VMware vSphere
技术指导手册

新虚拟化平台 VMware vSphere 技术指导手册

什么是 VMware vSphere？它主要有哪些新功能？如果升级到 vSphere，硬件要求是什么？如何创建 VMware vSphere 子操作系统？如何确保 VMware vSphere 的安全？VMware vSphere 的亮点究竟在哪里？

2009 年 4 月 21 日，VMware 公司宣布推出新一代虚拟化平台 VMware vSphere。这是 VMware 继三年前发布 VMware ESX 之后的又一重大举措。在本期技术手册中，我们将详细介绍 VMware vSphere，从下面几个方面进行探讨：

- vSphere 新闻
- vSphere 技巧（更新）
- vSphere 分析
- vSphere 安全（新增）
- 相关报道（新增）
- 更多技术资料

vSphere 新闻

VMware 于 4 月 21 日发布其下一代虚拟化平台，这个新品到底意味着什么？到底叫做什么？是 vSphere 吗？还是 VMware Infrastructure（VI4）或者 ESX 4？

- **VMware 将于本月发布 vSphere**

vSphere 技巧（更新）

VMware vSphere 有哪些新功能？如果你需要升级到 VMware vSphere，那么你的硬件需要满足什么样的要求？在升级之前，你应该如何进行测试？部署的时候该如何创建 vSphere 子操作系统？

- VMware vSphere 4 的特性分析
- 分析升级到 VMware vSphere 的硬件需求
- VMware vSphere：先测试后部署
- 如何创建 VMware vSphere 子操作系统？
- 如何使用 vSphere ESXi 的命令行？

vSphere 分析

尽管 vSphere 的 vCenter 提供了许多有用的新功能，但是有三个小功能，对于 VMware Infrastructure 3 和管理员来说最需要的。还有，你了解 vSphere 的许可信息吗？

- 分析 vSphere vCenter Server 的实用功能
- vSphere 的许可分析

vSphere 安全（新增）

使用 VMware 的 VSpere 4.0 中特定 iSCSI 启动程序验证能够在不限制系统功能或者控制灵活性的情况下增强安全性。VMware 把对虚拟机安全问题的研究方向集中在两个主要的 vSphere 组件上：VMsafe 和 vShield Zones。本部分详细论述如何增强 vSphere 的安全。

- 对 VSphere iSCSi 启动程序验证进行修改以增强系统安全
- VMware vShield Zones 组件及其工作原理介绍
- 如何安装和配置 vShield Zones？
- 管理 vShield Zones 的最佳技巧（上）
- 管理 vShield Zones 的最佳技巧（下）
- 如何在数据中心中安全部署 VMsafe 虚拟设备？

相关报道（新增）

本部分报道与 VMware vSphere 相关的新闻。

- VMworld 2009：存储厂商展示支持 vSphere 4 的新品

- VMware 降低 vSphere 4 价格吸引 Virtual Iron 用户
- F5 Networks 添加 vSphere 与 vCenter 集成
- VMware 发布众所期待的 VMsafe 安全 API

更多技术资料

这一部分提供更多的关于 vSphere 的技术资料。

- vSphere 官方技术手册
- vSphere 实施视频
- VMware ESXi 技术指南

深度厂商资源

下面的信息由 VMware 中国特别提供。

- vSphere 产品页
- VMware ESXi 产品
- VMware View 产品
- VMware 新闻动态
- VMware 奖项

VMware 将于本月发布 vSphere

VMware 将于本月 21 日发布其下一代虚拟化平台，与思科和英特尔展开竞争。

随着发布的临近，VMware 用户和合作伙伴都希望这家公司能结束这几月以来对这款产品的猜测，这个新品到底意味着什么？到底叫做什么？是 vSphere 吗？还是 VMware Infrastructure（VI4）或者 ESX 4?

VMware 的新版本

在过去的几个月中，VMware 揭露了其下一代平台的细节。在二月举行的 VMworld Europe 大会上，VMware 展示了许多新产品和功能。在其官方博客里也透露些新版本的情况，

因此我们知道一些事情。hypervisor 本身是 64 位的，提供对每个虚拟机高达 256GB 的 RAM 的支持以及对多路虚拟对称多处理技术的支持。在管理方面，可以聚集 vCenter 服务器，并且用户能够使用新主机档案和子机模板创建和配置虚拟机。

在存储方面，vSphere 带有新的可插的存储架构，允许环境直接利用存储阵列的本地功能，并将存储管理直接整合到 vCenter 客户端。vCenter 也提供对存储消耗更好的可视性，支持瘦磁盘，并包括关于 Storage VMotion 的图形用户界面。

另一个大领域的改进是网络，这是由于使用新的分布式虚拟交换机和思科专有 Nexus 1000V。使用分布式虚拟交换机，管理员只需要设置一次主机和虚拟机网络，而不是在集群里的每个主机上都要设置。

除了核心 ESX 和 vCenter 产品，VMware 也将发布一些新的辅助产品，包括期待已久的 VMware Fault Tolerance 以及对运行在虚拟机里的应用的性能管理工具 AppSpeed。VMware 也可能发布 VMsafe 应用程序接口，这将使安全厂商将 ESX 紧紧捆绑于产品中。

用户需求

与 VMware 用户交流时，很难确定哪个功能最突出。不过很明显，新存储、网络和高可用性功能都是很重要的。

政府的一名技术架构管理员 Terry Baker 期待 VI4 的可插存储架构能够启用，这样就能实现存储多路径。目前，VMware 提供了非常有限的对于存储区域网络（SAN）多路径的支持。不过在新版本中，可插的存储模块将使 SAN 厂商供应他们自己的多路径软件。因此，作为 EMC 的客户，Baker 所在的单位就能执行 EMC 的 PowerPath 多路径软件。他说：“这是我们期待很久的事。”

同时，新的分布式虚拟交换机承诺能够节省大量时间，一名 VMware 管理员 Bob Plankers 说。“我花费许多时间配置交换机，并且我只有 12 台服务器。我甚至不能想象如果我有上百台服务器该怎么办。”

财富 1000 强公司中的高级架构师 Tom Becchetti 说 VMware Fault Tolerance 是最受期待的功能。根据 Becchetti 说，Fault Tolerance 将使他的公司为用户提供新的完全新级别的服务。

除了这些特殊功能，新版本还有许多亮点，也更容易使用，一所大学的 Plankers 这样说到。例如，Plankers 喜欢新的主机档案功能，这就不需要使用他开发了许多年的自定义脚本，并且新的 vCenter 窗口明显显示了存储消耗情况。他说：“这减轻了许多工作量。”

市场策略

但对于 VMware 的所有追随者，多数 VMware 用户仍然不知道即将发布的新版本。一个 VMware 的合作伙伴，也是一位咨询顾问师这样说：“可能只有我们的用户群体和我们的销售团队知道要发布新品，但我不确定他们是否知道。”

这个合作伙伴认为 VMware 的市场策略有失误。从最近的 VMworld 大会开始，这家公司只关注在相对抽象的概念上，如 Virtual Datacenter Operating System（VDC-OS）和私有云，这让合作伙伴不相信会发布新品。

“这种方式丢失了销售先机，我认为 VMware 应该先从‘我们下一代的 ESX 怎么样’开始，再到‘云架构、软件即服务和架构即服务”。

因此，“像我这样的咨询工程师对于这些新功能和改进非常高兴，”一般的用户就没那么兴奋。“对于我来说，预测这个新一代产品有多少人使用很难。”

（作者：Alex Barrett 译者：唐琼瑶 来源：TechTarget 中国）

VMware vSphere 4 的特性分析

随着 vSphere 的发布，VMware 持续强调这个企业级 hypervisor 是成熟的。这强调了 VMware 决定注重的方面：补充其产品。VSphere 对 VMware ESX 3.5 作出的主要更改包括稳定性、可用性和安全性，这些都是服务而不是 hypervisor 功能。

VMware 已经发布官方申明，最新的产品套件围绕着其龙头产品 VMware ESX 建立，叫做 VMware vSphere。有了 vSphere，VMware 将其 hypervisor 定位为虚拟数据中心操作系统或者 VDC-OS。与先前的版本相反，许多新功能几乎是与单个系统相关的，新的 vSphere 几乎以服务为导向，通过 VMware 的名字选择就能看出来：Application vServices 和 Infrastructure vServices。Application vServices 是提供增强性可用性、稳定性和安全性的产品。作为一个整体，Application vServices 位于 Infrastructure vServices 之上，如 vCompute、vStorage 和 vNetwork。

在本文中，TechTarget 中国的特约虚拟化专家 Gabrie van Zanten 将介绍这些服务，并介绍 VMware vSphere 4 的新功能。

Application vServices

当涉及到业务应用，终端用户不关心运行应用的硬件或者运行应用的操作系统。用户希望应用作为服务运行，因此，主要的关心问题是在需要时服务是否可用，有多安全，什么时候需要更多的能耗和资源，扩展性能如何等。有了 Application vServices，VMware 在这些领域的每一个中都添加了新功能。

可用性

- **VMware Fault Tolerance**（VMware FT）。当需要增加可用性时，许多公司考虑集群技术，但这种技术很复杂。应用也必须运行在集群里，并能感知集群，但应用很少能做到。使用 VMware FT，虚拟机能在单独主机上使用“ghost”副本运行在 lockstep 里。如果出现问题需要虚拟机故障转移，故障转移马上就会发生。

每台虚拟机都可启动 VMware FT，目前的版本只需要花费 10%的性能。VMware FT 只运行在单个虚拟 CPU 的虚拟机里。这个技术最有用的部分在于虚拟机不需要感知 VMware FT，你也不需要对操作系统和应用作出任何修改。

- **VMware Data Recovery**（VMware DR）。VMware DR 使在文件级别和虚拟机级别备份和存储虚拟机数据更容易。VMware Disaster Recovery 比 VMware Consolidated Backup（VCB）提供了更高颗粒度。除了有图形用户界面（GUL），现在更容易指定备份、定义保留策略和执行恢复，只需要鼠标点击几下就能做到。VMware DR 是无

代理的，能使用重复数据删除技术存储增量备份。使用 VMware DR 有助于成本效益的存储管理。

安全性

- **VMware VMsafe**。如果环境中的每台虚拟机不需要本身的杀毒软件和恶意软件扫描该有多好！VMware VMsafe 是一个应用程序接口，能让安全厂商在影响到虚拟机之前扫描所有内存和网络流量。使用这种技术，病毒在影响到虚拟机之前就被截获，预防衍生物。对整个主机只进行一次扫描比对主机上的每个字操作系统进行扫描更好。
- **VMware vShield Zones**。作为管理员，你可以创建 VMotion、网络和配置感知的 vShield 信任区。换句话说，从一台主机迁移到另一台的虚拟机能受到来自网络外面的区域保护。分配给区域的虚拟机可能只能移动到另一台拥有相同渔区配置和相同防火墙的主机。

可扩展性

- **热添加设备**。在先前的版本中，只有虚拟磁盘能添加到运行中的虚拟机。使用 VMware vSphere，可以在虚拟机运行时添加更多 CPU（内存）。网络和存储设备也能进行“热添加”和“热移除”。通过这样的方式扩展虚拟机，由于给虚拟机添加内存时没有宕机，这就增加了应用的可扩展性。
- **新虚拟机限制**。能给与虚拟机的能耗最大值也增加了。在 VMware vSphere 里，虚拟机能最多拥有 8 个虚拟 CPU 和 255GB RAM。更多应用现在是运行在虚拟环境中的合适选后者。例如，用户可能不能在 VMware ESX 3.5 里运行大型 Microsoft SQL 数据库或者 SAP，因为 ESX 3.5 最多支持四个 CPU。现在虚拟机拥有八个 CPU，虚拟化这样的数据库或者 SAP 就可行了。

Infrastructure vServices

在基础设施层有几大改变，这就是 VMware 所指的 Infrastructure vServices。VMware 创造了三个焦点领域：vComputer、vStorage 和 vNetwork，这些新功简化了管理员的工作量，包括 Application vServices 的植入。

VMware vComputer

- **主机限制**。要使用 vSphere，主机最大需要有 512GB 的可访问 RAM 和 64CPU 核心，也就是说每台主机可以运行大量虚拟机。每核心运行三到四台虚拟机很正常，因此现在每台主机可能运行 192 台虚拟机。
- **网络和存储堆栈改良**。结合使用 Intel 的“Nehalem”处理器和 VMDirectPath 技术，允许 vSphere 跳过网络接口卡（NIC）的模拟，直接映射物理 NIC 到虚拟机，达到最大网络访问速度。使用改良的存储堆栈，vSphere 应该能达到每秒 40 万输入/输出操作，提供低于 2 毫秒延迟。

