



## **虚拟化部署的隐藏成本分析**

## 虚拟化部署的隐藏成本分析

我们都知道[虚拟化可以节省成本](#)，但尽管虚拟化带来了大量优点和特性，但重要的是要记住虚拟化技术并不是万能的，并且在某些情形和环境并不适合使用该技术。虚拟化技术确实存在一些缺陷，虽然这些缺陷未必对系统构成危害，但是用户需要在使用虚拟化技术之前意识到这些缺陷。

### 电力与管理

第一个经常被忽略的问题是用一个物理服务器支撑几个虚拟化服务器所带来的电力消耗以及排放大量热量。而且虚拟化技术也带来了一定管理上的问题。

#### ❖ 服务器虚拟化隐藏成本之电力与管理

### 网络与虚拟机蔓延

上一部分介绍了电力消耗和热量排放以及虚拟化技术带来的管理问题。虚拟化服务器存在什么样的网络问题？对虚拟化技术的使用不检查也不控制可能导致虚拟机的滋生和蔓延，这又该如何解决呢？

#### ❖ 服务器虚拟化隐藏成本之网络与虚拟机蔓延

### 许可、存储与高可用性等

保持软件许可证的遵从性仍然是另外一个挑战，管理员可以有很多选择来帮助维持对软件许可证的控制。存储问题为什么是另一个更具有挑战性的问题？表现在哪？还有那些额外的隐藏成本？

- ❖ 服务器虚拟化隐藏成本之许可与存储
- ❖ 实施虚拟化的隐藏成本
- ❖ [虚拟化隐藏成本之授权费用](#)

## 服务器虚拟化隐藏成本之电力与管理

在整合服务器和节省珍贵数据中心空间的潮流中，许多公司都转向虚拟化技术。通过整合一个数据中心的物理服务器到虚拟化服务器，企业可以提高服务器使用率，加大工作效率。

尽管虚拟化带来了大量优点和特性，但重要的是要记住虚拟化技术并不是万能的，并且在某些情形和环境并不适合使用该技术。虚拟化技术确实存在一些缺陷，虽然这些缺陷未必对系统构成危害，但是用户需要在使用虚拟化技术之前意识到这些缺陷。在本系列文章中，TechTarget 中国的特约作者 David Marshall 和 Dan Knezevic 将介绍若干个虚拟化实施过程中可能带来的几个关键问题。

第一部分主要介绍虚拟化带来的电力和热量费用和管理上的问题；[第二部分](#)讨论网络问题和虚拟机蔓延所带来的问题；第三部分阐述许可证发放、性能和存储问题。

那么我们就沿着这个思路开始介绍：

### 电力和热量代价

第一个经常被忽略的问题是用一个物理服务器支撑几个虚拟化服务器所带来的电力消耗以及排放大量热量。要知道毕竟虚拟化服务器将会带来对硬件资源的更高利用率，这意味着操作物理服务器所需要的电力要增加，并且同时也会排放大量热量。

一个支撑运行多个虚拟机的物理服务器以 80% 或者更高的使用率运转，非虚拟化服务器平均使用率是 15%。相比之下，前者的硬件要消耗更多电力资源。

许多数据中心并不具备应对支持虚拟服务器所必须的大量电力需求的能力。例如，如果每一个数据柜满载标准的 2U 服务器，那么对于每 42U 数据柜，用户为了满足电力需求，同时也提供必要的预备电力（以防一个单独线路故障），就可能需要 20 安培电力线路。这个电力规划实际上是标准电力规划的两倍，标准情况是仅需要为每一个柜提供 20 安培电力线路。

为每一个柜的电力线路翻倍给其自身带来问题，特别是如果这意味着数据中心需要升级整个电力基础设施。

### 管理

虚拟化技术也带来了一定管理上的问题，尤其是在打补丁、备份、主机供应、安全、监控和硬件需求等方面：

## 打补丁

在大规模虚拟化生产环境中，同时给物理主机和虚拟机打软件补丁确实是一个难题。如果需要重新启动系统的话，一台物理机支撑上百台虚拟服务器的情况下给业务正常运转所带来的影响要远远大于重启一台单独服务器所带来的影响。

