网络与虚拟化

网络与虚拟化

服务器虚拟化是数据中心服务器组和网络组里模糊不定的角色，因为服务器硬件虚拟化产品将网络带进了服务器。一个不齐全的数据中心设计给 IT 人员迁移带来了痛苦。网络问题会阻碍虚拟化的发展吗？服务器虚拟化对网络 I/O 的影响又表现在哪？如何解决？本指南将讲述网络与虚拟化之间的关系和一些实际例子。

虚拟化造成的网络问题

虚拟化造成的网络问题包括物理与虚拟交换机之间的高 NIC 密度、增加的网络流量和通信问题。这些问题具体的表现是什么？该怎么样避免呢？

- ❖ 网络问题是虚拟化的下一个障碍？

虚拟化与网络 I/O

服务器虚拟化对网络 I/O 的影响与其对 IT 架构其它方面的影响是同样的，那就是使它们的缺点更加暴露无遗。虚拟化技术是如何显现这些缺点的？该如何解决？

- ❖ 网络 I/O 虚拟化：让 10GbE 更加灵巧

具体应用

配置 Xen 虚拟网络可能非常不容易，如何正确分析并解决在虚拟网板上的故障？怎样解决 Windows Server 2003 网络配置错误？在 DMZ 里如何运行 VMware？

- ❖ 网桥与配置：在 Linux 上配置 Xen 网络

- 解决 Windows Server 2003 网络配置错误的问题
- 如何在 DMZ 里运行 VMware?

专家视角

本部分提供更多专家关于网络与虚拟化的看法和解决办法。

- 虚拟化在网络基础设施的挑战
- 在网络共享上如何存储虚拟机与硬盘?
- iSCSI 和虚拟化的关系
- Virtual Server 能直接访问网卡和串行端口吗?

网络问题是虚拟化的下一个障碍？

在本文中，你将学到虚拟化造成的网络问题，例如物理与虚拟交换机之间的高 NIC 密度、增加的网络流量和通信问题。

服务器虚拟化是数据中心服务器组和网络组里模糊不定的角色，因为服务器硬件虚拟化产品将网络带进了服务器。这不是一个齐全的数据中心设计或者说给 IT 人员迁移带来了痛苦。

在本文中，TechTarget 中国的特约虚拟化专家 Scott Lowe 将具体说明在数据中心里，网络上的服务器硬件虚拟化的影响。

例如由 VMware 的 VMware Infrastructure 3（VI3）、Citrix 的 XenServer 或者微软的 Microsoft Virtual Server（最终叫做 Hyper-V）所提供的服务器硬件虚拟化，在数据中心设计中有巨大的差异。

网络当然是一个受虚拟化影响的领域。

高 NIC（网络接口卡）密度

首先，在一个虚拟化环境里，每台物理服务器一般拥有更高的 NIC 密度。虚拟化主机有 8 个、10 个或者 12 个网络接口卡（NIC）是常见的，反过来，没有被虚拟化的服务器只有 2 个或可能 3 个 NIC。这成为数据中心里的一个问题，因为边缘或分布交换机放在机架里，以简化网络布线，然后向上传输到网络核心。在这种解决方案里，一个典型的 48 端口的交换机仅能处理四台虚拟主机，每台 10 个 NIC。为了完全添满机架，需要更多的边缘或分布交换机。

另外，更多的网络架构没有订购太多的边缘或分布交换机，因为更多的服务器没有完全利用它们的网络连接。网络资源和其他资源利用不足，使许多组织进行虚拟化部署，因为他们需要整合工作负荷、降低能耗、释放机架空间、冷却或减少物理服务器。不过在虚拟化环境里，当多个工作负荷整合到这些主机里时，根据运行在主机上的工作负荷数量，网络流量增加了。网络利用率将不再像过去在每台物理服务器上那样低了。

增加的网络流量

为了调节来自整合工作负荷增加的网络流量，可能需要增加从边缘或分布交换机到网络核心的向上传输数量。

网络设计问题

另一个关键的改变来自最新一代虚拟化产品的动态性质，拥有诸如热迁移和多主机动态资源管理。虚拟化里固有的动态更改性能意味着不能再对服务器之间的流量流动作任何假设。

当工作负荷捆绑于虚拟硬件，机架或交换机被告知将交换大量的网络流量时，服务器能分配到机架或交换机。既然工作负荷能动态地从一台物理主机移动到一台完全不同的物理主机，在网络设计里，位置不再用到。网络设计现在必须调节动态数据流，这可能从任何虚拟化主机到任何其他虚拟化主机或者物理工作负荷开始。摈弃传统的 core/edge 设计，数据中心网络可能需要找寻更多全网状架构或“光纤”，这能完全调节来自任何虚拟化主机或者任何其他虚拟化主机的交易流。

