领域，但是目前还处于理论阶段。

（作者：Ed Skoudis　译者：Tina Guo 来源：TechTarget 中国）

使用 Vmware 分析恶意软件

即使恶意软件分析不是你的第一职业，你偶尔也会想知道你桌面上不熟悉的恶意可执行软件的属性。行为分析观察与文件系统、注册表和网络相合的样本。使用行为分析开始调查可以快速产生有用的结果。Vmware 等虚拟化软件在这个过程中可以起到不可思议的作用。

使用 VMware 分析恶意软件的优势

VMware 允许模仿多个电脑在单个物理系统上同时运行。和使用清晰物理架构组件的实验室相比，使用这种方法进行恶意软件行为分析存在以下优势：

- 在分析实验室中有几个系统非常有很多好处，这样恶意软件可以和模拟互联网的组件相互作用。有了 VMware，就可以建立多组件的实验室，而不需要笨重的多个物理计算机。
- 可以在感染之前，对系统转态进行快照，并在分析中进行定期快照，这样可以节约时间。这种功能提供了一种简单的方式，可以几乎马上恢复到想要的系统状态。VMware 使用整合的快照功能简化了这项特征。VMware Server 是一种免费产品，只支持一种快照。VMware Player 也是免费的，就完全不可以使用快照。
- VMware 的主机网络很方面和使用没有硬件的模拟网络的虚拟系统互相连接。这种设置也可以降低分析师被引诱把实验环境连接到产品网络的可能性。在混乱的情况下，主机网络允许任何虚拟系统查看所有模拟网络上的流量。这样对样本的网络活动的监控就很容易。

开始 VMware 恶意软件分析

准备 VMware 分析实验室很简单。需要带有足够 RAM 和磁盘空间的系统作为物理主机。还需要必备的软件：VMware Workstation 或者 Server，以及在实验室中配置操作系统的安装媒体。

VMware 可以模拟电脑硬件，所以必须在每个虚拟主机上安装操作系统，而这些虚拟主机都是使用 VMware 的新型 Virtual Machine Wizard 创建的。一旦创建了操作系统，就可以安装 VMware 工具包，它可以在 VMware 内部优化系统操作。然后安装合适的恶意软件分析软件。

我建议在实验室中使用不用操作系统的虚拟机，每个都代码恶意软件可能会攻击的操作系统。这样可以观察本地环境中的恶意项目。如果使用 VMware Workstation。就需要在安全更新安装过程中，在虚拟系统的不同点进行快照，这样就可以在想要的补丁层分析恶意软件

保护产品系统的安全

当处理恶意软件的时候，采取一些预防措施，不要影响到产品系统。这样的泄漏可能在恶意软件处理不合适或者样本攻击 VMware 设置或者从电脑中逃逸的时候发生。在 VMware 中已经公布了一些漏洞，而这些漏洞在理论上可以允许恶意代码从虚拟系统中找到进入物理主机的方法（PDF）。

下面是减轻这些风险的方法：

- ✓ 保持 VMware 安全补丁的及时更新。
- ✓ 把物理主机完全用于 VMware 实验室；不要用于其它目的。
- ✓ 不要把物理实验室系统和产品网络连接。
- ✓ 使用主机软件检测软件（IDS）监控物理主机，例如文件完整性检查器。
- ✓ 定期使用纯系化软件重新给物理主机作图，例如 Norton Ghost。如果这种选择太慢，查看硬盘模块，例如 Core Restore，取消对系统转态的改变。

使用 VMware 进行恶意软件的分析的挑战之一恶意代码可以检测到是否是在虚拟机中运行，这将表明样本已经被分析了。如果不能修改样本代码，排除这项功能，就需要重新配置 VMware，使其更稳定。去年，Tom Liston 和 Ed Skoudis 提供了一些 VMware .vmx 文件设置，可以插入帮助完善。这些设置的最大问题是他们可能降低虚拟系统的性能。还需要注意他们不是 VMware 所支持的。

虚拟化选择和策略

当然，Vmware 不是可以用于分析恶意软件的虚拟软件的唯一选择。常见的替代品包括 Microsoft Virtual PC 和 Parallels Workstation。

虚拟化软件提供了一种简便省时的建立恶意软件分析环境的机制。只要确保建立必须的控制，阻止恶意软件从实验环境中逃逸。在调整良好的实验室中，可以最大程度的使用你的恶意软件分析技巧。