- **分布式电源管理（DPM）**。使用 DPM，当集群的负荷非常小的时候，可以将 vSphere 主机置于待定模式。DPM 将整合虚拟机腾出一台或更多主机，关闭这些主机以降低能源消耗。如果集群上的负荷增加，DPM 自动启动待定的主机。

VMware vStorage

- **连接的克隆和精简配置**。以前 VMware ESX 使用存储的方式导致经常要求存储空间，其实根本用不了那么多，这就浪费了存储空间。精简配置则杜绝了管理员的猜测，而不会导致存储过量使用。结合使用 Linked Clones 技术——相同磁盘上可以存储大量虚拟机。VMware 宣称使用其更新的虚拟机存储方法可以节省的存储空间能达到 50%。
- **存储提醒和监控**。在 VMware Infrastructure 3 里，vCenter 对精确的存储使用率小有远见。现在也提高了，在 vCenter 里的存储分配与消耗有更好的报告和告警。

vNetwork

- **分布式 vSwitch**。从 VMware ESX 2 起，分布式 vSwitch 就是管理员所需求的。在一台主机上创建一个虚拟交换机，并让其与其他所有主机上的 vSwitch 同步是复杂的。Distributed vSwitches 解决了这个问题，因为在分布式交换机上作出的更改将自动在所有主机上更新。这大大减轻了管理虚拟基础设施的负担。较少的管理任务意味着更少的错误和更多的运行时间。
- **第三方虚拟交换机**。除了 VMware 新植入的分布式 vSwitch，vSphere 也支持第三方虚拟交换机。思科是第一个对 vSphere 提供支持的厂商，发布了 Nexus 1000V。从思科购买一个独立许可证之后，就可以使用网络密匙激活 Nexus 1000V，网络管理员就能完全管理虚拟环境里网络的各个方面，而不需要让 VMware 管理员进行以前必要的配置。这也减轻了管理和减少了配置错误的风险。

附加的产品更新

这只是主机方面新功能的一部分，不过也有对业务操作有重大影响的更新。vCenter 的新版本有大量的改进，在 VMworld Europe 2009 大会上，VMware 宣布了其他的新服务，如 AppSeed 何 Chargeback，这些将在今年发布。这些服务主要从虚拟架构管理工具升级 vCenter，让其成为一个有额外价值的工具。

（作者：Gabrie van Zanten 译者：唐琼瑶 来源：TechTarget 中国）

分析升级到 VMware vSphere 的硬件需求

VMware ESX 的下一版本只能运行在 64 位 CPU 上。因此你可能疑惑你目前的硬件是否是 64 位 CPU，以便你能升级到 vSphere。

首先我们来看看什么是 64 位 CPU。在 CPU 中，术语 bit 指的是处理器存储器能存放的数据数量。因此在 64 位 CPU 上的每个处理器存储器能存放 64bit，而 32 位 CPU 的存放 32bit。bit 是测量信息存储的最小单位。一 byte 通常包括八 bit。多数 x86 服务器都是 32 位或者 64 位的。如今，几乎所有的企业服务器都有 64 位 CPU，不过许多较旧的服务器拥有 32 位 CPU。

拥有 64 位 CPU 的能运行 32 位和 64 位操作系统和应用。许多操作系统都有 64 位和 32 位版本，基于服务器硬件使用情况安装。不像有 32 位和 64 位 CPU 的不同版本的操作系统和应用，VMware ESX 3.x 默认下都支持，就没有必要安装某个版本。不过 VSphere 只能运行在 64 位 CPU 上。如果你将 VSphere 安装在只有 32 位 CPU 的服务器上，就会出现下面这样的错误信息：

为了解释这个图像，32 位版本指的是 ESX 3.5.x，因为它只支持 32 位 CPU，vSphere 只支持 64 位 CPU。你可能也怀疑“long mode”是 64 位 CPU，能在两个模式里运行：egacy 和 long mode。当操作处于 legacy 模式，CPU 仅仅运行 32 位代码，64 位没用使用到。当操作处于 long 模式，CPU 能运行本身是 64 位的应用，也以一种兼容的模式运行 32 位应用。

ESX 3.x 以 legacy 模式还是 long 模式运行取决于服务器所使用的 CPU 类型。VSphere 只能支持 long 模式，因此需要 64 位 CPU。VMware 这样做的原因在于增加可测量性和性能。

但是不是所有的 64 位 CPU 都相同。仅仅因为你拥有 64 位服务器并不意味着能在上面运行 64 位子操作系统。 x86 64 位架构旨在使用改良的内存模式，这种架构由 64 位地址空间组成，用在 32 位架构中的分段内存模式被移除。因此，这导致在虚拟主机服务器上的子操作系统出现问题。它们没有有效的机制来隔离来自 64 位子操作系统的虚拟机监控器。Intel 和 AMD 都已经在他们的 CPU 中添加了功能，以便以 Long 模式运行时支持内存分段，不过早期 64 位 CPU 模式没有这种功能。

Intel 和 AMD 服务器

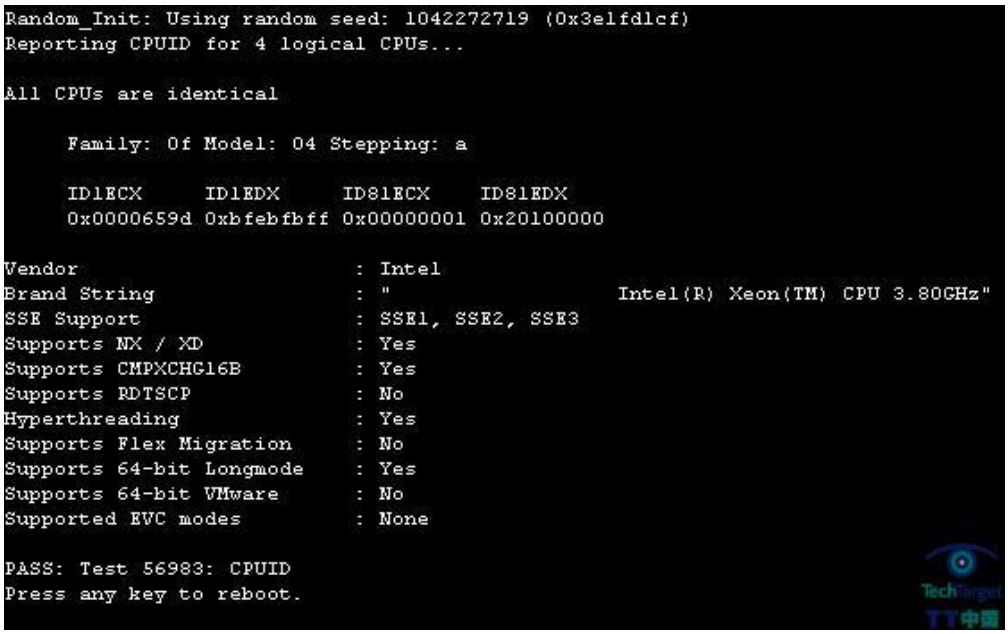
当以 Long 模式运行时，早期的 AMD64 CPU（C 版及更早版）丢失了内存分段支持，因此 D 版和后面发布的 CPU 要求运行 vSphere。如果运行在 AMD 皓龙处理器上，你需要 AMD 皓龙家族的 CPU Rev E 或者更后面的版本。此外，许多 AMD 服务器有个叫做 AMD-V（AMD 虚拟化扩展）的 BIOS 功能，这些服务器是必须支持 64 位子操作系统的。Intel CPU 需要 EM64T 和 VT 支持，以及服务器的 BIOS。EM64T 是 Intel 的 64 位技术， VT 是他们的虚拟化技术。Intel EM64T CPU 在 Long 模式下也没有内存分段支持，但是 VT 功能能允许 ESX 运行。

Intel-VT 和 AMD-V 功能默认情况下在服务器的 BIOS 里都是禁用的，因此检查 BIOS 查看是否禁用。这个设置的 BIOS 设置位置依赖服务器制造商的需求，但是一般位于高级或安全选项下面。如果在服务器 BIOS 设置没有看见这些选项启用虚拟化功能，这可能是由于服务器不支持，这种情况常见于较旧的服务器。或者你的 BIOS 版本应该升级了。与服务器制造商核对是否有较新的 BIOS 版本，以便升级后能启用这些高级功能。

需要 64 位处理器？

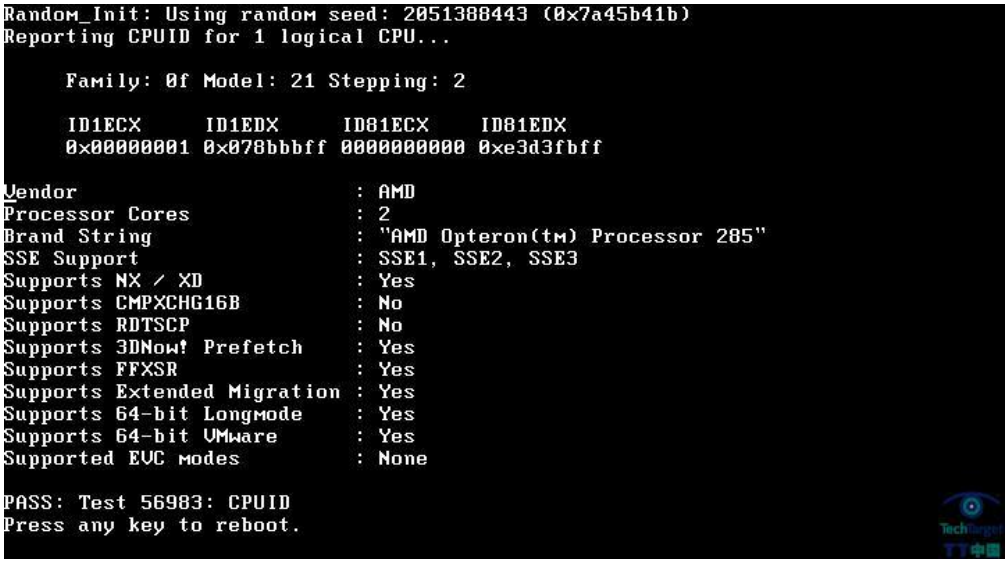
你如何查找你是否需要 64 位处理器？有几个可用的工具查看服务器，并看它们是否拥有 64 位 CPU 和运行 64 位子操作系统。第一个工具是 CPU 识别工具。这个工具是 VMware 提供的一个小型 ISO 文件，用以识别支持你主机的 CPU，并让你知道是否支持 64 位 long 模式和 64 位子操作系统。你可以将 ISO 文件刻录到 CD，或者使用远程管理面板启用，因此可以从 ISO 文件关闭和启动你的主机。

这个工具意味着直接运行在主机上，这就需要关闭它，不过我也加载 ISO 文件到子操作系统的虚拟 CD-ROM，从这启动得到相同的效果。我相信由于当多数子操作系统的硬件是一般虚拟硬件，CPU 通常作为牌子和在主机服务器里的任何模式显示。一旦运行此工具，如下图所示：



（注：点击图片本身查看原图）

在上面的 HP DL360 G4 例子中，你能看见它支持 64 位 long 模式，但是不支持 64 位 VMware 子操作系统。这意味着你能在服务器上安装 vSphere，但是只能在主机上运行 32 位子操作系统。下图是使用 AMD 皓龙 CPU 的 HP DL385 G1 服务器例子。