诸如 Xsigo 和 3Leaf 这样的厂商利用他们的 I/O 虚拟化产品，满足调节动态交易流的需求，不仅关于网络，也关于存储或 SAN 交易。

物理与虚拟交换机通信

第三，虚拟化使数据中心里网络层的一些能见度降低了。只有使用 VMware 的旗舰产品 ESX Server 3.5 的最新版本，才能使物理网络交换机与虚拟交换机通过像 Cisco Discovery Protocol（CDP）这样的协议进行通信。其他厂商没有这种协议。没有的话，网络工程师在虚拟交换机里没有能见度，也不能轻松决定哪个物理 NIC 对应哪个虚拟交换机。这在故障检修中是最重要的信息。

通过传统的网络入侵系统（NIDS）或网络入侵防护系统（NIPS），能见度的缺乏也影响捕捉并可能阻塞恶意网络流量的能力。尽管一些厂商已经开发了提供这种功能的虚拟应用，这些解决方案依赖混杂的 NIC，并且不能平衡交换机，例如一个镜像交换机不能为流量提供一个镜像端口。虚拟交换机也不能提供可配置的 SNMP 支持，因此不能参与网络管理系统。网络运营组必须依赖服务器运营组，以便帮助决定在虚拟交换机上的哪个端口该关闭，哪个 NIC 受影响等等。

职责的模糊可能是使虚拟化能见度减少的一个因素。服务器硬件虚拟化产品在服务器里带来了网络，服务器组与网络组的角色和责任开始模糊和改变。类似的变化也发生在服务器组、安全组和存储组，因为虚拟化使这些领域的边界变得很模糊。

关于作者：Scott Lowe 是 ePlus Technology 公司的高级工程师。他拥有广泛的经验，尤其是在存储区域网络、服务器虚拟化、目录服务和互操作性这样的企业技术方面。

（作者：Scott Lowe 译者：唐琼瑶 来源：TechTarget 中国）

虚拟化与网络 I/O

服务器虚拟化对网络 I/O 的影响与其对 IT 架构其它方面的影响是同样的，那就是使它们的缺点更加暴露无遗。在本文中，我们将看看虚拟化技术是如何显现这些缺点的，带宽管理的不足如何制约着服务器虚拟化的发展。此外，我们还将进一步探讨 I/O 问题的解决者——10Gb 以太网（10GbE）网卡。

网络 I/O 缺点

网络 I/O 资源并不如 CPU 或内存资源那么丰富。如果按照大多数服务器虚拟化厂商的最佳做法——每个虚拟机安装一个 1GbE 网卡，很快你就会发现虚拟化主机根本支持不了多少虚拟机。毕竟，网卡插槽只有那么多。

对于网络 I/O 的这些缺点，业界主要有如下几种应对方法。首先，几乎每个数据中心都是每增加一个虚拟机，就迅速分裂一次网卡。但是如果用这种方法，那么只有网络 I/O 需求较低的服务器是虚拟的。这样做有个明显的缺点，就是没有对整个环境进行虚拟化，会减低服务器虚拟化技术的优越性。第二种方法是常见做法，也是本文的重点——安装 10GbE 以太网卡。毫无疑问，10GbE 可以大大地提高带宽。物理架构的解决方案的确是很容易，但如果是虚拟服务器环境又该如何处理呢？

NIC 和网络 I/O

在虚拟环境下，多个虚拟服务器通过 hypervisor 层竞争同一网络 I/O 资源。Hypervisor 相当于一个“交警”，位于物理机和主机服务器的物理硬件之间。工作负载的处理遵循“先到先服务”的原则。随着每个物理硬件平台上的虚拟服务器数量的增加，hypervisor 被中断而来处理网络 I/O 需求的时间也会增多。这种情况下，如果多个虚拟服务器的网络 I/O 负载过大，就会出现问题，因为它们会给 hypervisor 带来过大的压力。