(作者：Lenny Zeltser　译者：Tina Guo　来源：TechTarget 中国)

使用英特尔虚拟化技术分析恶意软件

随着最近几年恶意软件的成熟和发展，研究人员更难分析恶意软件的样本了。很多恶意软件的制造者在程序中增加一项功能，可以检测这些程序是在物理机还是在虚拟机上运行。而这些功能是研究人员用于观察新的恶意软件样本行为的工具。

但是下个月，Black Hat 会议将会发布的新的分析工具可以使善意人士具有优势。Damballa Inc.的主要研究员 Paul Royal 开发了一种叫做 Azure 的新工具。它利用英特尔芯片中的虚拟扩展技术（virtualization extensions，VT）来规避恶意软件对虚拟机和物理机的检查。因为虚拟扩展（VT）存在于硬件级别上，是在主机操作系统级别以下的。恶意软件没有能力检测 Azure，这样研究人员就可以分析未受阻止的行为。

Royal 说：“整体的观念就是规避客户机操作系统，所有恶意软件就不可能检测到你，并发出攻击。英特尔的 VT 不存在 in-guest 方法的弱点，因为它完全是外部的。其它的使用 system emulators，但是如果 emulators 比较机警，一切都会完全正确。”

Royal 计划在 Black Hat 上发布 Azure 的源代码，而且这款工具将可以下载。他已经在过去的几个月里测试了这款工具的效力，发现它在拆封恶意软件方面的性能非常优秀。而这些恶意软件过去包含在数十个通常使用的信息包中，包括到处存在的 UPX 和 Armadillo。Azure 可以拆封他说测试的 15 个样本，而调试工具 Saffron 可以拆封 15 个中的 10 个；恶意软件分析工具 Renovo 则是 15 个中的 12 个。

英特尔的 VT 是在公司一些芯片上增加的延伸技术，可以帮助完成硬件上的虚拟化，而不是在软件层面。VT 技术是为帮助企业更好地使用它们的硬件资源和节省能源而设计的。但是 Royal 说 VT 可以为恶意软件分析师和安全研究人员提供有力的帮助。

他说：“恶意软件所作的是使用物理处理器上的无正式文件的说明。在 VT 中，比较棘手的部分是他们不是为恶意软件分析师而设计的，但是我将会提到的是，它对恶意软件

分析师而言具有绝对优势，以及使用 API hooking 检测全面的 system emulation 的方法。对于你是怎么做的并不明显，所以人们才没有考虑到它。”

Royal 说：“恶意软件已经成为网络犯罪的工具。了解恶意软件的目的非常重要。我们需要了解它的行为，而它的行为暗示了它的目的但是恶意软件的作者也不会不做任何抵抗地放弃他们的工作。”

Royal 说他仍然忙于为 Azure 的以后的新版本增加新功能，包括精确自动化拆封器和系统呼叫跟踪器。他将会在八月 6 日举行的洛杉矶 Black Hat 大会上公布工作的细节。

(作者：Dennis Fisher　译者：Tina Guo 来源：TechTarget 中国)

虚拟机操作安全问题

据虚拟化专家称，尽管在公司环境中引入虚拟机存在很大的复杂性和安全的不确定性，IT 人员还是必须随虚拟化项目前进，并接受这种风险。

虚拟化安全专家 Alessandro Perilli 在 2008 年的 Burton Catalyst Conference 上告诉与会人员说，不要盲目信任虚拟化方法，不要在配置虚拟化技术的时候，使用平常的安全习惯。Perilli 是 False Negatives 的创始人和首席分析师，同时，他还是虚拟化信息博客（Virtualization.info）的作者。

Perilli 说：“你引进新的一层将会增加在系统上的投入，你必须接受这个现实。”

Perilli 说，虚拟化服务器和物理结构要面对同种类的安全挑战。他说，但是 IT 安全人员和管理员必须重组操作架构，以解决环境中的复杂性。

他说“我们的架构中安全防御的薄弱部分是合我们管理操作架构的方法相关的。如果没有强大的操作架构，你就不能使虚拟中心的容量变为动态的。”

Perilli 说虚拟机受到攻击的风险很低，但是在以后的几年中，随着采用范围的扩大，这种风险也会增加。他说，当在环境中增加虚拟技术的时候，你增加的是软件。他指出 Vmware 的补丁发布从 2006 年的 15 个增加到了 2008 年的 70 个。