因此在一个非虚拟化环境中，公司可能不需要着重考虑 Windows 更新打包所带来的宕机时间；然而在一个虚拟化环境中，打补丁和重新启动一个单独主机服务器会带来更多更大影响。规划宕机时间本来很简单，现在却成为一个比较辛苦的工作。使用大量虚拟化主机服务器运行大企业工作平台的企业面临着一个复杂的问题，导致一些企业有选择性地只打关键补丁，从而导致系统处于比较脆弱的状态。

一些单位，如 ISS (Internet Security Systems)，为了保护没有完成实际打补丁的服务器而提供一些虚拟安全补丁技术。然而，这并没有解决应用稳定性和故障补丁所带来的问题，这些都必须适用于物理服务器。在这样的情况下，重新启动系统就不可避免了。

重要的是对于虚拟平台来讲，物理服务器重启的代价非常大。

## 备份

在虚拟化环境中实施一个合理的备份解决方案是虚拟化的另外一个痛点。第一个明显的问题就是用户希望备份的数据是什么？接下来如何解决以及备份频率多大？答案是备份整个虚拟磁盘存储还是整个磁盘镜像？或者是用户需要考虑只备份基本镜像，之后是各种各样对磁盘的重做和撤消操作？

另外就是用户需要面对一场严峻的挑战，需要备份数据的数量大得惊人。除非单位很庆幸有非常健壮的 SAN 或者其它磁盘备份解决方案，把很多 T 的数据备份到磁盘的速度很慢并且也十分低效。再有就是我们甚至还没有考虑如何处理备份物理主机服务器以及其操作系统配置。

## 供应

自动化物理主机供应的需求也很大，并且在物理服务器部署的时候这个需求下降得很快。但是物理服务器供应仅仅是问题的一个方面。一旦物理主机服务器正在运行并且满额负载的话，我们必须考虑虚拟服务器自动供应。

很多技术公司为部署和供应物理服务器提供一个自动化解决方案。许多那些相同单位，如 Altiris，也都能够自动提供虚拟服务器。但是这个过程非常复杂，尤其是如果用户单位使用多个不同虚拟化环境的虚拟平台，如 VMware 和微软虚拟服务器。自动化另外一个复杂性在于必须同时仔细权衡和考虑物理环境和虚拟环境。

## 安全

虚拟化环境中安全问题是一个更加复杂的问题，用户在虚拟化环境下必须考虑两层的安全问题：物理主机安全和虚拟机安全。如果物理主机服务器受到安全威胁，其上运行的所有虚拟机都会受到影响，之后就会给运行在同一个主机上的所有虚拟机带来负面影响。

### **监控**

虚拟化技术也有其自身独特的问题，监控就是一个典型。用户必须同时监控物理服务器和虚拟机以保证工作环境正确运转，这是因为一台物理主机服务器故障将导致几个虚拟机同时出现故障。

在物理主机上运行监控软件或者代理会消耗物理主机的珍贵内存和 CPU 周期，这些本来可以提供给虚拟机使用，从而给虚拟机性能带来潜在影响。所以很有必要计算监控器软件物理资源使用率，以决定用户是否可以备份这些资源。

### **其它硬件**

最后，每一台虚拟机主机服务器同时需要多端口网络适配器和几个物理连接的情况并不常见。每台服务器除了三到四个端口之外都是电线连接，特别是如果用户正在运行一个虚拟化平台，并且这个虚拟化平台没有提供横跨两个物理通道连接多个 VLAN 的能力。这也就带来了另外一个管理问题：用户工作平台将会消耗更多 Ethernet 带宽，并且转换端口跳转频率也将相当高。这个时候就必须购买大量访问控制层 Gigabit 转换器来应对虚拟化主机的需求。