为了解决这个问题，可以为每个虚拟机分配一个 NIC。这个方法将原来共用的 I/O 队列分为了多个 I/O 队列，每个物理适配器处理一个队列。这样做的好处是减少了 hypervisor 的中断时间，有利于更好地管理 hypervisor 的中断。然而，这种让每个虚拟机（或多个虚拟机）使用一个 NIC 的方法不仅会导致网卡插槽不够用，还会带来一些其它的问题。

多 NIC 显然是布线管理的一个噩梦，而且还会增加耗电量。例如，一个 1GbE 卡的功率通常约为 8 瓦，安装 10 这样的卡等同于一个 10GbE 卡的性能，所以总功率应该是 80 瓦，而且还会影响服务器自身的空气流通。空气流通的降低进而会增加冷却需求，风扇需

要转得更快，从而增加了服务器的电能消耗。相比之下，一个 10GbE 卡大约只有 15 瓦，而且对空气流通几乎没有任何影响。

由于这些原因，尽管 10GbE 卡存在上述所说的共用队列问题，它仍然是一个明智的选择，是未来发展的绝佳途径。10GbE NIC 的问题在于它利用了 10 倍的带宽，这种情况在虚拟服务器环境下变得更加恶劣。在非虚拟环境下，一台带 10GbE 卡的高性能服务器可以获得 9.9Gbps 的带宽。而在虚拟环境下，同样的服务器却只能达到 4.0Gbps。这是因为，在虚拟环境下所有 I/O 操作都要通过 hypervisor 中的同一队列完成，而且适配器中只有唯一的一个 I/O 通道。随着虚拟机数量和网络 I/O 负载的增加，虚拟机和虚拟机中的应用的性能将无法得到保持，因为它们都要在同一队列竞争 I/O 资源。

虚拟环境下网络 I/O 问题的解决

对于虚拟环境的网络 I/O 问题，有两种可能的解决方案。第一种，行业内的 hypervisor 厂商应该开发一个高级的 I/O 队列系统，允许分割 10GbE 卡的带宽。这种方案还需要有一个能充分利用队列系统的更加智能的 10GbE 卡。还有一种方案是，网卡厂商提高服务质量能力（QoS capability），允许对网卡进行硬件级别的分割，从而保证 I/O 通道的性能。

第一个具有 QoS 能力的 hypervisor 是 VMware 公司出的，不过其它供应商也将会跟着推出各自的产品。VMware 把它称作 NetQueue，它可以显著提高 10GbE 环境的性能。不过，它还需要得到 NIC 供应商的支持，目前的英特尔和 Neterion 网卡都支持 NetQueue。NetQueue 不用处理包路由工作，因此解放了 CPU 资源，缩减了延迟等待时间。

NetQueue 使广泛的服务器整合成为可能，它使用了优化的 10GbE 适配器，让 10GbE 适配器的带宽最大限度地接近其额定值。这样，要获得 9.8Gbps 的带宽就不是什么难事了。但是，有些关键任务需要保证一定的带宽，而 NetQueue 没有为这样的特殊虚拟机提供真正的 QoS。在交换机领域，QoS 早就成为了现实，而在 NIC 方面，QoS 能力还有待提高。

在“一个服务器一个应用”的日子里，的确没有太多的 NIC QoS 需求。服务器与交换机不同，交换机要处理多个数据源的通信，而服务器只有一个目的：为它的应用提供计算和处理能力。如今，由于虚拟化技术的出现，我们需要让某些虚拟服务器优先享有网络 I/O 资源，为它们保证一定的带宽。“先到先服务”的机制已经不再适合这种新形势了。一些供应商正在协力完成解决方案，进一步拓宽虚拟化。如，Neterion 开发了 IOQos。

作为 802.11 标准的一部分，IOQos 是从零开始设计的，用于多应用环境——多个应用竞争 I/O 资源的环境。基于硬件的信道隔离有利于管理，管理员可以对不同虚拟机数据通道进行绝对的 I/O 隔离。完全隔离的优点体现在安全性方面，避免了共用资源间的干扰，如内存和 CPU 资源。如今，大多数软件应用假定自己对系统资源和网卡有绝对的使用权。而在虚拟环境下的网卡是为多个应用共用的，软件开发者们并没有意识到这一点。如果网

卡资源的供应可以让软件自身觉得情况与它预期的一样，那将会大大地提高软件的兼容性。

最后，在将多个软件应用整合到物理主机中的虚拟机时，还需要有带宽作保障。从I/O的角度来看，可以让网卡把这个应用看作一个物理网卡，该应用可以获得有保证的带宽。在过去，系统管理员不得不为某些应用保证带宽，以保持服务器处于非虚拟化状态，或在虚拟服务器中为这些应用分配专用的NIC。这两种做法都不利于节省成本，虚拟化策略有可能帮助获得数据中心的成功。