他说：“安全厂商都不能证明它是完全安全的。”

Intuit Inc.的高级主管 Doug Martin 说他们公司正在测策划准备全能力生产虚拟化技术。Martin 说，受欢迎的 Quicken 和 Turbotax 的制作商计划通过削减一些物理服务器来降低成本。

他说：“我们正在准备全能力生产。我们想要有能力展开，而不限制支持未来技术。”

洛杉矶的社区学院区有几所卫星学院，超过 14 万名学生在这里学习。该区的 CIO，Jorge Mata 说他们团队已经成功配置了虚拟服务器。目前该区拥有 120 台虚拟服务器和 15 台物理服务器。他说，这种配置遇到一些令人头痛的事情，比如区域电子邮件系统的完全崩溃。

Mata 说：“我们经历了重大的失败。我们提前预备了一些东西。在存储方面，我们的准备已经超前了。”

Perilli 说一些厂商将会发布虚拟机生命周期管理软件，帮助公司在虚拟环境中创建强大的认证架构。他说，公司仍然可以从基础开始。他们应该在不同的安全层面上为没有区域设置不同的虚拟主机。他说：“在我们今天的虚拟化平台，不能只在虚拟机内部设置目前的安全层。”

Perilli 说：“虚拟化不是新词。把你知道的拿出来吧。”

(作者：Robert Westervelt 译者：Tina Guo 来源：TechTarget 中国)

虚拟机具有什么样的额外安全保护措施？

问：虚拟机是否具有杀病毒、防止黑客攻击的入侵保护系统等安全技术？如果黑客恶意攻击，攻破虚拟机的防御有多困难？

答：最好虚拟机能做一个和真实系统具有相同安全机制的“客户”系统。这也就是说，虚拟化不在“客户”机上运行的软件添加任何额外的保护。如果在真实的操作系统中，软件存在漏洞，那么在虚拟机上漏洞也同样存在。这是因为虚拟技术的目标就是为了制造一个和真实系统行为一样的虚拟机器。因此，你必须像对待真正的操作系统一样，加固“客户”机器，给程序打补丁升级。

现在，虚拟化能实现部分隔离功能。具体而言，将软件的某一部分放到“客户”机上运行，使它与主机或者另一台“客户”机的其它功能隔离。这需要谨慎小心，因为聪明的黑客可能攻击威胁虚拟机提供的隔离功能。虽然这种概率较小，但不是不可能。如果黑客能够得到运行在主机和“客户”机上的代码，就能创建一个虚拟通道穿过虚拟机。我的团队开发了一个叫做 VMcat 的小工具，可以创建自己的通信通道，在“客户”机和主机之间传送数据。目前，VMcat 需要黑客在“客户”机和主机上都安装而且运行一些东西，所以它不是一个纯粹的 Escape 软件。一个真正的 Escape 软件应该允许黑客在“客户”机上直接运行主机上的程序，突破“客户”机的隔离功能。

到我发稿为止，还没有真正意义上的 Escape 软件公开发布，不过，近期这个领域有一些很有趣的动向。2007 年 7 月，我的团队示范了 Escape 如何破坏一个未打补丁 VMware Workstation 系统。巧合的是，2007 年 8 月，微软发布了 MS07-049，针对其虚拟服务器和虚拟 PC 产品的安全漏洞而发布的补丁。微软称，“可以允许一个‘客户’操作系统用户在主机或者其它‘客户’操作系统中运行代码。”这就是书本里有关“虚拟机 Escape“的定义。同样，到目前为止，无论是针对 VMware 还是微软，暂时还没有发现公开的攻击事件。

面对这些问题，你应该怎么做呢？不断给虚拟产品打补丁更新。VMware 和微软都会定期发布补丁，你一定要及时安装补丁。与此同时，也要加固你的“客户”机和主机，尽量减少攻击者危害虚拟机双方安全的机会。最后，认真仔细架构你的虚拟机部署，尽量降低 Escape 有可能造成的损坏。通过用不同的主机，将那些没有存储重要数据的“弱”机器和存储有价值信息的“强”机器分离开来。不要把你的虚拟机当作防火墙，而是使用真正的防火墙。