(作者: David Marshall, Dan Knezevic 译者: 王越 来源: TechTarget 中国)

## 服务器虚拟化隐藏成本之网络与虚拟机蔓延

关于虚拟化实施隐藏代价的[第一部分](#)我们介绍了电力消耗和热量排放以及虚拟化技术带来的管理问题。现在，在第二部分，我们着重讨论网络问题和虚拟机蔓延带来的问题。第三部分阐述许可证发放、性能和存储方面的问题。

### 网络问题

虚拟化服务器有一个独特的网络问题。在虚拟网络中，用户可以看到比通常情况下更多的 IP 地址、更多的子网和 VLAN、更大的数据包流量、转换端口问题中更大的脆弱性、每一台主机负载机器数量需要更详细的规划以及 MAC 地址管理问题。

### IP地址

根据每台物理主机负载虚拟机数量的不同，用户很快就会意识到需要做一个网络规划。从外面看，100 台物理主机可能还不是一个大问题，但是如果每一台物理服务器上平均负载 6 台虚拟机，这个时候就有 600 台虚拟机和 100 台物理服务器，也就是说要为 700 台机器配置网络和 IP 地址。从网络规划角度看，重要的是把虚拟机作为物理服务器对待。更为重要的是要基于虚拟机和物理机总数量规划出网络配置及其子网的情况。否则会带来非常麻烦的问题。

### 子网和VLAN

随着物理主机服务器和虚拟机的数量不断增加，子网和 VLANs 的数量也需要随之增加，因此用户需要意识到将会有越来越多的子网和 VLAN 需要管理。并且如果用户在 VLAN（如多接口防火墙服务模块（FWSM: Firewall Service Module）的 Cisco 6509）之间设置访问控制列表（ACLs: Access-Lists）的话，通常情况下，就需要做好思想准备来管理相当大数量的对象组和一个相对大数量的 ACL 和防火墙配置。

### 高数据包流量

需要处理的一个显而易见的问题就是用一个物理接口来运行多个虚拟机，这将会带来网络适配器和物理网关端口上的高数据包流量（PPS: Packet per Second）。甚至 Gigabit 网关也会因为高 PPS 网络流量导致网关端口缓冲区溢出，这一点通过网关端口上的丢包和数据包重传可以看到。

### 给网关端口问题带来的更大脆弱性

另外一个问题是单独一个物理网关端口可能出现问题，就有可能带来一系列问题，从而影响使用该物理网络适配器的所有虚拟机，因为这个物理网关适配器连接到这个特定的



网关端口。我们来继续探讨这个问题，如果由于虚拟机网络性能问题进行故障检修，用户就必须考虑其它因素，例如运行在同一个物理网络接口上的其它虚拟机可能会给物理接口自身带来缓冲区问题。和非虚拟化环境相比，在虚拟化环境中这些情况和其它因素给网络监控提出更大挑战。

### **需要规划主机上虚拟机的数量**

每台物理机上的虚拟机数量问题是在规划和设计虚拟网络的时候时需要考虑的一个首要问题。随着虚拟化工作环境的推广，用户应该期望管理较大数量的 IP 地址，更多数量的 MAC 地址、子网地址和 VLAN。

接下来的一个问题就是在包含很多服务器的大型企业网络中将要面对的：核心网层必须强劲、稳定和高速，如在 Cisco 6509E 主板中。除非需要非常迅速地吞吐大量 IP 地址，否则考虑使用较小子网。

另外，为了保持广播流量在一个可管理的水平线上，考虑分解子网为/23 网络，允许每个子网上有 500 台左右的虚拟机并且仍然能够保证网络性能。依赖于如何管理 inter-VLAN 流量，并且如果 ACL 适用于每个 VLAN 的话，考虑使用 FWSM 解决方案满足大数量接口和高吞吐量需求。ARP 表包含了大量的 IP 地址，这就是说预先花费了大量的钱在网络工具上，这些功能能正常工作。