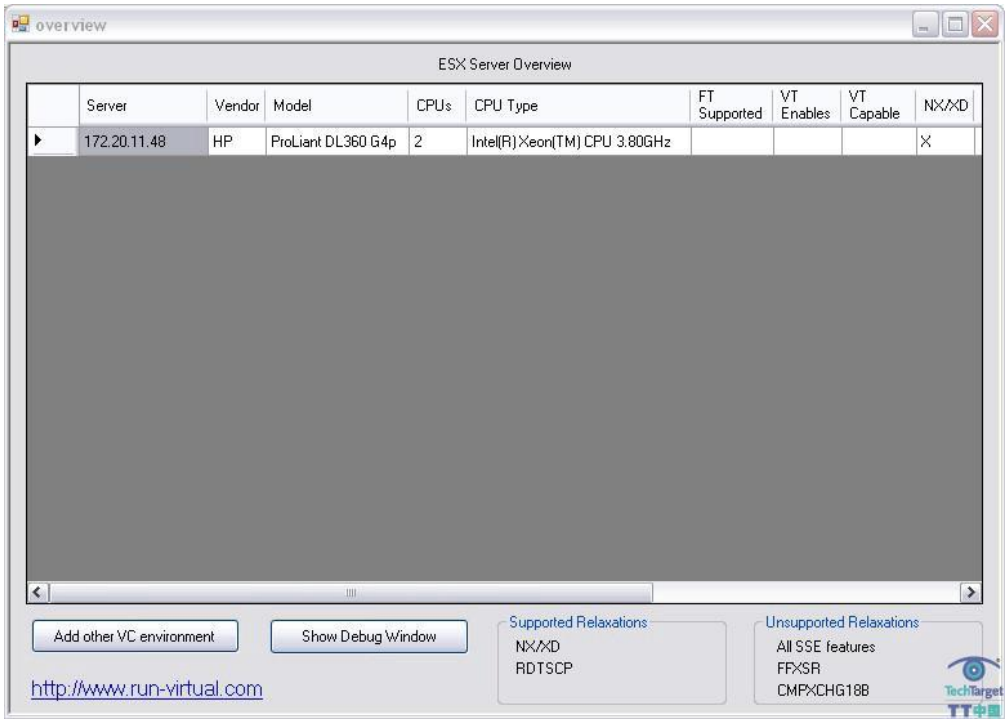
（注：点击图片本身查看原图）

这台服务器支持 64 位 long 模式 64 位 VMware 子操作系统，因此你能在其上安装 vSphere，并且运行 32 位和 64 位子操作系统。

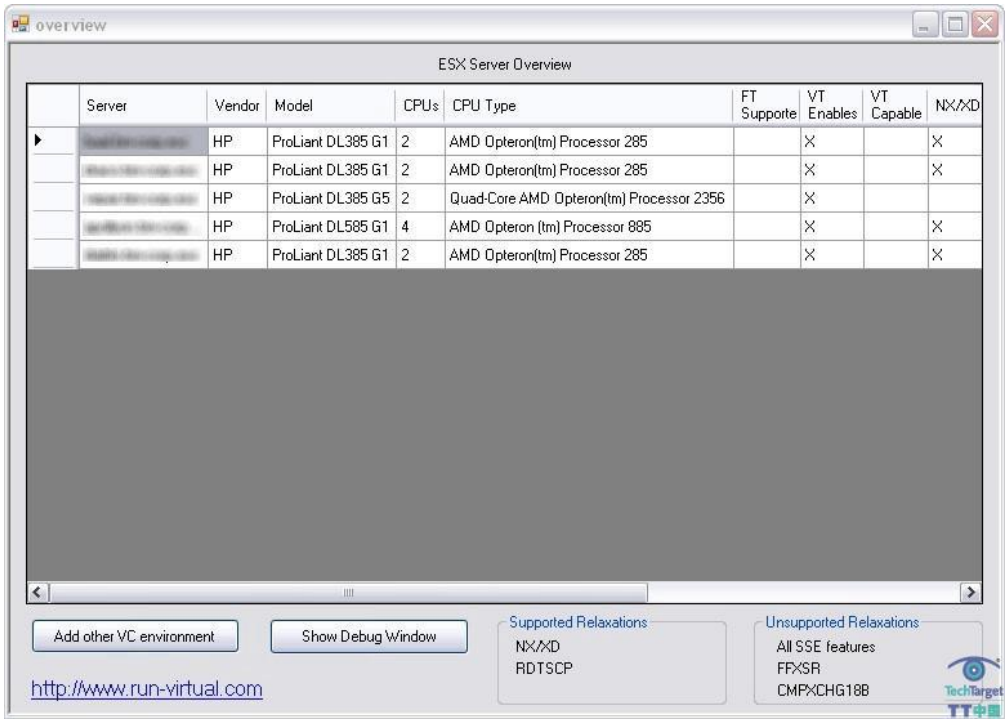
检查主机服务器 CPU 的另一种方法是使用工具 VMware CPU Host Info。这个工具能运行在任何工作站，连接 vCenter Server（尽管不过单独的 ESX 主机）和汇报每个主机的 CPU 性能。不过，这个工具只能说明主机是否有 VT 功能，或者是否能运行 64 位子操作系统。它不能告诉你主机是否支持 64 位 long 模式。

VMware CPU Host Info 通过使用 VMware Infrastructure SDK 从每台主机查询系统信息工作。然后以电子表格形式显示。这个工具的额外好处是能显示主机是否能与 vSphere 的新 Fault Tolerant（FT）功能工作，因此这个功能只与最新的 CPU 类型工作。一旦你下载并在工作站运行这个工具，可以指定想要连接的 vCenter Server，并且显示了由 vCenter Server 及其 CPU 信息所管理的所有主机服务器。

下图显示的在与先前相同的 DL360G4 服务器上使用这个工具的情形。它显示服务器没有 VT 功能，但没有告诉你服务器支持 64 位 long 模式，其实支持 long 模式。另一个圆柱显示是否支持 FT，是否启动 FT，以及存在各种各样的 CPU 功能。



下图显示的是使用该工具在另一台服务器上运行的样子。



注意，所有工具都报告了所有主机都有 VT 功能。我认为工具所写入的方式只显示主机是否支持 VT 或启用 VT，但是不能都显示。如果工具报告主机有 VT 功能，你可能需要修改它的 BIOS 设置以启用 VT 功能。

既然知道了如何查看主机以识别是否拥有 64 位 CPU，就能决定是否从 VMware Infrastructure 3 升级到 vSphere。了解你的服务器硬件及其支持范围将帮助你规划你的升级，并允许你升级所需的服务器硬件成本。

（作者：Eric Siebert 译者：唐琼瑶 来源：TechTarget 中国）

VMware vSphere：先测试后部署

VMware 主要的下一代数据中心虚拟化产品 vSphere 已经发布了。多数管理员喜欢新版本的操作系统和应用，并将其用于他们的环境中。我作为一名管理员，当我得到一个新产品，就像在圣诞节打开礼物那样高兴。在先前几个月，关于新版本的预测建立在最终版本上，我拍不急待地想安装它。许多管理员都在使用测试版本，以便熟悉 vSphere 并使用它，但是在升级到生产环境之前，管理员需要考虑到一些事项。

第一版的漏洞风险

首先，没有任何软件是完美的。几乎所有的新软件都有漏洞，随着时间推移，漏洞被发现，软件就随之改进。三年前，VMware Infrastructure 3 (VI3)才稳定。vSphere 是 VMware 最大的，与之前版本相比有许多更改。因为 VMware 想一直领先竞争者，由于它只有生产级别虚拟化平台，在这种情况下提前发布了其新版本。因此这个版本将包含未发现的漏洞。VMware 是否已经从时间炸弹漏洞吸取教训还待观察。只有时间能证明这个虚拟化领导者是否已经提升了质量保障和测试过程，以防止再次出现漏洞。

不管 VMware 是否已经做出改进，很难说这个软件没有漏洞，主要的代码更改将引发问题。Beta 版和内部测试旨在帮助识别这些问题。但在许多情况下，向公共发布软件是修复未发现漏洞和错误的唯一方法。新软件的早期采用者本质上是额外的测试者。同样，每个用户环境不能在软件发布之前进行测试，因此软件公司依赖用户识别公司可能忽略掉的漏洞。

由于这些因素，要谨慎使用新版本，尤其对于生产环境。一般来说，等待第一个升级或修复版本是好策略，许多在第一个新版本未发现的漏洞通过第一个修复版本可以修复。因此当考虑是否升级你的生产环境到 vSphere 时，首先想想这个生产环境的重要性，还有你是否能承担潜在的问题。

如果你担心采用 vSphere 会出现问题的话，可以首先升级到开发环境，并测试服务器，看运行得怎么样，没有问题的话再用于生产环境的服务器。这样可以获取使用 vSphere 的经验，而不用将生产环境置于混乱境地。或者，可以下载一个评估许可证，设置一个独立的环境来测试新版本。如果你用得很顺手，在环境里也很稳定的话，可以开始生产部署。

你有合适硬件吗？

另一个推迟升级到 vSphere 的原因是你可能没有所需的服务器硬件来运行它。不像 VI3 那样运行 32 位和 64 位 CPU，vSphere 只能运行 64 位 CPU。如果你的服务器硬件较旧，可能需要替换成新的才能运行 vSphere。此外，如果你计划使用 VMware 的新 Fault Tolerance（FT）功能，这个功能需要特定的 CPU 才能工作，并且集群里的所有主机必须

有兼容的 CPU。关于运行说明的更多细节和服务器硬件支持请查看我写的另一篇技巧“分析升级到 VMware vSphere 的硬件需求”。

如果你没有兼容的硬件，你需要在升级到 vSphere 之前进行计算。你应该也阅读了 VMware 硬件兼容列表（HCL），包括服务器、I/O、备份和存储设备。VI3 HCL 上的较旧硬件可能没有列于 vSphere HCL 上。如果你的硬件没有显示在 HCL 上，这不意味着不支持 vSphere。因此如果你使用不受支持的架构组件，VMware 帮不上忙。

现有 VMware 管理产品的兼容性

接下来，考虑 vSphere 与现有 VMware 管理和自动化产品，以及第三方厂商应用的兼容性。这包括来自 VMware 的产品，如 Lab Manager、Site Recovery Manager、Stage Manager 和 VMware View，以及来自 Vizioncore、PHD Technologies 和 Veeam Software 等第三方厂商的应用。此外，你还应该关注其他应用或者集成在虚拟环境里的进程，包括脚本、备份和监控应用，和其他使用的附件和插件。把这些应用做个列表，与厂商核实这些应用与 vSphere 兼容。多数厂商现在都与 vSphere 兼容，不过你可能需要升级到这些应用的新版本。

对 vSphere 没有充分了解，也没有经验，使用 vSphere 升级生产环境就是个错误。因此，由于 vSphere 较新，与 VI3 有明显差异，确保升级到 vSphere 之前对其有充足了解。在生产环境使用 vSphere 之前，学习如何正确配置、监控并修复它。确保对如何使用 vSphere 的新功能有了解，如主机档案和分布式 vSwitch 及其它新功能，还要了解如何修改服务器控制台命令。由于 vSphere 很新，目前没有 vSphere 培训课程，因此可以学习官方文档。阅读其他博客和网站的资源，许多作者都是测试参与者，对 vSphere 有一些了解，也有一些经验可供你参照。另外，使用评估许可证设置一个测试环境的方法很好，这样可以获取使用 vSphere 的经验。一旦出现培训课程，去参加培训是最佳选择。你可以从课程材料中受益，也可以得到具体的问题答案。

最后，在升级到 vSphere 之前，确保你了解升级路径和所有依赖关系。VMware 出版了每个版本的升级指南，解释了不同 VMware 组件之间的升级要求和依赖关系与兼容性。当你升级到新环境时，通常有个你需要遵循的升级指令。使用 VMware，通常以紧跟主机、数据存储和子操作系统之后的 vCenter Server 升级开始。如果不按照指令升级就会出现问题。例如 vSphere 主机不能由 vCenter Server 版本 2.5 管理。对于子操作系统，在升级目前虚拟硬件到新版本之前，可能需要升级 VMware Tools。

升级练习

在升级关键主机之前要进行练习。最好设置测试的 vCenter Server 2.x 和 3.x ESX 主机，将它们升级到 vSphere。如果需要，可以使用评估许可证。尝试创建一个新子操作系统测试 vCenter Server 的管理。一旦拥有升级每个组件的练习，就可以准备升级关键主机了。

