NETGEAR®
Connect with Innovation™

白皮书

服务器虚拟化

面向 SMB 客户的游戏规则改变者

简介

IT领域的每个人基本上都听说过服务器虚拟化，以及数据中心和企业客户在媒体所鼓吹的惊人成就。大型公司在服务器扩展、电源、发热及技术支撑方面都面临着大量的物流和财务的问题。服务器虚拟化可以解决这些问题，并且可以改变测试和开发环境，从而在根本上改变业务连续性和容灾的能力。但中小企业（SMB）市场的“数据中心”可能只是一个由少量服务器和一些旧的网络部件组成的备份安排和非正式运行的IT机架。如此，是否也有类似的解决方案？

市场定义	
小型企业	5-75个用户
中型企业	76-500个用户

简而言之，服务器虚拟化是在相同的硬件平台上运行多个并行操作系统的能力。在大多数情况下，单个操作系统或单套应用只能利用10%可用的处理能力及现行的硬件平台资源。这浪费了大量的硬件投资。

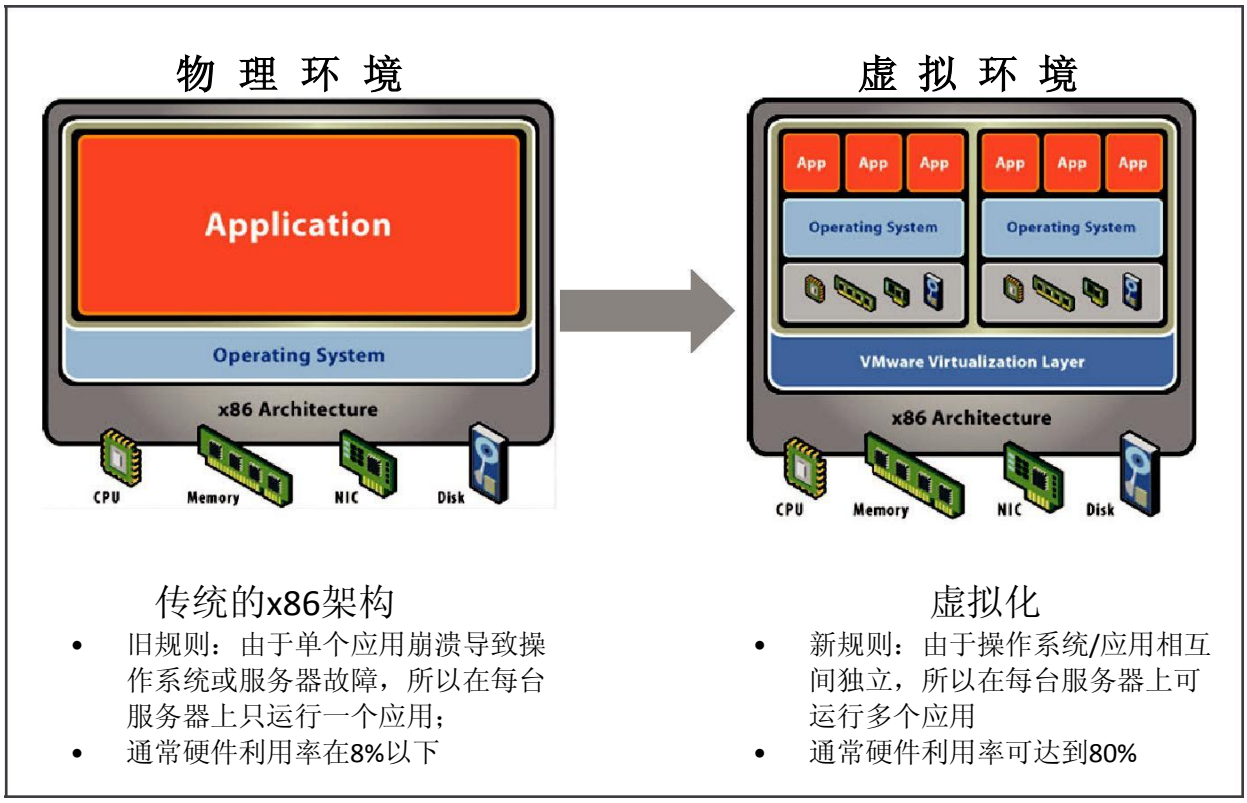

图 1： 虚拟化架构

虚拟的服务器环境通过软件包（管理程序）来给虚拟机分配硬件资源。广义上来讲，就是现在有一台高利用率的服务器，而不是5台每台只有10%利用率的服务器。除了降低了使用的服务器数量以外，虚拟化同时也增加了灵活性。更多的虚拟机可根据需要在服务器上增加（或者移除），但不会引起服务的中断和停止。总而言之，服务器虚拟化把硬件和处理能力分离开来，让管理员可以独立地管理和调整它们。