如果10GbE结合虚拟厂商的智能队列系统、NIC厂商对队列系统的支持和IOQos的应用，我们将可以实现更广泛、更密集的服务器虚拟化部署。此外，还可以优化基础设施投资，获得更高的投资回报率。

（作者：George Crump 译者：涂凡才 来源：TechTarget中国）

网桥与配置：在 Linux 上配置 Xen 网络

配置 Xen 虚拟网络可能非常不容易。domain 0 操作系统显示大量的网络接口并且它通常不能辨别哪个在做什么。在本文中，TechTarget 中国的特约虚拟化专家 Sander van Vugt 将解释这种差别，学习如何正确分析并解决在虚拟网板上的故障。

如果你的 SUSE Linux Xen 环境安装在默认设置下，网络的核心是虚拟网桥。考虑你的物理网桥和交换器在服务器里是虚拟的。所有虚拟网络设备的通信都通过网桥。SUSE 也提供虚拟路由器和 NAT 设备，不过还是没有达到稳定状态。

由于虚拟网桥是你虚拟网络架构的核心，所有网络维护都从这里开始。这意味着你不能再使用 YaST 来改变网络配置。在 domain 0 里，虚拟网卡 IP 地址的简单改变意味着你必须首先关闭虚拟网桥，传统的 SUSE 机制现在已经不再管理网络了。

表 1：使用 network-bridge 命令让网桥运行。

```
lin:/etc/xen/scripts # ./network-bridge start

eth0 device: Broadcom Corporation NetXtreme BCM5752 Gigabit Ethernet PCI
Express (rev 02)

eth0 configuration: eth-id-00:18:8b:bb:f5:40

eth0 IP address: 192.168.1.68/24 (DHCP was already running)

eth0 device: Broadcom Corporation NetXtreme BCM5752 Gigabit Ethernet PCI
Express (rev 02)

eth0 configuration: eth-id-00:18:8b:bb:f5:40

Nothing to flush.

Nothing to flush.

Waiting for peth0 to negotiate link.... eth0

eth0 configuration: eth-id-00:18:8b:bb:f5:40
```

eth0 (DHCP) . IP/Netmask: 192.168.1.68 / 255.255.255.0

一旦网桥启动，你将看见一大堆与网络相关的接口。显示它们的最佳方式是通过使用下表 2 中的 ifconfig 命令。

表 2：ifconfig 命令显示所有可用的网络接口。

```
lin:/ # ifconfig

eth0 Link encap:Ethernet HWaddr 00:18:8B:BB:F5:40

inet addr:192.168.1.68 Bcast:192.168.1.255 Mask:255.255.255.0

inet6 addr: fe80::218:8bff:febb:f540/64 Scope:Link

UP BROADCAST NOTRAILERS RUNNING MULTICAST MTU:1500 Metric:1

RX packets:165 errors:0 dropped:0 overruns:0 frame:0

TX packets:38 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:0

RX bytes:11342 (11.0 Kb) TX bytes:5106 (4.9 Kb)



lo Link encap:Local Loopback

inet addr:127.0.0.1 Mask:255.0.0.0

inet6 addr: ::1/128 Scope:Host

UP LOOPBACK RUNNING MTU:16436 Metric:1
```

RX packets:140 errors:0 dropped:0 overruns:0 frame:0

TX packets:140 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:0

RX bytes:11769 (11.4 Kb) TX bytes:11769 (11.4 Kb)

peth0 Link encap:Ethernet HWaddr FE:FF:FF:FF:FF:FF

inet6 addr: fe80::fcff:ffff:feff:ffff/64 Scope:Link

UP BROADCAST RUNNING NOARP MTU:1500 Metric:1

RX packets:151 errors:0 dropped:0 overruns:0 frame:0

TX packets:30 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:1000

RX bytes:10686 (10.4 Kb) TX bytes:4430 (4.3 Kb)