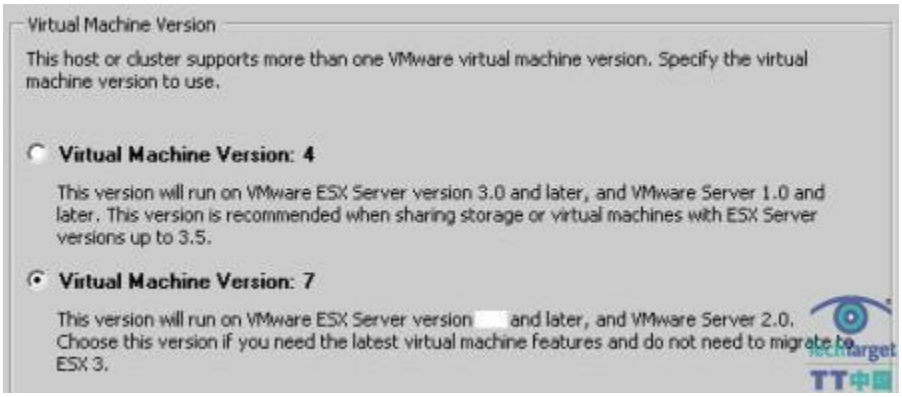
vSphere 承诺是个令人兴奋的版本，在部署之前要谨慎。确保你作了所有准备工作。对于新版本，我都会等待第一个升级或者三个月后再使用。在等待期间，可以查看 VMware 知识库和 VMTN 论坛，学习易经识别的问题和漏洞，并学习其他用户使用 vSphere 的经验。通过时间做好准备以及这个版本也越加成熟时候，你成功升级到 vSphere 的机率就更大了。

（作者：Eric Siebert 译者：唐琼瑶 来源：TechTarget 中国）

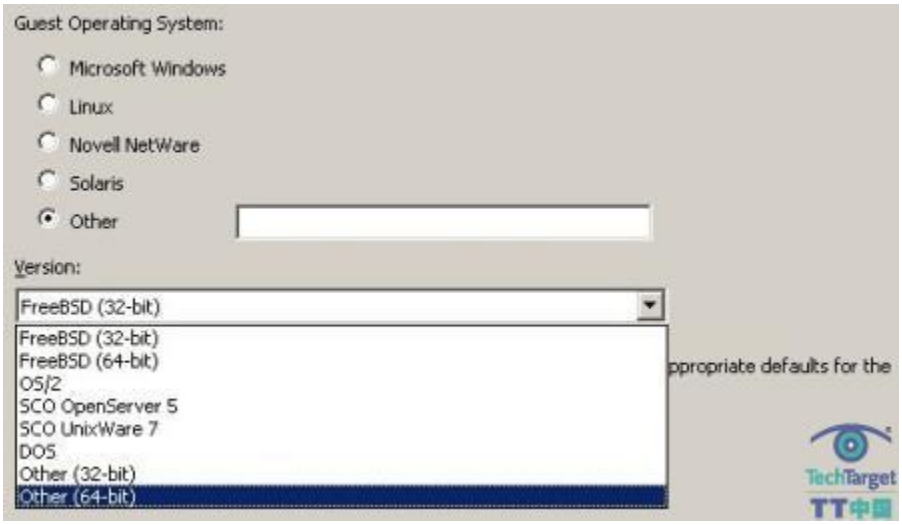
如何创建 VMware vSphere 子操作系统？

当你在 vSphere 的下一版本 VMware ESX 里创建虚拟机时，你能发现这个过程有大量的更改和改进。例如，有更多的操作系统选项和更多的网络适配器选择，你能创建精简配置磁盘。在本文中，TechTarget 中国的特约虚拟化专家 Eric Siebert 将讨论在主机 VMware ESX 服务器上创建新子操作系统的方法。

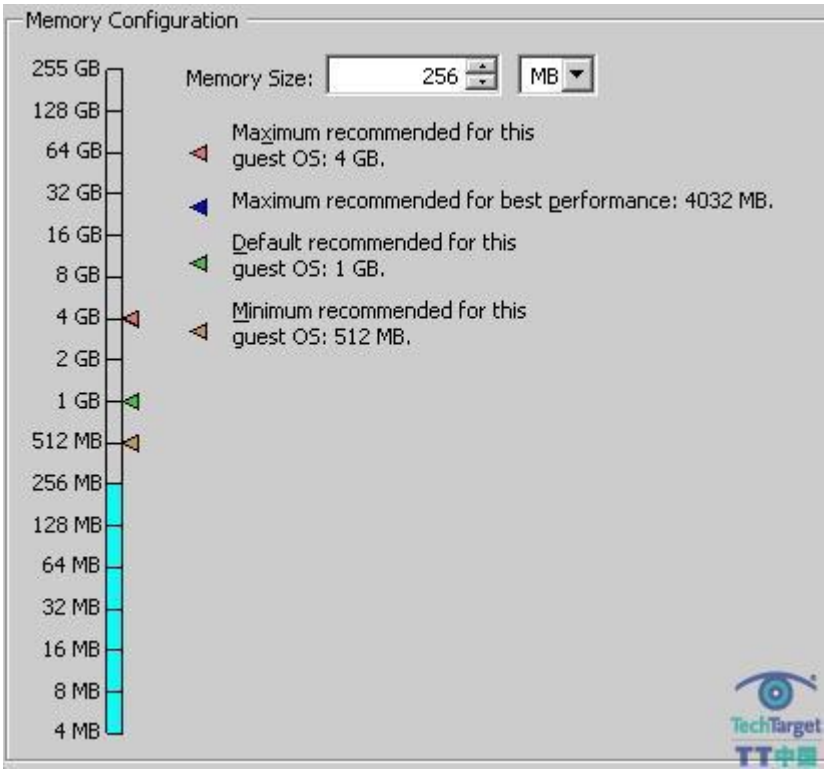
如果你选择自定义安装，你首先必须选择虚拟机版本 4 或 7。版本 4 用于后面与 ESX 3.x 和 Server 1.x 的兼容。版本 7 专门用于新版本 ESX，与 Server 2.0 也工作得很好。为什么 VMware 会选择 4 到 7 的版本？因为想让它与 Workstation 相一致，Workstation 目前的版本是 6.5，下一个版本据推测是 7。如果你选择一般安装，默认的就是版本 7。



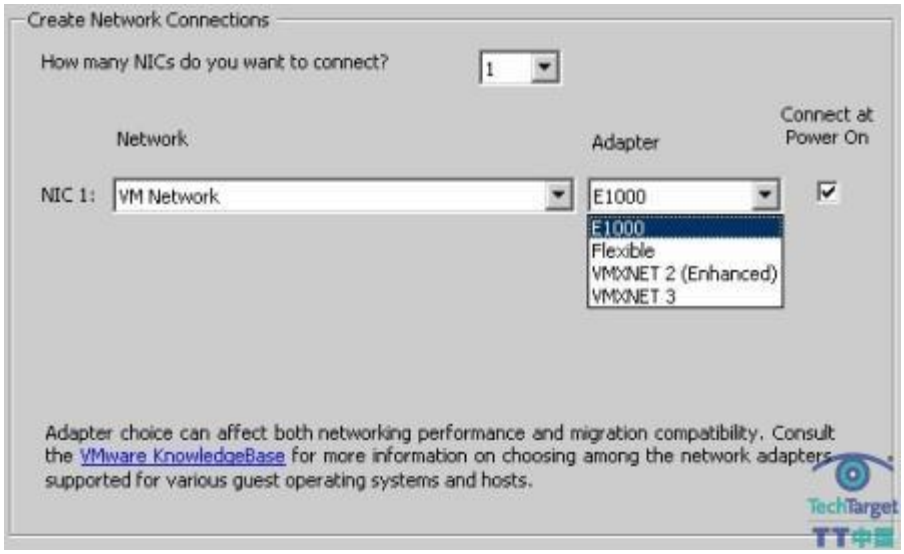
Guest Operating System Selection 这一屏比先前的 ESX 版本有更多的操作系统可选。有更多的 Linux 版本，现在更有“其他”目录，而不仅仅是 Other 32-bit 或者 Other 64-bit。这个选择屏幕不能为你安装操作系统，反而能用于在向导里设置适当的默认值，如所需的内存数量，调整最佳操作的设置， 并与子操作系统里某个行为和漏洞工作。



为操作系统选择内存数量的屏幕稍微有所不同，有一个新的色块滑动器。

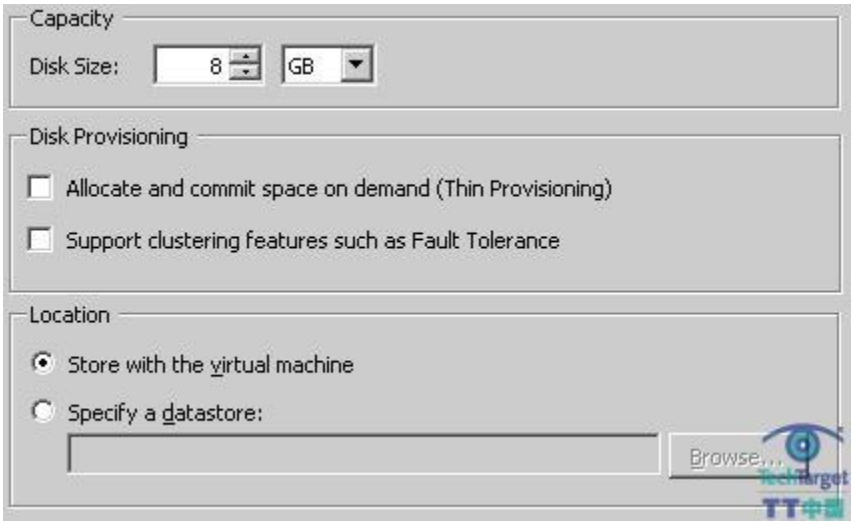


为子操作系统添加网络适配器有更多的选择。所显示的选择是基于虚拟机的操作系统类型，在新版本中，有一个新的 VMXNET 版本 3 适配器。

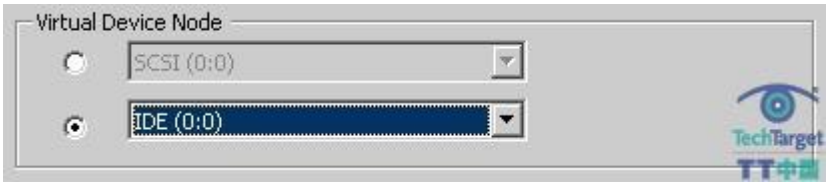


也有更多的 SCSI 适配器类型可选。除了标准的并行适配器类型——BusLogic 和 LSI Logic——你现在能选择 LSI Logic SAS（串行附属存储）或 VMware paravirtual。VMware paravirtual 是性能更高的适配器，只支持特定操作系统（Windows 2003 和 2008，还有 Red Hat Enterprise Linux 5），但不能使用某些功能，如高可用性（HA）和分布式资源调度（DRS）。

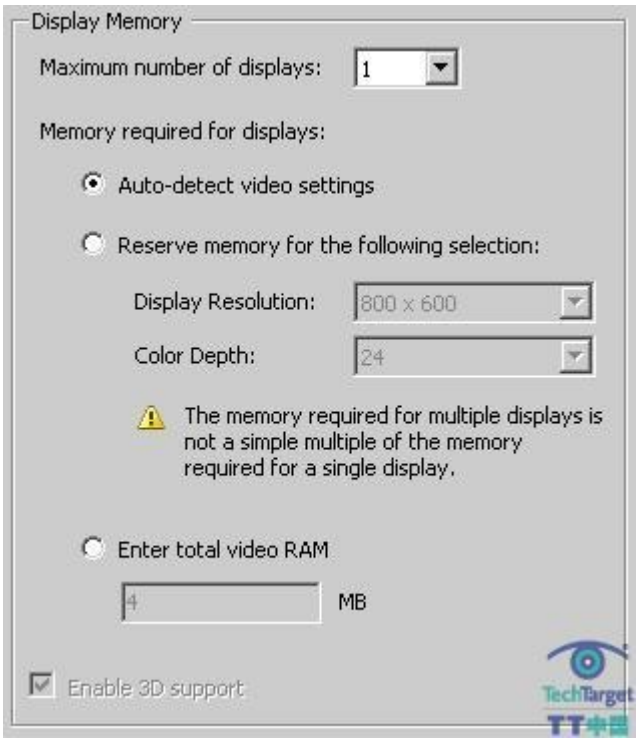
在为子操作系统创建新虚拟磁盘时，你现在可以选择创建精简配置磁盘。以前你只能创建瘦磁盘，使用命令行 vmkfstools 工具按需分配磁盘空间。瘦磁盘开始很小，随着磁盘块写入子操作系统而增大。