（作者：Ed Skoudis 译者：Shirley 来源：TechTarget 中国）

如何确保虚拟服务器环境的安全

对于今天的企业，虚拟机就像是90年代的虚拟局域网（VLAN）交换机：一个使IT简化的变革性技术。它是如此引人注目，在短时间内就能够普及。

不幸的是，天下没有免费的午餐。企业安全团队很大程度上忽略了VLAN的安全内涵。结果，如今渗透测试团队经常可以侵入接待员的桌上型电脑，并直接攻击主机和存储网络，这是一个例子。

计算机行业如何能避免与虚拟化同样的错误？通过跟踪虚拟化发展时的技术，并且站在攻击者的角度思考。这篇文章中，我们将介绍提前在虚拟服务器环境中创建安全措施的方法。

服务器虚拟化需要新思维

首先，停止以目前使用虚拟机的方式思考。该技术今天被广泛配置，但是明天将是普遍的。新的应用软件不会简单地配置在物理硬件上；很快，几乎所有的应用服务器将受一个虚拟控制台的操纵。

以攻击者的角度来看架构：虚拟化控制着企业的每一个应用程序。因此，虚拟基础架构是网络上最有价值的目标。它是攻击者追逐的首要目标。

使用方针和技术

接下来，记住 IT 安全的一个铁的定律：不管有什么样的方针和控件，一些机器仍将会受到损害。应为此制定计划。

在虚拟机之前，那些受到损害的系统会为攻击者提供访问内部网络的权限。有了虚拟机，攻击者不仅可以访问网络，也可以访问任何附属的虚拟基础架构，使所有的虚拟系统——和它们所包含的数据——处于危险之中。

虚拟安全最重大的挑战是，防止访问成为一个“game-over”的威胁，它会威胁到企业中所有其它虚拟机。如何能做到呢？这里有一些策略：

按处理的信息分割虚拟机。不错，高安全虚拟机管理着信用卡号码，医疗信息以及其它最重要的数据。但仍然有大量的虚拟机，用于质量保证和系统测试，这里管理员的密码就是“密码”。指望它吧。不要犯与 VLAN 相同的错误：预先要讲清楚，有一个方针，两种类型的虚拟机决不能共享相同的硬件。然而，今天它也许听起来不现实，假设如果攻击者能在一个虚拟机上运行代码，他们也能在同一台机器上的任一其它虚拟机上运行代码。

留意密码系统。企业使用密码系统的地方比你能想到的更多，像强化 Active Directory 服务器、保护 SSL 连接，以及在 Web 应用程序上产生 session cookies。由于隐藏在基础硬件里的 timing artifacts，虚拟化在保护加密的机密方面是有缺陷的。不要在虚拟化的共享主机上配置金融应用软件。

创建标准锁定图像。在虚拟化下，主机安全意味着更多，因为共享硬件的虚拟机经常能直接互相对话。你的整个就够应当严格地使用一个基线 Windows 服务器装置，或者严格地使用一个 Linux 构造。构造应该锁定为紧密；换句话说，应该坚固，配置最小的痕迹和最大的安全控制。

安全地存储、移动和备份。虚拟机常常以存储区域网络（SAN）技术存储，像 iSCSI；在标准 TCP/IP 网络上移动；使用 FTP 备份。记住所有这些的关键是，如果攻击者能够在传送或者静止时，看见并且改变那些虚拟机位数，攻击者就可以轻松地改写虚拟机，使你的安全系统完全无效。紧密控制对虚拟机存储的访问，就像您对域管理员密码和 SSH 钥匙访问的控制那样。

（作者：Thomas Ptacek　译者：李娜娜 来源：TechTarget 中国）

如何整合物理机和虚拟机的安全

管理和整合物理机和虚拟机的安全-无论在线和离线-无疑都是一个挑战，截止当前，还没有明确的“最佳实践”方法。根据 Gartner 公司最近的研究报告，2009 年，60 %虚拟机的安全性将弱于相应的物理服务器。这一数字突出了确保虚拟机安全面临的挑战，也突显了培训一些能在需要的时候在物理环境和虚拟环境之间转换的管理员的匮乏。