Interrupt:17

vif0.0 Link encap:Ethernet HWaddr FE:FF:FF:FF:FF:FF

```
inet6 addr: fe80::fcff:ffff:feff:ffff/64 Scope:Link

UP BROADCAST RUNNING NOARP MTU:1500 Metric:1

RX packets:38 errors:0 dropped:0 overruns:0 frame:0

TX packets:165 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:0

RX bytes:5106 (4.9 Kb) TX bytes:11342 (11.0 Kb)
```

```
xenbr0 Link encap:Ethernet HWaddr FE:FF:FF:FF:FF:FF

inet6 addr: fe80::200:ff:fe00:0/64 Scope:Link

UP BROADCAST RUNNING NOARP MTU:1500 Metric:1

RX packets:132 errors:0 dropped:0 overruns:0 frame:0

TX packets:0 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:0

RX bytes:6815 (6.6 Kb) TX bytes:0 (0.0 b)
```

Xenbr0 与 peth0

Xenbr0 设备用于表示网桥本身。网桥自己必须与服务器里的物理以太网板通信。物理板通过 peth0 接口表示。由于它只是物理网板的表现形式，你通常不用直接管理它。你所需要做的是与 peth0 通话，在 domain 0 环境是 eth0 接口。它实际上是用在 domain 0 里的虚拟接口。每台虚拟机（域）都有一个 eth0，取决于 eth0 的配置，可能还有其他的 eth。

Eth0 与 vif

eth0 接口是虚拟机所用的接口，所有这些接口需要在 domain 0 有所表示。它们就是 vif 接口，直接连接到 Xen 网桥，并使虚拟机与其他机器通信成为可能。所有的 vif 接口都有个名字，例如 vifx.y。在此名字中，x 相当于显示在 xm list 命令中的虚拟机数量，y 表示这台虚拟机的接口数量。例如，如果 ID1 虚拟机有两个网络板，你在 domain 0 机器上将看见 vif1.1 与 vif1.2。

总结

在本文中你已经学到了虚拟网络接口的配置。我们讲解了一些基本知识。在接下来的 SUSE Linux Enterprise Server 文章中，将描述路由器和 NAT。也有一些负载均衡问题。例如，在某些具体环境，使用两个而不是一个虚拟网桥能使 eth 接口更好的操作。

（作者：Sander van Vugt 译者：唐琼瑶 来源：TechTarget 中国）

解决 Windows Server 2003 网络配置错误的问题

问：我在 Windows XP 上运行 Microsoft Virtual Server。我安装了 Windows Server 2003 作为 DC。我能连接 Windows XP 虚拟机到域里，不过当我尝试从服务器管理它时，得到一个错误：computer \x cannot be managed because the network is unreachable。我也不能返回到 XP 虚拟机，但我能从 XP 虚拟机返回到服务器。我的设置有什么错误吗？

答：我大胆假设你的 Server 2003 系统的网络没有正确配置——也许其 DNS 没有正确配置，这就能解释它为什么不能解析另一台机器。如果你还没有在虚拟域控制器里运行 NETDIAG 和 DCDIAG，按照下面的做，看看会怎么样。

另一个要注意的是关于虚拟化域控制器上的撤消磁盘：

“在子机或者域控制器上有撤消磁盘吗？这可能是你问题的原因所在，也是为什么我要你提供精确的错误信息。一个域成员在域里有一个帐号，这更像一个用户帐号，有个密码保护这个帐号。这个密码周期性地改变（这个周期取决于操作系统）。因为密码周期性改变，你必须小心使用撤消磁盘。可能发生的改变有下面这些：

1. 成员服务器和域控制器都在运行。
2. 成员服务器更改了它的计算机帐号密码。
3. 这个更改在成员服务器和域控制器上都能看见。
4. 成员服务器关闭，更改在撤消磁盘里的被丢弃。
5. 成员服务器现在有旧密码，而域控制器用新密码。
6. 成员服务器重新启动，尝试使用域控制器设置一个安全通道，由于密码不匹配而失败。

为了防止这种情况发生，你需要不使用撤消磁盘，或者在使用撤消磁盘时意识到这是个潜在的问题。

（作者：Serdar Yegulalp 译者：唐琼瑶 来源：TechTarget 中国）

如何在 DMZ 里运行 VMware？

问：一个正在进行的考虑是关于在互联网和运行 Windows 2000 Web 站点的子机的内联网之间共享一台 VMware ESX 主机。让 ESX 主机在面向内容时用互联网，让这台主机上的其他子机使用内联网类型的网和应用服务，那么拥有相同 ESX 主机的风险在哪？在一个 DMZ 里使用 VMware 的话，您有什么建议？