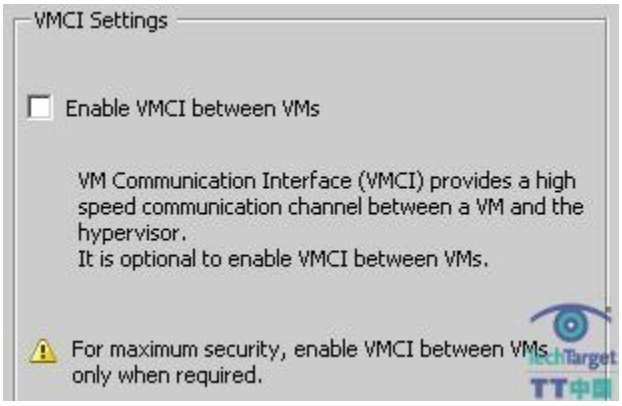
在虚拟磁盘高级选项里，你现在能为子操作系统在集成电子驱动器（IDE）或者 SCSI 磁盘中作出选择。以前只有 SCSI 磁盘能用于 ESX 主机。IDE 磁盘使用标准的 IDE ATAPI 控制器，也可用于虚拟 CD/DVD 驱动。如果你选择使用 IDE，那么你先前所选择的 SCSI 适配器在虚拟机创建的时候自动移除。



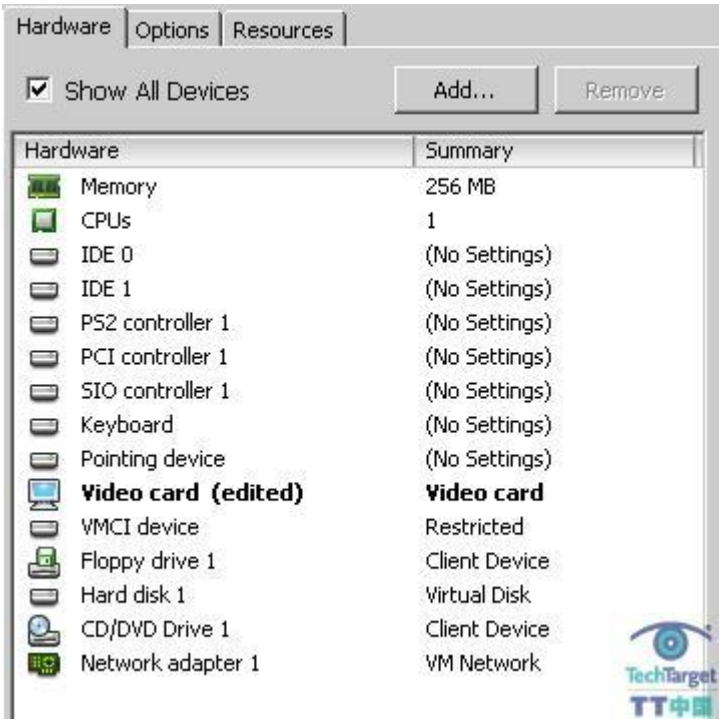
创建新子操作系统之后，可以编辑设置，并更改一些不能访问的硬件。视频显示卡已经设置，可以调整使用一些高级配置，包括设置分配给它的 RAM 数量，显示器数量，分辨率和颜色深度。这对于服务器操作系统不是特别有用，这是专门让虚拟桌面拥有更好的图形功能。以前的视频显示卡被隐藏，并且不能配置。



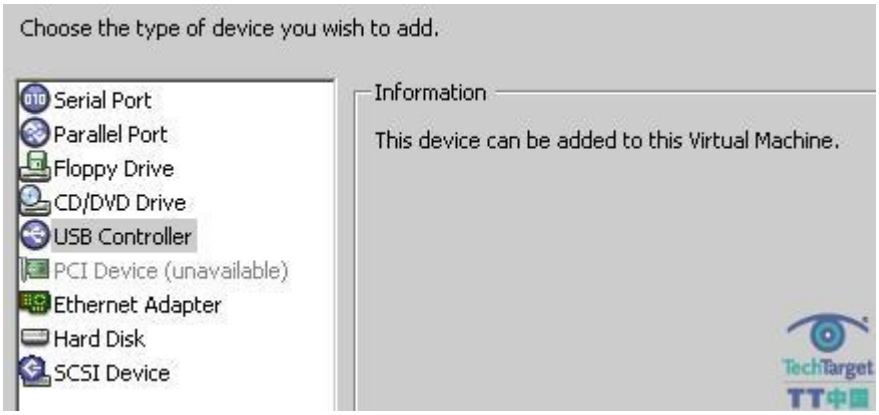
在这里也能看见一个 VM Communication Interface（VMCI）设备，支持子操作系统及其主机服务器或者相同主机上的多个虚拟机之间的快速和有效的通信。这个功能作为 Workstation 6.0.x 里 VMware Tools 的实验功能包含其中，在 Workstation 6.5 将被弃用。你可以在 VMware 网站上查看该功能的更多细节。



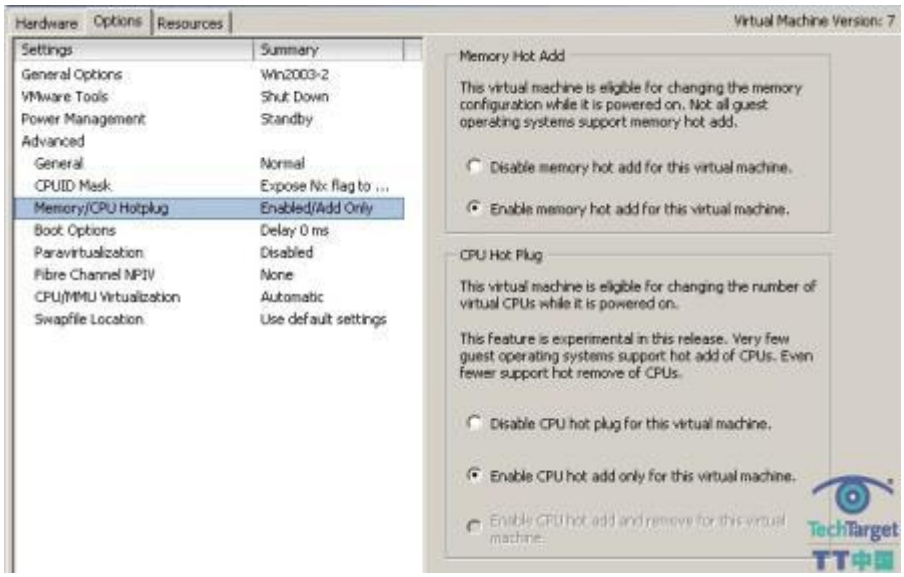
显示所有子操作系统通常隐藏和不能配置的额外硬件有新的选择。这包括 IDO 和其他控制器，以及键盘和鼠标。



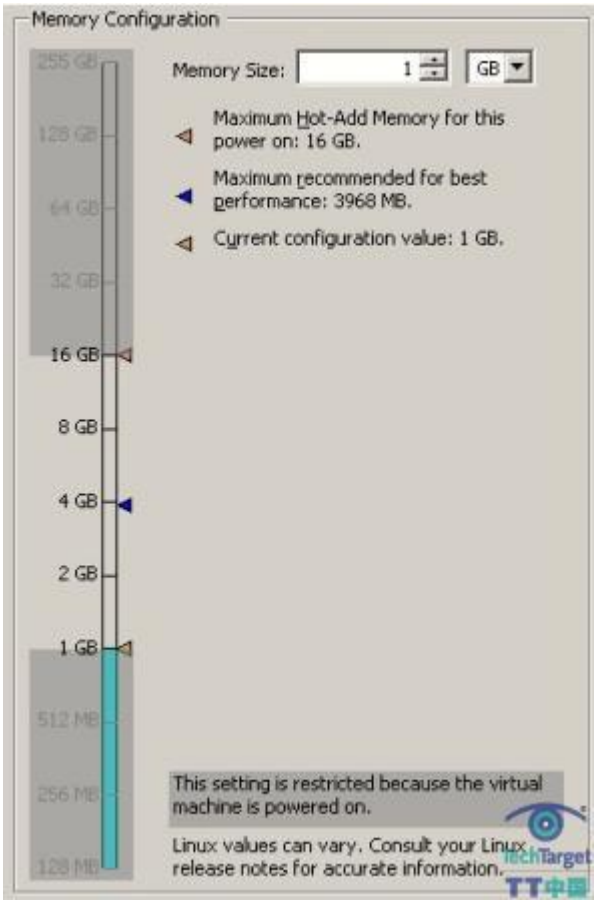
如果你添加了新设备，你现在能创建 USB 控制器，这允许你附属 USB 设备（例如，可移动存储、许可密匙（植入安全认证机制）将主机服务器连接到子操作系统。以前，USB 设备不能与子操作系统一起使用。



在子操作系统设置的 Advanced Options 选项中，你能启用内存热添加与 CPU 热插入功能。由于这些功能不是受所有操作系统的支持，只能基于你先前所选的子操作系统类型显示。受支持的操作系统包括 Windows Server 2003 Enterprise 和 Datacenter、Windows Server 2008 和某些 Linux 版本。不过，Windows 操作系统内存只支持内存热添加，取决于你所选的 Linux 版本，可能只支持内存热添加或者两者都支持。



一旦启用内存热添加功能，如果虚拟机操作系统支持，在虚拟机运行的时候就能调整子操作系统内存大小。



如你所见，在下一代 ESX 中，创建子操作系统有许多新功能。

（作者：Eric Siebert 译者：唐琼瑶 来源：TechTarget 中国）

如何使用 vSphere ESXi 的命令行？

在需要保证 VMware 服务器相同配置的要求下，使用命令行工具来配置大量主机是非常有必要的。目前 vSPhere 已经面世，并且命令行选项多种多样。所以 VMware 管理员需要掌握一些命令行方法才可以管理其工作环境。

本文介绍在服务器指定给 vCenter 服务器管理之前，通过该服务器的免费许可证和脚本预配置工作，使用 ESXi 4 命令行的方法配置主机以独立使用。

激活 ESXi 4 上的命令行接口

如同在 ESXi 3 中一样，命令行接口（CLI：Command-Line Interface）也是不可用的，除非知道如何激活和访问 CLI。ESXi 默认配置在 vmkernel 界面上开始，如下图 1 所示：

点击放大

F2 和 F12 选项允许进行基本网络和系统事件配置，但并不是允许可以进行任何操作。使用 Alt-F1、输入“unsupported”，然后点回车键，就可以激活本地控制台提示符。之后再需要输入根密码，接着就可以进入 ESXi 主机的本地控制台界面，如图 2 所示：

点击放大

现在就可以通过 HP 公司的 Integrated Lights-Out 或者 Dell 公司的远程访问控制器（DRAC：Dell Remote Access Controller）管理接口等诸如此类的工具运行命令或者激活 ESXi 主机的安全 Shell（SSH），点击如下链接可以得到关于如何激活 ESXi 主机上的 SHH 详细说明。

使用 esxcfg-vswitch 配置虚拟交换机

这个命令的基本功能后项兼容于 ESXi V3（这一点非常不错）。因此很多过去为 ESXi V3 所写的创建标准虚拟交换机的脚本程序在两类工作平台中都可以良好的运行，尤其是在相同的物理硬件设备上执行就地升级的话，这个功能更是非常必要。然而这个命令有很多新的参数，并且相当一部分参数都是为了支持新 Nexus 1000V 虚拟交换机而设置的。esxcfg-vswitch 命令有两个主要新参数并不适用于 Nexus 1000V，即 - x 和 - X，这两个参数分别表示显示交换机上行线路的最大数量和配置交换机上行线路的最大数量。这里是指指定给 vSwitch 和 vmnics 的接口数目，而不是虚拟交换机的端口数目。

如果不使用 Nexus 1000V 虚拟交换机的话，为 ESX 3.x 和 ESXi 3.x 所写的很多脚本都可以很好地翻译给 Sphere 使用。点击如下链接可以获得更多关于如何为虚拟网络的创建写脚本程序的更多信息。但是如果倾向于使用 Nexus 1000V 虚拟交换机的话，esxcfg-vswitch 命令的新选项对 DV 端口也是可用的。

使用 esxcfg-mpath and esxcli 对内部进行多路径修改

由于虚拟交换机命令和以前的版本非常相似，vSpere 中 Multipath 命令接口是不同的。我曾经使用 esxcfg-mpath 执行两项主要任务：从虚拟存储设备中获得逻辑单元号（LUN）序列号和通过脚本的接口设置多路径策略。

在基于虚拟机文件系统（VMFS：Virtual Machine File System）的共享存储中（iSCSI、本地、光纤通道）使用到三种多路径策略：最近经常使用、固定使用和循环复用。如果多路径输入/输入（I/O）在共享存储设备上是一个选项的话，我经常把固定使用或者最近常用默认状态修改为循环复用。VMware vSpere 把循环复用带出了实验模式，现在可以通过 esxcfg-mpath 命令进行配置。对于 ESX/ESXi V3 服务器，使用如下命令可以修改 LUN 为循环复用多路径策略：

```
esxcfg-mpath --policy=rr --lun=vmhba2:0:1
```