### **MAC地址管理**

虚拟化环境中提及到的最后一个问题就是 MAC 地址管理。不能按照通常情况来考虑这个问题，因为在物理服务器上，MAC 地址烙在物理网络适配器上，但对于虚拟服务器并非如此。一个虚拟机网络适配器可以是用户或者静态指定或者动态指定 MAC 地址。无论哪种方式，用户可以在网络中看到大量 MAC 地址。更重要的是，每一个单独物理网络接口和网络网关端口，都有多个 MAC 地址。随着网关数量的增加和每个网关端口对应多个 MAC 地址，跟踪一个恶意 MAC 地址将会成为一个非常费力的工作。

### **虚拟机的蔓延**

在某些情况下，可能需要为了虚拟机的增加而增加物理服务器的数量。如某个公司六个月以前的数据中心管理着 100 台服务器，在服务器整合之后，该公司把物理服务器数量减少到 50 台服务器。六个月以后，该公司可能就会发现他们不仅仅管理 50 台物理服务器，同时管理每一台物理服务器上面的 8 台虚拟机，也就是说总共管理 450 台机器。管理机器的数量是 450% 的增长，仅仅在六个月以前该数量还是 50% 的下降。

这个数量膨胀后面的一个原因就是需要管理的虚拟机创建起来非常容易。在传统 IT 部门中，如果一个业务部门需要一台新服务器，IT 管理员必须经过一系列的审核来证实该部门是否真正需要。在使用物理服务器的时代，需要经过大量的合理的控制和流程，第一步是物理购买。一旦一个服务器规范定义并且该顺序排出来之后，就需要花费一定的时间



来购买和配置该服务器。第二步就是物理控制服务器，物理服务器需要开箱、摆放、排列、布线和配置。这些步骤通常都是 IT 部门控制，原因很简单：需要物理上接触这些设备。

在虚拟化环境下配置新虚拟机相当简单，创建一台新虚拟机并不需要物理访问服务器。并且因为创建一台新的虚拟机只是简单地从一个位置拷贝一个文件到另外一个位置，几乎公司的每一个人都可以做到。对虚拟化技术的使用不检查也不控制可能导致虚拟机的滋生和蔓延，随着虚拟机零星地出现在整个 IT 基础设施中，虚拟机就会逐渐变得难以管理和难以控制。

[点击此处查看第三部分](#)，在第三部分中讲解许可证发放、性能和存储。

*(作者: David Marshal, Dan Knezevic 译者: 王越 来源: TechTarget 中国)*

## 服务器虚拟化隐藏成本之许可与存储

在[第一部分](#)中，我们讨论了电力耗费和热量排放以及虚拟化管理问题；[第二部分](#)介绍的是网络问题和虚拟机蔓延带来的问题；最后，在第三部分我们以阐述许可证发放、性能和存储结束本系列文章。

### 证书发放

保持软件许可证的遵从性仍然是另外一个挑战，管理员可以有很多选择来帮助维持对软件许可证的控制。但是在虚拟化环境中又该如何控制呢？随着 ISO 镜像、虚拟机里 KVM 功能的使用以及从 PSOT 屏幕往上控制软件许可遵从性，物理限制在虚拟环境中似乎作用不大。

但是 IT 管理员可能面临的最大问题是虚拟化平台克隆和复制虚拟机的能力。没有控制大量复制和部署虚拟机进程的方法，许可证一致性的保持将会是系统管理员的噩梦。

在虚拟机模板或主镜像里有客体操作系统和任何预安装软件应用程序，任何一个或者所有的这些都包含一个软件许可证和相对应的许可证限制。管理员需要有能力和跟踪总共部署多少个镜像实例。如果用户在部署虚拟化之前就认为维持对许可证的控制是日常工作的话，那么这个问题就被夸大了。

### 性能

服务器虚拟化背后的一个驱动因素就是需要提高服务器资源未使用部分的性能输出。当然服务器虚拟化可以更高效和有效地使用服务器处理能力，但是虚拟化技术给其他物理资源所带来的额外压力却经常被忽视。在服务器整合过程结束后，磁盘子系统可能会成为系统一个更大的瓶颈问题。