答：这种做法的风险与你放置在 VMware ESX 里的网络协议层的信任数量是成比例的。如果你放置互联网和内联网在一个独立的 Virtual Switch（或端口组）上，并关掉混合模式、IP 欺骗和 MAC 欺骗，那么就可能使用 ESX 构建了最安全的网络设计，如果你留意 VMware 在底层是如何执行的，那么就可以换个设计，不仅可以通过访问共享存储隔离 ESX 服务器，也可以通过互联网或内联网隔离。希望这些对你有帮助！

（作者：Andrew Kurtz 译者：唐琼瑶 来源：TechTarget 中国）

虚拟化在网络基础设施的挑战

问：虚拟化表现在网络基础架构方面的挑战是什么？

答：由于物理对应性，虚拟机（VM）通常需要相同类型的资源。例如，一台 Web 服务器工作负载将通常要求相同数量的带宽，无论它运行在物理服务器还是虚拟机上。总的来说，这不算太坏，大多数组织已经在为他们目前的物理服务器考虑容量规划和性能监控。

主要的问题是要记住饱和的或超载的物理主机服务器资源。你需要为每台虚拟机的总计负载作计划，添加由直接运行在主机上的任何应用或服务放置的负载，然后包括虚拟化的负载“开销”。重要的子系统包括 CPU、内存、磁盘和网络资源。例如，如果你在一台服务器上有一个单独千兆以太网连接，并在这台机器上放置了一群网络密集型虚拟机，物理 NIC 可能迅速地成为一个瓶颈。你将需要观察使用多个（大多数虚拟化平台支持的）NIC 端口以及负载均衡和 NIC 端口聚合这样的功能。总的来说，问题能找到，不过不要因为在购买产品之前做的性能分析失败而陷入安全威胁里。

（作者：Anil Desai 译者：唐琼瑶 来源：TechTarget 中国）

在网络共享上如何存储虚拟机与硬盘？

问：管理所有我需要支持的虚拟机太困难了。我能把虚拟机和虚拟硬盘存储在一个网络共享上吗？

答：当然能。如果你支持许多不同的虚拟机，你可能有个问题——为 Virtual Server 的所有设备管理你需要的所有虚拟硬盘文件。整合管理的一种方式是存储所有的虚拟机到一个诸如标准的 Windows 文件共享这样的网络设备或一个网络附加存储（NAS）设备。如果虚拟硬盘配置成只读（例如，如果你使用差分磁盘或 undo disks），你甚至能让各种虚拟机在相同时间访问相同的虚拟硬盘。

配置这个很简单：只需要添加你所需要的搜索 Virtual Server 配置路径 UNC。标准的安全需求应用。在 Virtual Server 服务下运行的服务帐户必须要有权限。

（作者：Anil Desai 译者：唐琼瑶 来源：TechTarget 中国）

iSCSI 和虚拟化的关系

问：iSCSI 可以进行虚拟化部署吗？使用 iSCSI 而不是光纤通道的决定因素是什么？那如果使用光纤通道而不是 iSCSI 的决定因素呢？

答：可以部署。目前 VMware 和其他技术支持这个协议，因为数据和启动设备的存储附属（到 ESX 服务器）。真正的问题是你的 IP 网络是否能承受实施 iSCSI 而需要增加的流量。SAN 用于高负载、块级流量的存储密集型应用。因此从根本上说，我们知道你能为 ESX 使用 iSCSI，不过你需要问：使用任一配置，你需要有适当的路径或网络冗余配置吗？虚拟机或 ESX 服务器需要高带宽吗？并且目标站点与你复制时可能用到的源站点之间的连接点是什么？同样，实施 iSCSI 能使用现有的 IP NIC，不过这个要求很高，你可能需要考虑一个独立的 TCP 卸载引擎（TOE 或最优化的 iSCSI 网络卡）。你不想要你的主机推论管理这些交易的周期。一般来说，iSCSI 适合较少 I/O 请求的应用。

（作者：James E. Geis 译者：唐琼瑶 来源：TechTarget 中国）

Virtual Server 能直接访问网卡和串行端口吗？

问：Microsoft Virtual Server 2005 能直接访问网卡（如果需要不用虚拟路由器）和串行端口吗？

答：Virtual Server 模拟多端口网络适配器，每台虚拟机有大于四个的网络连接。它也模拟两个以上的串行端口，用于映射物理的串行端口。

（作者：Serdar Yegulalp 译者：唐琼瑶 来源：TechTarget 中国）