然而， esxcfg-mpath 命令在 vSpere 中并不是特别有帮助。为了在 ESXi 4 系统上执行同样的多路径策略配置，需要使用 esxcli 命令。令人耳目一新的是，esxcli 是字符驱动型命令。Esxcli 命令对多路径空校验非常直接。如下命令可以列出所有卷的多路径策略：

```
esxcli nmp device list
```

如下图 3 所示的是对拥有一个本地 VMFS 卷和一个 iSCSI VMFS 卷的 ESXi 4 主机使用该命令后的显示结果（黄色标识的是策略）：

点击放大

为了把 iSCSI LUN 上的策略改为循环复用，我们需要知道设备的完整名字。LUN 的长名字可以在问题中包括路径部分的第一行中找到，如上图中绿色标识的部分。如下命令可以把有问题的 LUN 双方都转化为循环复用：

```
esxcli nmp device setpolicy --device
     t10.F405E46494C45400155716660743D2D6753583D203054496
     --psp VMW_PSP_RR
esxcli nmp device setpolicy --device
     t10.F405E46494C45400969407E61726D2A6457586D2633477E4
     --psp VMW_PSP_RR
```

一旦接受这些命令之后，VMFS 卷的配置就修改为循环复用了。图 4 显示的是这个配置：

点击放大

对于用 VMFS 卷进行光线通信存储，循环复用更适合于作为标准设置。iSCSI 的列子例子显示该命令的语法。Esxcli 命令有很多选项，例如可以对具体的字节数目或者 I/O 操作（这是推动存储驱动进行下一步的开始）设置策略。点击 VMware 网站上的这个链接获得更多关于 vSpere CLI 参考文献的信息。

激活 iSCSI 存储设备和扫描磁盘

通过命令行可以配置 ESXi 4 主机以激活 iSCSI 存储设备和扫描磁盘。作为先前安装的脚本的一部分以及配置网络接口和虚拟交换机，这些命令非常有用。如下命令可以激活 iSCSI 引导程序，并且在之后进行扫描：

```
esxcfg-swiscsi  -e
esxcfg-swiscsi  -s
```

控制台上的显示如图 5 所示：

点击放大

在这个命令完成之后，配置 ESXi 服务器上的存储适配器。虽然因为 VSpere 和 ESXi 非常相似而比较熟悉，但是很多配置部分还是不同的，并且在管理员对迁移到新平台完全准备好之前需要一些规划和测试。

相关专题：VMware vSphere 技术指导手册

（作者：Rick Vanover　译者：王越 来源：TechTarget 中国）

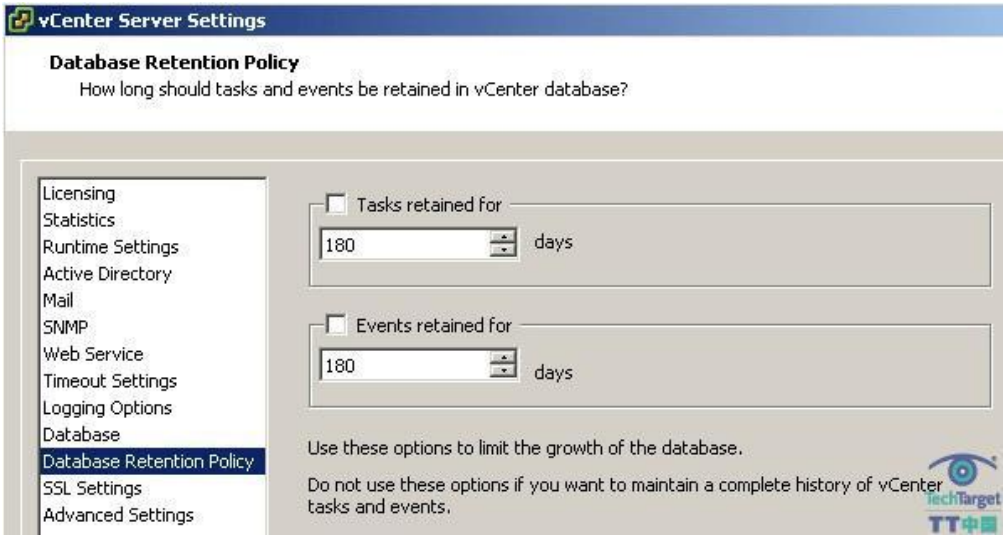
分析 vSphere vCenter Server 的实用功能

尽管 vSphere 的 vCenter 提供了许多有用的新功能，但是有三个小功能，尤其对于 VMware Infrastructure 3 来说最需要的，所以我很高兴这个版本的发布。

第一个能解决 vCenter Server 数据库数据太多的问题。vCenter Server 数据库的大部分数据来自子操作系统和主机历史性能参数，还包括任务和事件数据。统计数据在每个间隔设置存档，因此对数据增长有所限制，不过任务和事件数据将永远保存在数据库，甚至包括从 vCenter Server 目录删除的子操作系统和主机所遗留的数据。

没有简单的办法从数据库清除这些旧数据。VMware 为 VI3 提供了 SQL 脚本，你可以修改并运行用以完成清除数据的任务，但是这种方法很复杂。VMware 现在添加了清除旧有任务和事件数据的功能，可以直接从 vSphere Client 清除，消除了使用脚本的要求。

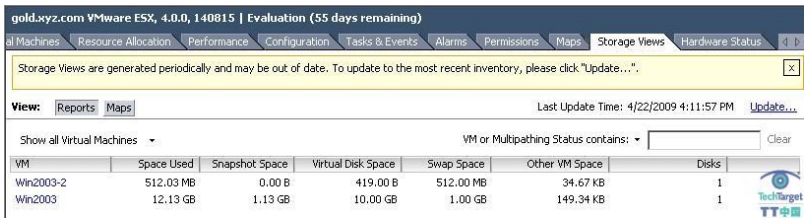
通过管理台、vCenter Server 设置以及数据库保留协议链接可以访问该选项。你可以定义任务和事件数据的保留期限，超过时间的旧数据将自动从数据库删除。



下一个功能体现在快照管理。虽然 VMware 没有为快照添加一个集中管理组件，但他们添加了在环境里直接浏览所有快照的方法。在 VI3 中，查看所有运行着的快照的方法是使用第三方脚本和工具。现在在 vSphere 里，有个新的 Storage 视图，它可以显示快照和其他虚拟机文件信息。

这个新的视图可以在任何对象（例如虚拟机、主机、集群）上使用，并且能显示数据存储、虚拟机文件、SCSI 路径、NAS 加载等各种信息。当选择虚拟机文件选项时，你能自定义设置以显示各种信息，包括所有文件占用的总体空间、快照使用空间、虚拟磁盘空间

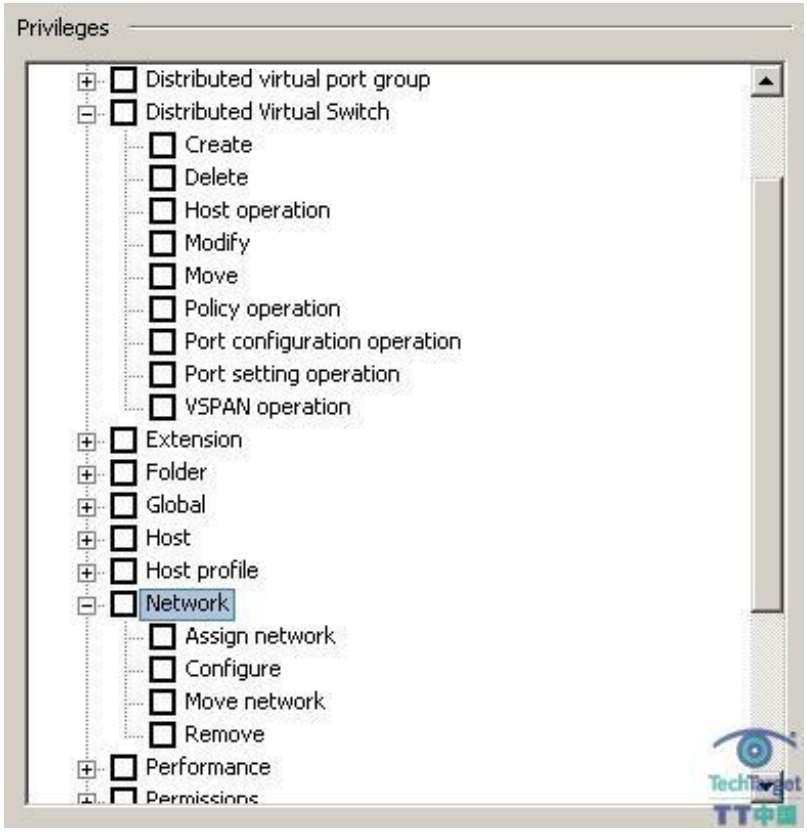
（显示真实的瘦磁盘大小），哪个包含日志文件。通过适当地分类这些栏，你能很容易查看哪台虚拟机在运行快照，因为没有运行的话，那么快照显示将是 0 字节。这种方法很轻易就能找到运行在环境中的快照，所以你能注意到并能删除。



最后一个功能是 vSwitch（虚拟交换机）。在 VI3 中没有可用的许可能阻止某些人将虚拟机从一个 vSwitch 移动到另一个。有间接许可可以阻止这种行为，但使用这个也意味着限制其他的活动。

阻止某些人将虚拟机从一个 vSwitch 移动到另一个的能力对于连接到内部和外部 DMZ 区域的主机来说非常重要。让一台虚拟机桥接内部和外部网络，或者有一台可以移动到 DMA 的安全的虚拟机是存在风险的。

在 vSphere 里，对于网络控制现有有更多的颗粒许可，包括分配网络、配置与移动网络。以前，删除功能在网络下仅有的可用许可。此外，在分布式虚拟端口组和分布式交换机下有许多新许可。这些新许可将极大地增强网络安全，并且能更好的控制虚拟环境中的网络组件。



虽然 vSphere 里有更多的新功能，但作为一名管理员，我就对以上的三个小功能更感兴趣。

（作者：Eric Siebert 译者：唐琼瑶 来源：TechTarget 中国）

VMware vSphere 的许可分析

在 4 月 22 日，VMware 发布了 vSphere。不过许多人很失望，因为他们发现 vSphere 离真正意义上的发布还很远。现在 vSphere 处于 GA 阶段，不久用户就可以使用了。

下面我们概述下许可的更改：

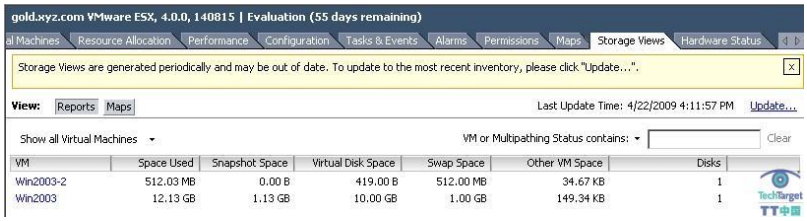
VMware vSphere 提供七个版本：ESXi 单个服务器、基础版、基础增强版、标准版、高级版、企业版和企业增强版，从下图中可以看出，每个版本都有不同的功能。新的基础版适合小型环境，并且包括 ESX Server 和 vCenter Server 包。ESXi 单个服务器版本仍然是免费的，并且包括对精简磁盘的支持。企业版上新的一层叫做企业增强版，它包括对主机文档（Host Profiles）和分布式 vSwitch（Distributed vSwitches）的支持。

	ESXi Single Server	Essentials	Essential Plus	Standard	Advanced	Enterprise	Enterprise Plus
ESX/ESXi	ESXi Only	✓	✓	✓	✓	✓	✓
vCenter Server Compatibility	None	vCenter Server for Essentials	vCenter Server for Essentials	vCenter Server Foundation & Standard	vCenter Server Foundation & Standard	vCenter Server Foundation & Standard	vCenter Server Foundation & Standard
Processor Cores	6	6	6	6	12	6	12
vSMP Support	4-way	4-way	4-way	4-way	4-way	4-way	8-way
Memory/Physical Server	256GB	256GB	256GB	256GB	256GB	256GB	No license limit
Thin Provisioning	✓	✓	✓	✓	✓	✓	✓
VC Agent		✓	✓	✓	✓	✓	✓
Update Manager		✓	✓	✓	✓	✓	✓
VMSafe		✓	✓	✓	✓	✓	✓
vStorage APIs		✓	✓	✓	✓	✓	✓
High Availability (HA)			✓	✓	✓	✓	✓
Data Recovery			✓		✓	✓	✓
Hot Add					✓	✓	✓
Fault Tolerance					✓	✓	✓
vShield Zones					✓	✓	✓
VMotion					✓	✓	✓
Storage VMotion						✓	✓
DRS						✓	✓
vNetwork Distributed Switch							✓
Host Profiles							✓
Third Party Multipathing							✓