虚拟化架构中五个必不可少的组件：

- 软件（像VMware、Hyper-V或XenSource等虚拟化软件）
- 服务器硬件（像Dell、HP或IBM刀片服务器等标准的1U服务器硬件平台）
- 存储（联网的，并与NAS和SAN兼容的统一存储）
- 交换机（1GE或10GE以太网，可网管实现最佳的流量控制功能的交换机）
- 安全（可避免外来入侵或严重的流量中断）

特性	优势
加固的服务器	更好的资源利用率、更低的电源使用率、更少的热量
动态预配置	应用程序和存储更好的灵活性
工作负载管理	改善的QoS
工作负载隔离	更高的可用性/安全（如果发生崩溃，则可以进行隔离）
混合的产品和测试	不具备风险地尝试新的事物
混合的OS类型/发布	无需太多专用的传统服务器和应用程序
低廉的专用服务器	根据需要配置新的虚拟机，无需另外购买和安装
单独的存储和处理	根据需要增加或移除容量

表 1. 特性/优势表

软件（管理程序）

在管理程序领域有三个主要厂商：VMware、Microsoft和Citrix。管理程序允许在相同的硬件平台上运行多个虚拟机并且提供在每个虚拟操作系统与底层的CPU、内存和IO资源之间的管理接口（像网络及存储设备）。

在SMB环境中，免费但扩展性有限的管理程序使应用不会存在经济上的负担，并且通过许可证可升级的特性来实现未来的增长。高级的实例包括整体虚拟架构的规划、迁移、管理及控制功能。第三方可提供一些软件及硬件工具以确保稳健的冗余性、恢复时间和细粒度的恢复点。

注意在这种情况下“免费”并不意味着“薄弱”，这一点很重要。即使最低端的管理程序也适用于SMB客户，并且实惠的解决方案可以构建用来解决业务连续性、备份复原以及灾难恢复的挑战。