我认为挑战可分为两类：人员和安全工具，或人员和安全工具的缺乏。当涉及到安全管理的人为因素时，尽量避免将物理系统管理和虚拟化资源管理分开为单独的管理结构。如果发生什么事情，IT 部门的人员必须得准备更加密切地工作，否则你会为此浪费时间和资源。在纯粹的物理 IT 环境中，许多角色是独立的清晰明了的，如服务器管理，存储，网络和安全。当服务器虚拟化被引进时，在这个行业仍然在学习虚拟化如何充分影响网络和服务器的安全性景观。现有确保物理服务器安全的策略，技术，配置和实践，根本无法简单地以同样的方式应用于虚拟服务器。比如，安全设备和策略需要消除对 IP 地址的依赖性，因为由于虚拟机的创建、删除或者迁移将引起 IP 地址更加经常地变化。

此外，在虚拟化主机内网络可视性将会有所降低。传统的网络安全工具不一定能看到在同一主机内不同虚拟机之间的通信，这使异常通信的检测变得困难。变更管理程序也应进行检查，以确定如何和何时记录变化。例如，将来的审计员，是需要对主机创建变化日志还是对客户机创建变化日志，或者两者都要？

第二个挑战是寻找帮助确保混合基础设施安全的工具。物理世界和虚拟世界的安全工具绝大多数是不一样的。例如，虚拟机的工具和实用程序在类似 VMware 的环境下运行良好，但他们并没有真正被设计为能复制到综合物理系统中。许多厂商，如微软，戴尔，IBM 和惠普公司正在试图解决这个问题。例如，Check Point 软件技术公司的 VPN - 1 虚拟环境，为物理网络和虚拟应用提供统一的安全管理，允许系统管理员从同一个接口运行虚拟、物理和网络安全任务。重要的是它为包括虚拟环境在内的整个安全基础设施提供了统一的日志记录。这是混合环境审计和遵守的关键因素。

当涉及到的补丁管理，Shavlik 技术公司的 NetChk Protect 现在能为在线和离线的虚拟机、物理机提供集中的补丁程序管理。它也能发现离线的虚拟镜像。赛门铁克公司的

Backup Exec 12.5 支持 VMware ESX 和微软 Hyper- V 的虚拟机和物理机备份，并允许系统管理员使用一个控制台来备份物理机和虚拟机器到磁盘。

毫无疑问，虚拟化显然有许多好处，并能减少了总成本，但是在今后的一段时间内，运行异构基础设施的物理机和虚拟服务器将仍然是一种挑战。企业安全管理人员应及时了解虚拟化系统面临的威胁以及虚拟化在发展过程中的安全创新。

（作者：Michael Cobb 译者：Lily 来源：TechTarget 中国）

虚拟化安全利弊分析

长期以来，企业往往在部署新技术之后，才开始对安全方面进行思考。虚拟化提供了如此之多具有吸引力的优点，所以，很容易被应用到 IT 架构中。但是，使用虚拟化技术需要注意哪些安全问题呢？在本文中，TechTarget 的虚拟化专家 Anil Desai 将针对使用虚拟化技术时存在哪些与安全相关的利弊进行探讨。目的是让你大致了解你应该知道的不同类型的安全问题。

虚拟化技术的安全好处

与在物理服务器上运行相比，在 VM（虚拟机）上运行工作具有众多潜在的好处。这里是对这些益处的总结，并且附有一些简要的解释：

由于虚拟机是在独立和隔离的环境中创建的，所以系统管理员能够很容易用各种方法进行配置。比如，如果某个特定的虚拟机不需要连接到互联网或是其它生产网络，那么配置该虚拟机时，就会对它与其他环境的连通性加以限制。这样，某一被感染的单独系统影响大量用于生产的计算机或是虚拟机的风险就能够降低。

如果发生安全冲突（例如安装恶意软件），虚拟机可以恢复至某个特定的时间点。虽然对文件和应用服务器进行疑难诊断时，这个方法可能不一定奏效，但是，对于包含相对静态信息的虚拟机（例如网络服务器负载）来说，这个方法非常有用。

理论上讲，虚拟化产品是在虚拟机和底层的物理硬件之间增加了一个抽象层。这样能够有助于限制可能发生的破坏量，例如，恶意软件试图修改数据。即使整个虚拟硬盘都被毁坏，但位于主机上的物理硬盘也不会受到影响。这一点对于其它组成部分也适用，例如网络适配器。