点击图片就能放大

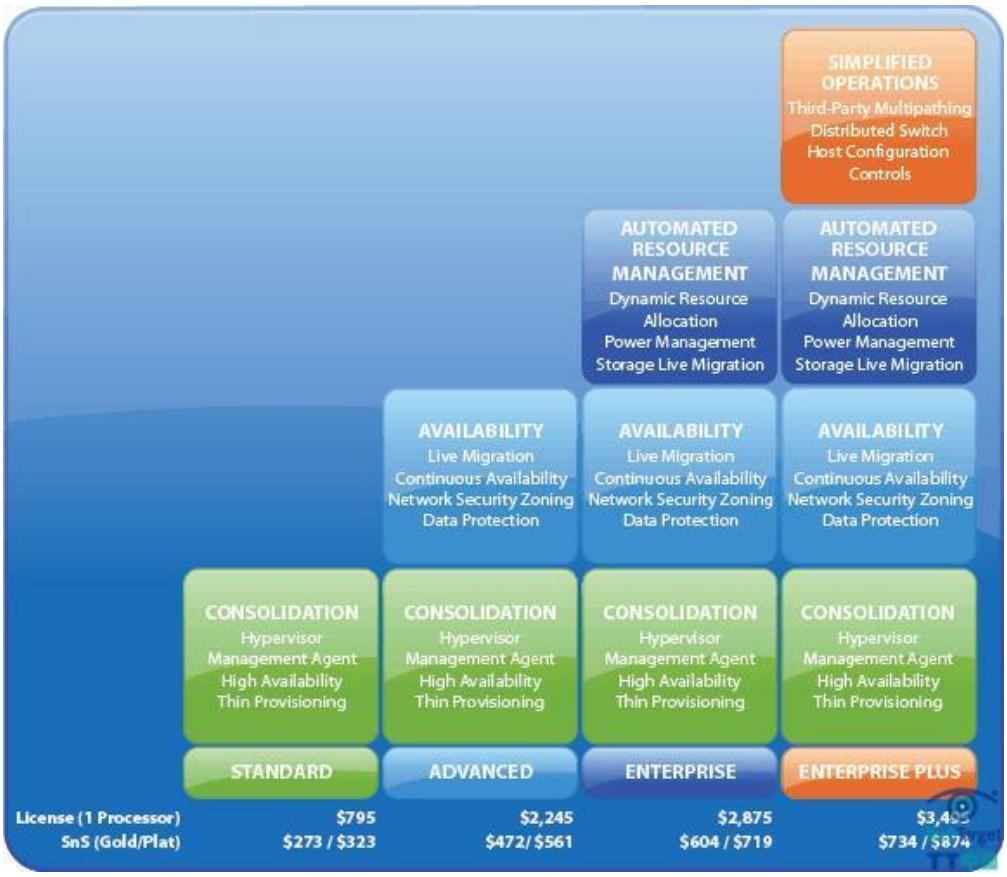
所有的版本（除了高级版和企业增强版支持每个物理处理器高达 12 个 CPU 核心）都能支持每个物理处理器六个 CPU 核心。你现有的 VI3 Foundation 和 Standard 许可将变成 vSphere Standard 许可，你现有的 VI3 Enterprise 许可变成 vSphere Enterprise 许可。

不过你必须有一个激活的 Support and Subscription（SnS，即支持和订阅合同）以便获取新许可。



如果你想获取更多的功能，可以从一个版本升级到另一个，所需要的费用如下图所示：

到今年年底有一个特别促销活动，允许现在拥有激活 SnS 的用户升级到功能更多的版本，花费不到标准升级价格的一半。从标准版本升级到高级版本，每个处理器降到 745 美元，从企业版本升级到企业增强版，每个处理器降到 295 美元。更多促销信息可以参看升级页面底部。



基本版和基本增强版包括三个物理服务器的许可（达到两个六核处理器）和一个 vCenter Server。这两个版本本身都包括解决方案，可能不能拆分开或结合其他版本使用。vSphere 基础版的价格是 995 美元，包括一年订阅服务；不过这种服务在预约的情况下是可选的。基础增强版的价格是 2995 美元，不过 SnS 可以单独出售，至少要购买一年的 SnS。VMware 的许可很复杂，许多用户可能很难计算清楚。幸好 VMware 在其网站上提供了大量帮助文档。点击下面的链接帮助你更好地理解这些新更改。

vSphere 4 定价、包装和许可概况
vSphere 版本比较
vSphere 主要特点和功能介绍
vSphere 4 基本版本
vSphere：许可方面的改动
vSphere 升级说明
vSphere 升级中心——许可

现在的许多企业版用户很失望，因为他们发现如果不付费（每个处理器 295 美元）升级到企业增强版，他们就没有权利享有新主机文档和分布式 vSwitch 功能。以前的企业版是最高级的版本，包括所有功能，但是 VMware 选择添加更高的版本替换了两个旧功能，

两个新的功能对于管理大型环境来说非常有用。VMware 试图在新版本中获取更好的投资成本是容易理解的，通过给现有企业用户提供这些新功能。从五月 21 日开始就能开始升级和购买这些新的 vSphere 许可。现有的用户将注意到他们能登录新的许可入口，并下载新的他们能用的许可。

(作者：Eric Siebert 译者：唐琼瑶 来源：TechTarget 中国)

对 VSphere iSCSi 启动程序验证进行修改以增强系统安全

如果有机会能够在不限制系统功能或者控制灵活性的情况下增强安全性，就再好不过了。使用 VMware 的 VSpere 4.0 中特定 iSCSI 启动程序验证改动可以实现该条件。

第一个主要修改是 VMware ESX 或者 ESXi 主机当前可以同时使用不同 iSCSI 主机，即使这些 iSCSI 主机属于不同的管理组或者是拥有不同的验证能力。这二个主要修改是 VMware ESX 4.0 增强了 VI 3 中的 iSCSI 验证程序，主要是通过另外的四个不同安全级别、手动挑战-握手验证协议（CHAP：Challenge-Handshake Authentication Protocol）安全以及为多目标独立配置验证的能力实现。

匿名和验证访问

在验证级别， ESX 3.5 对 iSCSI 目标支持两种不同类型的访问方式：匿名访问和验证访问。ESX 3.5 验证访问使用挑战-握手协议。访问的实施有时候会受到限制，因为仅仅使用一个本地名字和证书密钥集合。在有多个潜在 iSCSI 目标的工作环境中，这种情况有可能会有问题。在这些多目标有不同验证程序的工作环境中，只有那些具有相同值的目标才可以使用。这也就是说，实际上 ESX 3.5 中的 CHAP 验证要么是对全部对象适用，要么是不起作用。

然而随着 ESX 4.0 的问世，VMware 对 iSCSI 验证模式提供了进一步的灵活性。可以在 iSCSI 启动程序的根用户级别或者目标级别配置 CHAP 验证程序。在根用户级别配置证书，当然如果需要的话，也可以从目标级别继承。ESX 4.0 也新增了手动 CHAP 验证，这在主机和 iSCSI 存储系统之间增加一个新安全级别。

例如，假设一个公司在企业内部使用很多不同的存储技术：这个项目用这一项技术，另外一个项目用那一项技术等；另外也假设 VMware 项目用到其中一项技术，但是 iSCSI 目标的配置却各不相同。为使用 VMware 以及这两种解决方案，必须对 ESX 3.5 的存储技术做出修改才可以使用这两项技术。

在 ESX 4.0 中配置手动 CHAP

为研究如何在 ESX 4.0 中配置手动 CHAP，我使用 StarWind 软件公司的 iSCSI 存储区域网络（SAN：Storage Area Network）作为 iSCSI 存储系统。StarWind 的 iSCSI SAN 解决方案是运行在 Windows 操作系统之上的应用程序，配置起来非常简单。我根据主要工作用途选择企业版的解决方案，因为其可以轻量级供给存储。

首先下载 StarWind iSCSI SAN 并安装在 Windows 系统上。我选择完全安装，在安全结束后启动管理界面开始进行存储系统配置。登录 iSCSI 连接之后，通过给连接增加一个设备来增加一个存储系统。由于我的测试环境没有足够的空间并且我希望使用轻量级供给

iSCSI 目标，所以我选择的是“快照和 CSP 设备（Snapshot and CDP device）”。同时我还确保允许多 iSCSI 连接，因为我在其它测试 ESX 主机中也要用到该设备。

激活手动 CHAP 验证

修改连接许可权限，把对 StarWind iSCSI SAN 的 CHAP 验证程序添加进来，另外对 ESX 主机新增 CHAP 验证程序。因为多 ESX 主机将会使用这个验证程序，我也为其它主机增加 CHAP 验证程序。

为访问主机级别已有的 iSCSI 目标，可以修改 ESX 4.0 主机上的 iSCSI 软件启动程序，在 ESX 4.0 上配置表项中的存储系统适配器控制面板中可以进行修改。在 ESX 3.5 中有一个配置表项，该表能够只接受 iSCSI 目标的 CHAP 验证证书。ESX 4.0 把 CHAP 配置工作移到一个按钮上，它不仅新增手动 CHAP 验证，并且增添和 CHAP 可以使用的安全级别相关的规则。CHAP 安全设置如下表所示：

CHAP 安全级别	内容	支持的启动程序
不使用 CHAP	没有使用 CHAP 验证，验证程序不可用。	软件 硬件
目标要求的情况下使用 CHAP	主机选择不使用 CHAP，但 CHAP 可以作为一个可选项。	软件
目标阻止的情况下不使用 CHAP	主机选择使用 CHAP 验证，但也可以使用 CHAP 不可用的连接。	软件 硬件
使用 CHAP	要求使用 CHAP 验证程序，如果没有 CHAP 验证将无法成功建立连接。	软件

需要切记的是硬件 iSCSI 启动程序不支持手动 CHAP。

为了在主机和 StarWind iSCSI SAN 之间配置验证程序，我首先进入 CHAP 域中 iSCSI 目标的本地用户名和密钥进行配置，然后进入手动 CHAP 域中主机的本地用户名和密钥进行配置。在点击“OK”之后，系统提示是否重新扫描软件 iSCSI 启动程序。这样在 ESX 4.0 和 iSCSI 目标之间就成功创建了双向连接。

除了支持手动 CHAP，ESX 4.0 允许不同目标支持多种 CHAP 验证级别和不同的 CHAP 证书。在不太复杂的工作环境中，可以在启动程序级别配置这些设置，并且每一个目标都可以继承这些设置。正如当今的经济领域一样，当需要把简单问题逐渐复杂化时，从目前已

有的系统上入手开始工作。如果能够不中断这些资源正在提供的服务而配置系统的话，最终将会更加灵活，同时也可以节省成本，这正是我在本文中提到的对 Spere 4 做出修改后所能提供的优点。