因为虚拟机可以打包成文件并且可离线拷贝用于简单的容灾恢复，所以虚拟机经常变革容灾技术。正如下图所示：

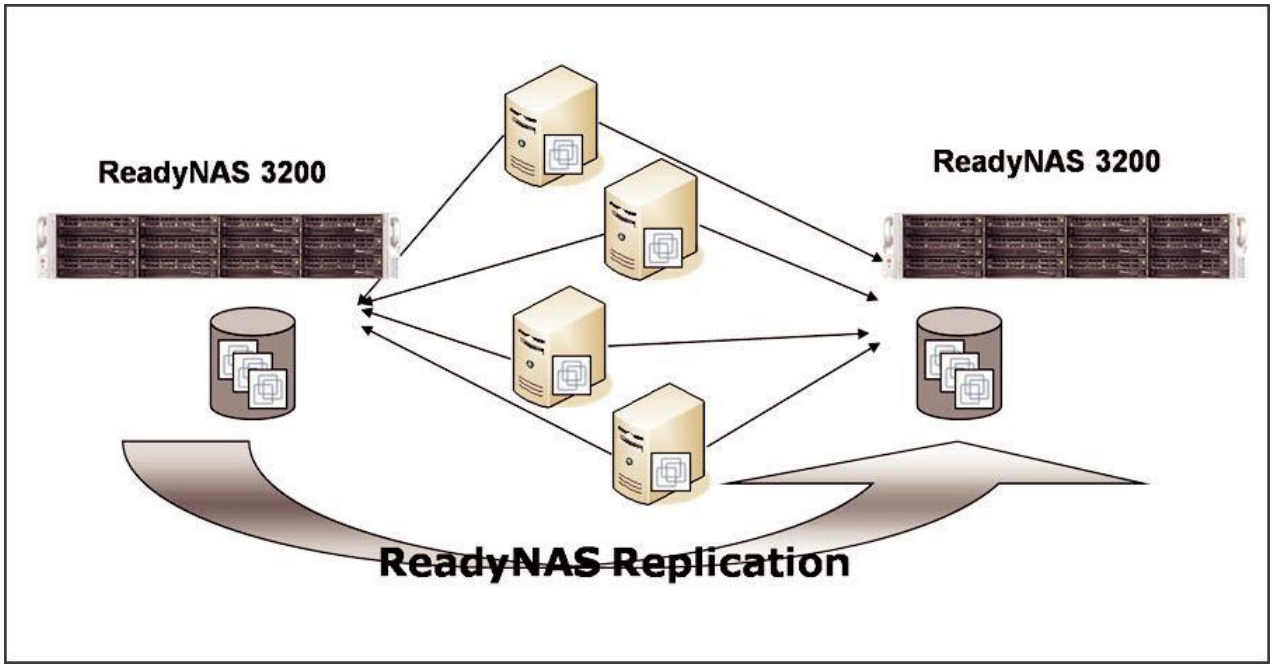

图 2. ReadyNAS复制

供应商	VMware		Microsoft			Citrix
产品	ESX	ESXi	Server	Windows Hyper-V R2	Hyper-V R2	XenServer
版本	4	4	2.0.1	2	2	5.5
费用	Fee-based	Free	Free	Cost of the OS version	Free	Free
虚拟磁盘格式	VMDK format	VMDK format	VMDK format	VHD format	VHD format	VHD format
支持NFS	Yes	Yes	Host OS dependent	No	No	Yes
支持iSCSI	Yes	Yes	Host OS dependent	Yes	Yes	Yes
快照VMs	Yes	Yes	Yes	Yes	Yes	Yes
迁移VMs	VMotion	VMotion	No	Live Migration	Live Migration	XenMotion

表 2： 产品比较

大多数现行的操作系统和应用与定制的管理程序一起运行。如有疑问，请与应用程序供应商确认。现行的管理程序软件也包括从物理到虚拟（P2V）的有效工具，从而简化从物理服务器到虚拟机（VM）的初步转换。

智能的和价格可负担得起的网络存储以及交换机产品可以与任何管理程序一起使用来改变小型企业的IT环境。让我们看一下完整的解决方案的细节。

服务器

鉴于旧的服务器日益增长的重要性，最佳的解决方法包括升级到一个坚固的服务器硬件平台以作为新的虚拟机的主机。顶级的管理程序供应商都可提供最小的硬件建议或硬件认证。即使管理程序包括内存管理特性，一般情况下物理内存安装的数量应该反映各种操作系统和将要虚拟化的应用结合的需求。如果有四台独立的服务器且每台服务器需要2G的RAM，那么虚拟主机服务器应该配置为8GB。这可以避免内存的更换和以后性能上可能产生的问题。

存储

虚拟化实际的功能通过网络存储来增强。像高可用性（VMware HA）、负载均衡（Hyper-V实时迁移）和现场恢复（VMware SRM）等特性都需要共享的网络存储。当存储设备被集中管理时，虚拟机可以连接到各自的容量，然后在仍然运行的平台之间迁移。自动的负载均衡，让操作系统在基于策略设定的主机服务器之间移动，这样可以实现负载均衡和硬件投资的最大化。如果虚拟机崩溃，则只需要触摸一个按钮就可以在另外一台主机上简单地启动。高可用性可以复制VM到另外一个位置并使用一个新的硬件平台作为VMs的主机，这样就可以集成远程主机进行灾难恢复。

统一的存储系统允许最大的灵活性。通过存储中的NAS和SAN功能，文件服务器可以完全淘汰并直接转移到NAS，同时应用服务器可以通过选择的协议（NFS，iSCSI或两者）转换到VMs。NETGEAR® ReadyNAS®统一的存储系统经过认证可与许多虚拟化供应商一起协同工作，从而确保兼容性和互相间的支持。

尽管可靠性很重要，但许多中小企业都受到成本限制。尽管两个电源成本很高，但ReadyNAS®系统仍具有现场可替换组件，则系统可以在现场快速地恢复。

通过离线复制安装Microsoft Hyper-V的一个极好示例，请参考Headlands资产管理成功案例。在这个案例中，客户降低50%的物理服务器，同时替换老式高端存储设备，这样可以降低80%的资本、运营维护成本和机架空间。另外，客户通过使用内置的ReadyNAS®软件无需额外的费用来实现离线灾难恢复解决方案。

交换

因为虚拟机（VM）需要访问网络资源来运行，所以网络基础架构对虚拟环境是绝对关键的。在一个外部物理网络上的交换基础架构必须足够快来处理网络流量的增长，同时必须足够可靠和强大来管理流量、QoS及安全性以及能让SMB客户可以负担得起。NETGEAR ProSafe网管交换机具有终生的保修期，并通过灵活和易于管理的软件提供连接到物理服务器、客户端、网络存储和其它资源的网络基础架构。

- 10GE的连接和链路聚合实现更高的吞吐量/性能
- 端口的故障转移配置实现可靠性
- VLAN实现隔离备份NAS或SAN流量
- 网络流量管理实现总体性能的提升

阅读NETGEAR如何为公共图书馆系统提供可靠的IT基础架构

安全

任何新技术总是带来新的威胁和与之相关的安全性问题。虚拟化也不例外。在2007年10月，Gartner预测直到2009年60%的虚拟机将比对应的物理设备更不安全。以下是虚拟化所面临的主要安全威胁：