虚拟化通常被用来执行备份和灾难恢复。由于虚拟化解决办法与硬件独立开来，复制或移动工作负载的过程能够被简化。一旦发现安全漏洞，位于一个主系统的虚拟机会被关闭，同时，安装在另一个系统的另一个“备用”虚拟机启动。这样，在快速恢复对系统的访问同时，可以为查找和解决问题提供足够的时间。

最后，通过虚拟化，跨多种操作系统分配工作负载变得更为简单。由于受到成本、能量和物理空间的限制，开发者和系统管理员可能会倾向于在同一台电脑上安装一个包含许多组件的复杂应用。通过将不同的功能（如中间件，数据库以及前端 Web 服务器）分布到不同的虚拟环境中，IT 部门可以为每个组件进行最好的安全配置。例如，数据库服务器的防火墙设置可能可以允许与中间层服务器进行直接交流以及与内部的备份网络建立连接。另一方面，通过标准的 HTTP 端口，Web 服务器组件可能能够获得所需的访问。

虚拟化安全的优势远远不止于此，不过，这算是对潜在的虚拟机安全提供了一个简明的介绍。

虚拟化的潜在安全风险

和很多技术解决方案一样，使用虚拟机在安全方面存在潜在的风险。有些风险是系统架构本身所固有的，而有些风险则可以通过改善系统管理得以减轻。采用虚拟机技术普遍存在一个共同关心的问题，就是如何在一个单独物理计算机上安装各种不同的工作负载。硬件故障及相关问题可能潜在地影响许多不同的应用和使用者。在安全领域，恶意软件很有可能给系统资源造成相当大的负荷。这些问题很有可能影响到安装在同一台计算机上的其它虚拟工作负载，而不仅仅影响一个单独的虚拟机。

虚拟化的另一个主要问题是，在虚拟环境中倾向部署许多不同配置的系统。在物理服务器部署中，IT 部门通常会在部署之前执行一套严格的审查流程。他们保证只有得到支持的配置才能安装在生产环境中，并且保证系统符合企业的安全标准。在虚拟机环境下，许多没有支持的操作系统和应用可以由环境中的任何一个用户进行部署。对于 IT 部门来说，通常很难知道他们正在管理什么，更别说如何管理一个复杂的异构环境。

当不同的工作负载在系统上运行的时候，主机的安全变得更为重要。如果一个未经授权的使用者获取了主操作系统的访问权限，他/她便有可能将整个虚拟机复制到另一个系统。如果这些虚拟机里包含敏感的数据，那么这些数据被破坏也只是时间长短的问题了。同时，恶意的使用者可以通过改变网络地址，关闭关键的虚拟机以及进行主机层的重新配置，造成很严重的服务中断。

如果考虑每一个子操作系统的安全性，就必须记住，虚拟机也很容易受到攻击的。如果某个虚拟机能够访问生产网络，那么它通常会具有和物理服务器相同的许可权。不幸的是，它们并不具备限制物理访问的优势，例如通常用于数据中心环境的控制。每一台新的虚拟机都有潜在的安全问题，因此 IT 部门必须确保遵守安全策略，并且保持系统及时更新。

总结

以上分析很可能会给虚拟化安全图景蒙上一层阴影。解决安全处问题第一步是理解某一具体技术存在的潜在安全问题。下一步是寻求解决方案。不过不要担心，总有可以找到降低安全风险的方法。

(作者：Anil Desai　译者：史静 来源：TechTarget 中国)

深入剖析虚拟化之安全利弊

IT 专家已经听到很多基于桌面和服务器虚拟化的安全好处，从更高效的打补丁过程到数据的集中存储（否则，数据就要保存在终端设备中）。但是已经在环境中进行测试的 IT 管理人员同时发现了潜在的安全缺陷，尤其是与其它安全系统的兼容性。

对 John Petrie 来说，兼容性已经是一个主要的挑战。Petrie 是一家金融服务公司的首席信息安全官，该公司有 5,500 名员工和十五个地点。经过辛苦地测试来自几个不同厂商的技术，他发现虚拟化的全面部署将会迫使他对那些经检验证实可靠的安全控制重新进行修改----这项工作将给 IT 部门和公司员工造成混乱。

“采用虚拟化的话，我们已有的集中安全控制不得不改变。”他说，“那将迫使我们改变我们整个对安全的集中观点，令我们的工作暂停。”