服务器处理器的运行要比在硬盘上快几个数量级，因此一旦服务器整合更好地利用物理服务器处理器，磁盘 I/O 性能相应就会下降。随着物理服务器上虚拟机的数量的增加，客体操作系统的数量也不断增加，这些客体操作系统每一个都产生很多磁盘 I/O 请求。

磁盘 I/O 请求指数级的增长进一步激发已有的瓶颈服务器组件。重要的是要记住随着每一台虚拟机增加对共享磁盘子系统的使用，就显著地降低了任何一个和其它所有虚拟机共享该工作平台的性能。

磁盘碎片整理也可能引发磁盘 I/O 瓶颈和性能问题。虚拟化技术可能加重碎片问题，创建一个固定大小的虚拟硬盘文件（一次性创建整个文件大小）可以帮助减轻部分磁盘碎片问题。

但是更受欢迎的虚拟硬盘文件选择似乎是动态扩展磁盘，起初创建的文件比较小，随着虚拟机创建数据量的增加，磁盘大小也随之增加。这样可以预先节省宝贵的磁盘空间，但是会带来巨大性能问题。由于数据不停地写入虚拟机、移出虚拟机，数据在物理文件系统中零星地变化，导致随着时间的变化磁盘空间越来越零碎。碎片问题越来越严重，磁盘 I/O 瓶颈问题和该物理储存设备上虚拟机的性能问题也越来越严重。

虚拟化技术也增大了对服务器内冗余组件的需求，现在一个单独物理组件出现故障将影响到大量工作平台的性能和正常工作时间，而不再仅仅只影响到一台服务器。同样，使用虚拟化技术整合服务器需要认真规划、评价以及合理配置。

同组件故障一样，虚拟平台不合理的规划和错误的配置将会给大量虚拟机性能和正常工作时间带来负面影响，而不仅仅是一个虚拟机实例。

## 存储

存储问题成为一个更具有挑战性的问题，并且在管理员的优先列表上的地位也得到很大提升。在一个小的虚拟机工作环境中，把虚拟硬磁盘文件或者虚拟机镜像存储到本地服务器上，从直观上来讲应该是一个不错的解决方案，但是随着工作环境不断扩大，本地磁盘存储的弊端就显现出来了。

使用本地磁盘存储一个很明显的限制就是很多服务器并没有足够的空间来存储若干个大的虚拟机镜像文件。虚拟机镜像文件有大有小，但是一个单独虚拟硬盘文件甚至可能达到 100GB 以上。如果几个这样的虚拟机整合到一台相同的物理服务器上，空闲磁盘空间很快就会被占用掉。

如前面给出的解释，如果允许大量复制虚拟机，而没有任何合理的监管和控制。可能一个简单的拷贝命令就会很快地占用本地存储空间。

下一步就是转向网络存储解决方案，如 SAN 或者基于 NAS，这两者都是出于性能原因和更容易镜像管理考虑的。购买这样一个解决方案的另一方面的问题是花费太大，不仅仅是购买这个实际的设备花费大，企业运行该设备的费用也比较高。

把虚拟化技术和网络存储解决方案结合起来并不像听起来这么简单，选择恰当的存储解决方案是一个非常微妙的问题，并且甚至很难预测在维持可接受的 I/O 吞吐量和提供合理的终端用户体验的时候，同时可以操作的虚拟机数量。

在权衡存储解决方案的大小和容量与已经实现的性能时，许多单位都采用“起初取小”的策略，购买一个 50TB 存储设备或者一个较小的 SAN 解决方案。这些单位之后会意识到他们低估了企业的存储需求，需要升级到 100TB 以上容量的解决方案。购买新空间和高端 SAN 解决方案增加的费用和迁移所有的数据消耗的时间是大多数虚拟化环境部署中必须面对的两个主要问题。