- 虚拟化特定攻击
- 传统的威胁
- 管理的职责
- VM无计划地扩展
- 虚拟机的细分

大多数公司对以上所列的一部分威胁有更多的处理经验，而且都是传统的威胁。正如许多面向VM的威胁仍然通过传统的方法（例如垃圾邮件及恶意网页）进入网络那样，这也正是保护虚拟环境安全的一个好的开端。多年来，服务器和最终用户的PC都经受到大量在线威胁的攻击。

全球每年都生成数以百万计独特的恶意程序。这些恶意程序通过网页和垃圾邮件来“推”上用户的桌面电脑。因为虚拟机在本质上是“实际”设备的但不具有物理部分的机器，所以这些威胁对于虚拟机和物理设备一样都是易受到攻击的。大多数的威胁并不区分虚拟机及物理设备。不管是否虚拟机，垃圾邮件都会攻击邮件服务器。

虚拟机通过执行病毒代码从而被病毒感染。此时不仅VM本身有风险，而且管理程序和在上面运行管理程序的所有机器都有风险。一旦管理程序本身受到攻击，则将失去所有的东西。 访客VM上的所有数据和应用都处在危险之中。一直以来，访客VM都很在意这些攻击。

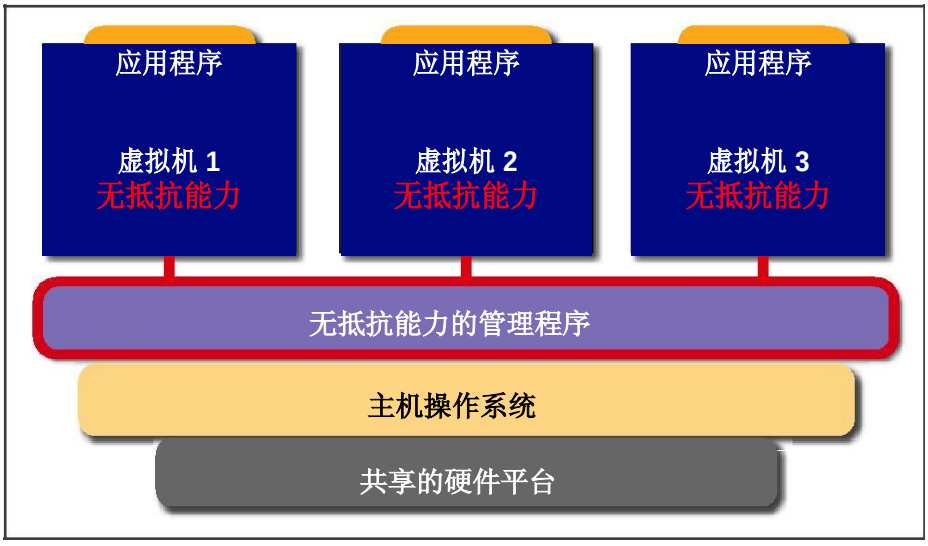

图 3. 受攻击的管理程序和VMs

比以往的任何时候都更需要遵循传统的安全措施和策略。反病毒软件必须在每台VM上部署，特别是在主机系统本身。需要为每个虚拟资源清晰地定义访问权限。最好的是在网关上部署分层的网关安全解决方案。入侵保护系统可以阻止基于非恶意软件的攻击，如SQL注入。反垃圾邮件及网页过滤可以防止用户暴露于网页及邮件中携带的恶意软件。对于那些设法绕过这层的恶意软件，网关的反恶意软件扫描可以在恶意软件到达服务器或最终用户设备之前检测并移除相应的文件。

无论环境是完全地或部分地从物理的向虚拟的迁移，从恶意活动中保存资源仍然是最重要的。寻找产品，能减少IT周期并且涵盖内部和外部威胁（恶意软件、病毒、木马、垃圾 邮件和非法的URL）。如果仍然受到传统安全风险的威胁，那么简化你的网络基础架构就没有任何的意义。

NETGEAR ProSecure安全网关保护网络免受来自不同厂商的数以百万计的内部和外部的安全威胁。欲想了解成功的案例，请阅读零售商J Peterman和他们通过NETGEAR交换、存储和安全产品构建成功案例的经验。

阅读NETGEAR ProSecure UTM25如何为销售商提供“非常优秀”针对威胁的保护

总结

通过使用适当规模和合理价格的产品及服务，SMB也可以实现与大公司相同的虚拟化。大型公司传统上为小型企业提供低端产品时，都会存在产品薄弱或比预想更多的不相关的利益冲突。只有NETGEAR能同时提供产品及作为合作伙伴来提供这些关键组件：服务器、软件、存储、交换及安全性。

想了解更多关于这方面的信息或联系NETGEAR经销商，请访问www.netgear.com.cn。