对有的人而言，虚拟化存在的缺陷是目前还没有，但将来可能变得严重的威胁。Forrest 研究机构的安全分析师 Natalie Lambert 指出针对 hypervisor 的潜在未来攻击。Hypervisor 是一个虚拟平台，允许多个操作系统共享一个单一的硬件处理器。

“最大的一个担心是，如果在 hypervisor 中发现漏洞，攻击者可以进入位于一个虚拟服务器的上千台台式电脑，那将会发生什么事情？”Lambert 说，“现在这还不是现实，但是肯定是将来担心的一个问题。”

尽管存在这样的缺陷，但多数已经测试虚拟技术的 IT 专业人士表示，虚拟化带来的好处是真实可见的。其关键是需要多挑选厂商，进行认真地调查和研究。

非兼容的挑战

目前 Petrie 准备在公司的电话中心和刀片系统中部署虚拟服务器，但因为考虑到他发现的兼容问题，短期内不可能进行全面的部署。他的计划包括不断的测试和小范围的增量部署。

“我们需要在更低的成本上增加计算能力，所以我们对几个电话中心的应用和消费者数据进行测试阶段的虚拟化。”他说，“基于一些成功的测试，我们计划很快将一些部署向前推进，但是由于存在太多的互操作性问题，我不认为将在企业范围内全面实行虚拟化。”

对他而言，现在最大的局限性是公司基于 IBM 大型主机技术和用 COBOL 编写的薪水和财会应用软件。Petrie 说，没有人能够虚拟一台大型主机，而且基于他的测试，COBOL 语言也无法虚拟化。

Tony Beaird 是 Cinch Connectors 公司的网络基础设施管理员。这家价值八千万的公司为航空业和交通制造业等行业供应连接器。Beaird 也碰到了自己的非兼容问题。目

前他正实施一套新的 ERP 系统，将公司的数据和流程整合到一个统一的系统。根据他的测试经验，他选择通过 VMware 的 ESX Server 对 ERP 和所有必要的相关系统进行部署。

“我认为我们面临最大的挑战是选择合适的 SAN 后端。”他说，“因为我们已经安装了几个 SAN 网络，所以出现了 ESX 3 和已经安装的 SAN 不兼容的问题。该厂商解决了这个问题，但这让我们不得不考虑其他 SAN 厂商是否也有解决方案。”

虚拟化的安全好处

虽然非兼容带来了挑战，以及对未来 hypervisor 漏洞的担忧，但是受访者仍然看到了虚拟化技术为安全性和可管理性的改进带来的巨大潜力。

例如，Beaird 能够通过虚拟系统改善补丁测试和部署过程。“带给我们很大的好处是，在重复的环境中，无需一个单独专门的硬件环境，就能行测试补丁的功能。这对于像我们这样规模的公司来说，通常是很难实现的。”他肯定 VMware 的 VMotion 技术在这方面带来了很大的改进。

根据 VMware，VMotion 利用服务器、存储和网络的完全虚拟化将整个运行中的虚拟机从一台服务器转移到另外一台。如果 ESX 需要打补丁，Beaird 说，他可以简单地将所有的东西从每一台服务器中 VMotion（虚拟移动），进行更新。

Lambert 指出，桌面虚拟化在企业中日渐普及。这些企业看到目前 PC 环境太昂贵，想寻找一种节省成本的方法。但是，在她看来，虚拟化带来的好处更多在于安全性和可管理性。

“采用这种技术你开始集中数据，而不是让数据继续存在于你的终端设备中。”她说，“想一想所有易于存储在手提电脑的数据。不将数据存储在手提电脑内是一个很大的安全好处。托管的桌面虚拟化意味着丢失的手提电脑将不是那么大一回事，因为数据并不在手提电脑内。”

寻找合适的厂商

想采用虚拟化技术的企业大部分都知道 VMware，许多业界专家认为它是业内领先的厂商。Beaird 很满意他购买的 VMware 技术，但他购买初期时，也看过其他的厂商，包括微软。微软在这个市场的产品有微软 Virtual PC 2007 和 Virtual Server。

“如果采用微软的解决方案，我们看到的一个风险是，运行 Virtual Server 的 Windows 主机系统需要打补丁。”Beaird 说，“因为微软不具备虚拟移动虚拟机的功能，所以，不像 VMware，这将需要我们完全中断主机系统来进行更新。”