和其它设备一样，存储组件并不能避免虚拟化和组件故障问题。如果使用本地存储或者基于网络存储，任何停电时间和存储设备故障都会影响到相当大数量的虚拟机，这些虚拟机都依赖于该设备读取虚拟机镜像文件。单独一个存储组件故障有可能造成成千上百个虚拟机故障而不仅仅是一个物理服务器。

(作者: David Marshal, Dan Knezevic 译者: 王越 来源: TechTarget 中国)

## 实施虚拟化的隐藏成本

对许多组织来说，采用虚拟化主要是为了降低数据中心成本。这听起来似乎很简单：物理服务器数量的减少必然会节约成本，对吧？如果你和一名推销员讨论这个问题，你很可能会这么认为，因为他会极力向你推销虚拟化。然而，虚拟化会带来一些附带的开销，这些开销并不像它节约硬件成本所带来的好处那么明显。在本文中，TechTarget 中国的特约作者 Sander van Vugt 将探讨一下虚拟化的这些成本因素。

### 虚拟化的高可用性成本

在实行虚拟化时，你会尽量减轻物理机事故带来的影响。如果一台宿主 4 台虚拟机的物理机死机了，其影响将是巨大的，这就是为什么虚拟环境总是需要额外的网络投资的原因。为了使它尽可能的冗余，你需要把虚拟机存放到存储区域网络（SAN）。这有助于获得高可用性（HA），以便在物理机死机时保护虚拟机。

如今，大部分公司都已经有一个合适的 SAN，因此你可能不需要额外地在 SAN 上花钱。不过，高可用性解决方案在大多数情况下还会带来一些额外的花费。主要有两个原因：第一，为了保证 HA 工作稳定，你需要一个防护装置以便终止出故障的物理节点。这需要确保一台虚拟机不能同时在两个物理服务器中启动。一台虚拟机在两台物理服务器中同时启动的情况是存在的，因为如果没有防护装置，网络架构问题会冒着分裂（split brain）的危险，两个集群都认为另一半是关闭的。因此，防护是必要的。由于防护是基于硬件的，所以会带来额外的费用。

证书是影响 HA 执行成本的第二个因素。所有主要虚拟平台都会额外收取高可用性费用，而且这个费用可能很高。只有开源虚拟化平台 Xen 提供免费的 HA 解决方案，能够以 Heartbeat 群集的形式获得。但是，这个解决方案太复杂，只有少数人能够完全掌握它。

### 额外虚拟成本

执行虚拟化的另一个主要成本因素在于管理成本。在一些大型公司里，虚拟化项目日趋复杂，所以需要一些人员专门管理它们。即使是小型企业，员工也需要熟练的技术以便管理好复杂的虚拟环境。每年，昂贵的培训课程和额外的工作量动辄达到好几万美元，即使是小型企业也是如此。用同样多的费用，公司可以另外安装两台物理服务器了。

由于虚拟化使得 IT 架构更加复杂，所以其复杂性成为了新增成本的又一根源。例如，一个旧的备份系统的功能可能不够齐全而不能备份其中一个文件系统或不能备份完整的虚拟机，而且可能需要另外的证书。别忘了，好的管理界面也不便宜。你能免费获得的最好管理界面是基于图形或网页的管理界面，可以让你一次管理一台服务器。

最后，服务器在虚拟环境下运行效率更高意味着它们也会消耗更多的电力。当服务器的平均负荷量低于 20% 时，机柜的电源可能没问题。但是当所有物理服务器的平均负荷量达到 70% 时，它们就需要更多的电力。这可能意味着要升级数据中心的电力设施。如果这其中包含了不间断电源（UPS），那么执行虚拟化的必需费用将会更高。

执行虚拟化环境起初看起来可能是能减少数据中心成本的方案。然而，培训、额外证书和架构措施是需要成本的。在做虚拟化的成本估算时，一定要周全地考虑这些成本因素，以免中途碰到令你惊讶的花费。

*(作者: Sander van Vugt 译者: 涂凡才 来源: TechTarget 中国)*