他的公司决定采用 VMware 主要是顾虑到 Windows 服务器主机打补丁存在的风险。通过 VMware，他的公司安装了六台 ESX 3 服务器，与一个 EMC 的 SAN 共享存储。

Lambert 说，除了 VMware 和微软之外，可以考虑的厂商还有 Citrix 和赛门铁克最近收购的 Altiris 技术。她建议，想在虚拟化进行投入的 IT 部门应该注重安全性和可管理性的好处，而不是可能节约的成本。她说，“短期而言，实施虚拟化是昂贵的。公司应该了解，与该技术相关的成本节约将至少需要三年时间才能实现。”

（作者：Bill Brenner 译者：Shirley 来源：TechTarget 中国）

虚拟桌面安全软件保障远程客户端安全

虽然大多数 IT 人士了解虚拟桌面，而且知道它可以用于数据中心，但这种技术非常实用的一个用途却常常被人忽视。桌面虚拟化现在使用起来非常轻便了，员工可以远程连接到他们需要的应用程序上，同时更好地保证他们的设备安全。

最近我和一个亚特兰大的金融公司谈过，他们使用的是 RingCube Technologies 公司虚拟桌面的安全技术和 McAfee 公司产品的 SafeBoot 磁盘加密功能，从而保证了远程客户端的安全。

安全性，特别是为远程用户强制执行标准配置和设备使用策略的需求，是支持企业的虚拟桌面使用的主要动机。该业务需求是在远程用户通过 VPN 访问企业网络时，能够具备一个安全的环境，同时降低成本。远程用户需要的只是一个 VPN 客户端、基本的电子邮件代理、IE 浏览器、微软 Office 桌面应用程序和一些少量的第三方应用程序。

公司的 IT 部门不用试着去微观的管理每个远程笔记本电脑，而只需管理那些能远程允许访问的核心组件，包括清理可执行的和有效的设备控制策略。IT 有一个牢固的应用程序，可以在虚拟桌面和业务流程上独立于其他可执行文件运行于终端，以减少恶意软件感染的危险。终端用户点击图标就可以启动虚拟桌面，这种桌面是独立运行在本地环境里的。

虚拟桌面可以协助 IT 部门对设备执行一项可接受的使用策略，尤其是对于 USB 接口的设备。远程用户不能随意的把数据放在可移动设备上，这样 IT 部门对设备数据的读取将无法控制，而这可能会影响虚拟桌面的会话（session）。因为策略是集中管理的，所以在必要的时候，IT 部门也可以放松对用户设备的控制策略。

为了防止笔记本电脑丢失后数据的泄密，那些敏感的数据需要被集中的进行全磁盘透明加密。如果一个员工的笔记本电脑丢失或被盗，这种加密可弥补数据泄密带来的损失。

在我与财务公司的讨论中，IT 部门表示，远程用户呼叫帮助台的次数已经减少了很多，因为它配置了虚拟桌面，包括 VPN 软件，从而减少了终端用户在 VPN 配置文件和安装中的错误。

IT 部门还发现，虚拟桌面的一次刷新用时不到一小时，这样每次刷新就能节省大量的时间，总计约 3 个小时。IT 部门表示， 在为远程用户修复软件的时候，对 IT 部门资源需求有所减少。这些远程用户常常会遇到硬件故障、设备丢失的情况，从而购买新的笔记本电脑。

虽然还没有实现，但该公司还希望从终端投资中获得更长期的回报，并密切监控着软件的部署，从而得到更为有利的软件许可。

无论是在 IT 界还是在用户社区中，该公司的经验都是值得肯定的。预计在今年年底，该公司将推出虚拟桌面。Virtual Computer 公司和 Moka5 公司是另外两家专门从事虚拟桌面软件的厂商，它们也为远程客户端的安全要求和业务控制搭建了平台。还有其它一些形式的虚拟桌面，同样也着眼于安全，这包括大型的金融机构在其瘦客户端上运行的 Citrix 系统公司和 VMware 公司的产品。

安全性是一个关键的决定因素，它使 IT 组织注重使用虚拟桌面来控制终端。在这种情况下，公司不仅能够缓解由远程用户数量增加所造成的威胁，也能通过减少昂贵的帮助台请求来节约成本，并延长员工的笔记本电脑寿命。

（作者：Eric Ogren 译者：Sean 来源：TechTarget 中国）