（作者：Jase McCarty 译者：王越 来源：TechTarget 中国）

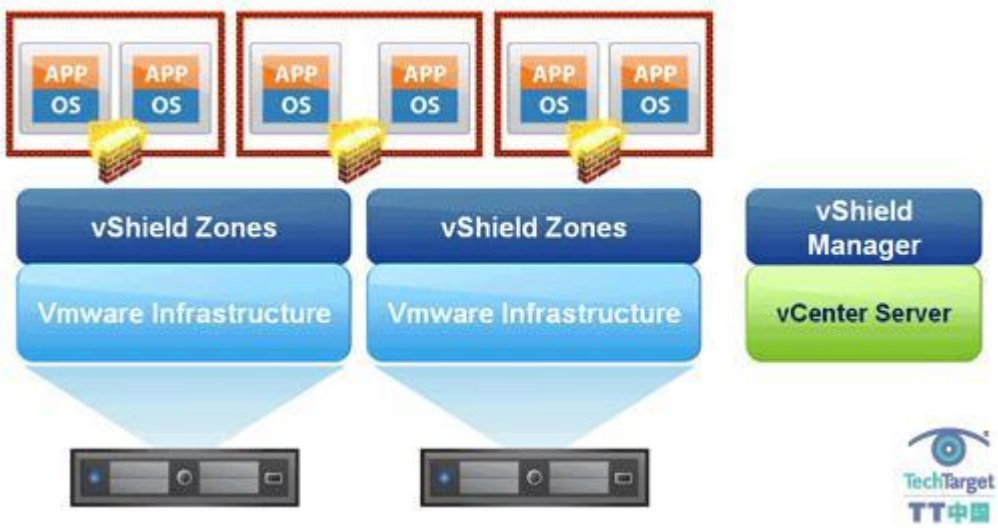
VMware vShield Zones 组件及其工作原理介绍

VMware 把对虚拟机安全问题的研究方向集中在两个主要的 vSphere 组件上：Vmsafe 和 vShield Zones。其中 VMsafe 是一个应用程序通用接口组件，用于帮助第三方厂商创建虚拟化安全产品以更好地保护 VMware ESX，而 vShield Zones 是一个面向 VMware 管理员的安全工具。

vShield Zones 本质上是一个设计来保护虚拟机和分析虚拟网络流量的虚拟防火墙。接下来我会用连续的三章，来解释如何安装和有效管理 vShield Zone。现在，让我们从最基本的介绍开始：什么是 vShield Zones 以及它是如何工作的。

vShield Zones 概述

vShield Zones 本质上是一个基于 2008 年发布的 Blue Lane 技术实现的虚拟防火墙，被设计用来保护虚拟机和分析网络流量。现在的 vShield Zones 1.0 版本还无法跟 Vmware 最新的 Vmsafe 技术集成。根据 Vmware 的计划，在即将发布的新版 vShield Zones 中会使用 VMsafe API。在 Advanced、Enterprise 和 Enterprise Plu 版本的 ESX 和 ESXi 已经提供 vShield Zones 组件的免费下载功能。



Vmware 通过部署 vShield Zones 使用核心产品 实现对虚拟网络的基本保护功能。vShield Zones 提供的网络防护和分析功能与很多第三方的程序类似。如：Reflex Systems Virtualization Management Center、Altor Networks Virtual Firewall 和 Catbird 的 V-Security。但是相比而言 vShield Zones 没有那么复杂，是一个简化版的产品。简化的好处就是 VMware 的管理员会发现 vShield Zones 使用起来非常方便。用户无

需成为安全方面的专家就可以熟练部署虚拟机环境中的安全策略。下面列举了 vShield Zones 为您的虚拟网络带来的新功能：

- **防火墙防护**——vShield Zones 提供跨 vSwitch 的防火墙防护技术，通过添加规则来允许或阻止特殊的端口访问、协议和流向。防火墙功能被称为“WM Wall”，在数据中心和集群基本中提供一个集中的分级的访问控制列表。其中 Layer 4 和 Layerv2/3 的访问规则是可用户自定义的；对应于 OSI 网络协议模型的数据链路层、网络层和传输层。
- **流量分析**——所有通过 vShield 设备的数据都获得监控，收集和汇总关于源、目标地、流向和服务相关的信息到 vShield Manager。流量分析功能被称为“VM Flow”，可以在做网络故障诊断、可疑流量分析、创建访问规则时作为参考。
- **虚拟机扫描**——vShield agents 终端是一个扫描进程，用来查找被使用的操作系统、应用和端口及流量分析。一旦这类信息被收集和分析，可以用来在制定防火墙访问规则时做参考。

VShield Manager 和 vShield 代理

vShield Zones 由两个部分组成：VShield Manager 和 vShield agents，这两部分都被作为虚拟设备组件封装在 OVF（Open Virtualization Format）文件中。VShield Manager 是用来管理所有 vShield 代理的中央管理程序，它定义访问规则和监控网络流量。通过 Web 界面登陆的一个 VShield Manager 可以管理来自多个 ESX 或 ESXi 主机的 vShield 代理。一旦用户设置了通过 vShield Zones 保护 vSwitch，VShield Manager 将在 vSwitch 所在的虚拟主机中安装 vShield 代理。通过 vShield 代理提供防火墙保护、网络流量分析和安全区域设置的功能。vShield 代理把所有流量分隔为被保护域和未被保护域，所有来自未被保护域的网络流量穿过 vShield 代理到达虚拟机所在的被保护域。

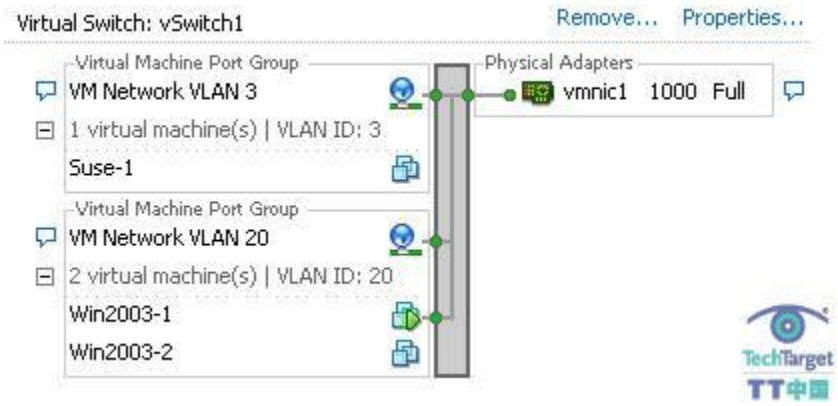
试想原来有一组可以通过公路到达的房子。为了保护这些房子，使得只有被允许的访客可以进入，我们首先把这些房子搬迁到一个独立的小岛上。所有试图进入小岛的客人，都必须跨越一座唯一的小桥。在小桥的入口处放置一个守卫（vShield 客户端 ），他只允许出现在访客列表上（防火墙规则）的客人通行。同时，警卫会监控和管理所有通过小桥的人流来排查任何可疑的情况（流量分析）。

接下来用技术术语说明部署 vShield 代理的步骤：

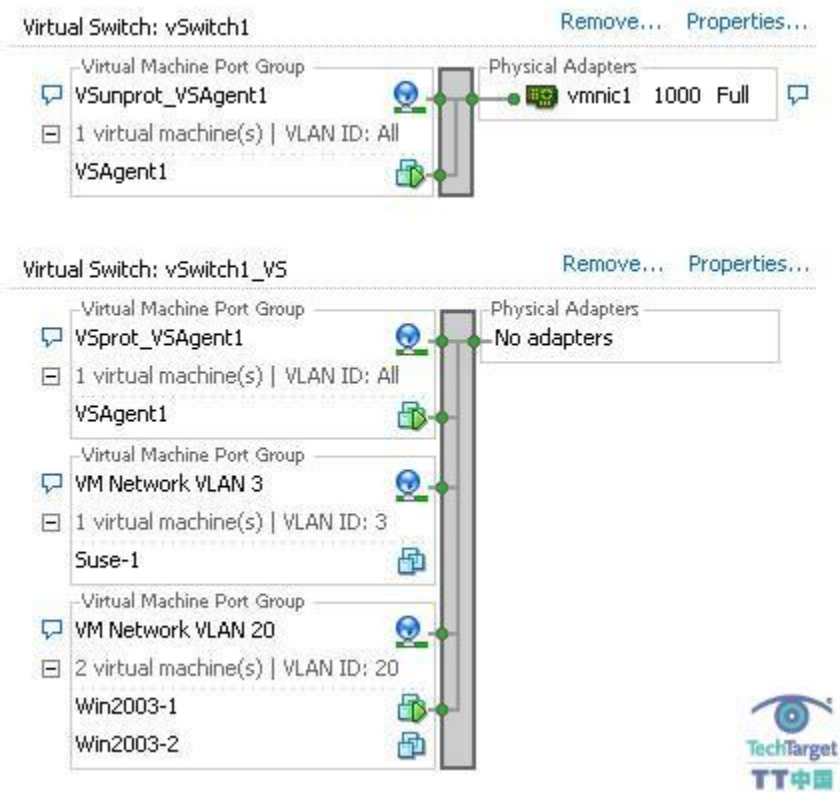
1. 根据样本为 vShield 客户端程序创建一个新的虚拟机。然后为虚拟机分配三块虚拟网卡（vNIC），一个用于跟 VShield Manager 之间的对话；一个连接到原有的 vSwitch（vSwitch1）接管未被保护的流量（入口），另一个连接到新创建的 vSwitch（vSwitch2）作为到达虚拟机的被保护流量通道（出口）。
2. 创建新的 vSwitch（vSwitch2）时不分配物理网卡。
3. 在 vSwitch 1 上创建一组新的端口用于未被保护的流量通过，在 vSwitch2 上创建一组新的端口用于被保护的流量通过。vShield agent 的虚拟网卡（vNIC）分别建立跟这两组端口连接。

4. 在 vSwitch2 中创建所有原来位于 vSwitch 1 中的虚拟机端口，修改每个虚拟机的设置，并且把物理网卡转移到 vSwitch2 的新端口组中。
5. 一旦虚拟机被移动到 vSwitch2 中，把原始端口从 vSwitch1 中移除。

这是 vShield Zones 部署前的 vSwitch 显示界面：



这是部署 vShield Zones 之后的显示界面：



从图上可以看到所有的流量必须通过位于 vSwitch1 上的物理网卡，然后穿过 vShield agent 虚拟机，到达新的虚拟机所在的被保护的 vSwitch1_VS vSwitch。

如果需要部署 vShield Zones，首先具备的基本需求是 VMware ESX 或 ESXi 4.0 主机和 vCenter Server 4.0，然后您需要拥有可以增加和启动虚拟机的管理权限，和用于分配给 vShield Manager 和每个 vShield agent 的静态 IP 地址。

另一方面，还有一个重要因素没有提到。就是 vShield Manager 虚拟机创建时需要预先分配并保留 2GB 内存空间，vShield agent 的创建需要预先分配并保留 1GB 内存空间。由于保留内存空间的需求，当 Manager 和代理启动之前，您必须确保主机有足够的可用空闲物理内存空间。虽然可以通过修改虚拟机的设置来配置预留内存的大小，但是我并不建议这么做。这种做法会导致设备的性能受到影响，进而影响到功能的实现。而且也无需增加分配给 vShield Manager 和代理的内存空间，这样也不会改善性能。

当然 vShield 也具备如下列举的这些端口需求：

- Port 11——Secure Shell，或 SSH（Transmission Control Protocol TCP）——用于在 vShield Manager 和代理之间的通讯
- Port 123——Network Time Protocol (User Datagram Protocol, UDP)——用于 vShield Manager 和代理的时间同步
- Port 443——HTTP Secure（TCP）——用于 PC 机通过 web 图形界面登陆和管理 vShield Manager
- Port 1162——Simple Network Management Protocol, SNMP (UDP)——用于从 vShield 代理到 vShield Manager 发送 SNMP 信息，包括内存和 CPU 在内的所有其他静态设备，都使用 Port 22。

vShield Manager 和代理都会占用主机资源，其中内存和硬盘的占用是静态的，CPU 的占用率基本上取决于通过代理的网络流量大小。另外在流量通过代理时会存在一定的网络延迟，这是由于从代理到达虚拟机的时候增加了额外的跳转导致的。从设计原理分析，每个 vShield 客户端最多支持 40，000 个并发的对话（session），这个吞吐量不受它所在主机硬件情况和分配给客户端的资源的限制。vShield Manager 和代理的资源占用情况列举如下：

Restore	vShield Manager	vShield 代理
磁盘空间占用	8 GB	5 GB
内存占用	2 GB （预留）	1 GB （预留）
CPU 占用	3 - 7 %	3-10%
网络延迟	N/A	500 微秒

vShield Manager 可以管理最多 50 个 vShield 代理，一个单独的 vShield Zones 客户端可以保护最多 500 个虚拟机。

在这个系列的下一章节，我们将讨论：如何安装和配置 vShield Zones Manger 和代理组件。

（作者：Eric Siebert 译者：李哲贤 来源：TechTarget 中国）

如何安装和配置 vShield Zones?

在这个系列的第一章，我讲述了“VMware vShield Zones 组件及其工作原理”。接下来我将继续解释如何安装和配置 vShield Manager 及 vShield agents。

在开始安装前，我们应该准备好以下几个文档以便随时查阅：vShield Zones 注意事项、vShield Zones 说明书、快速部署指南和管理员手册。

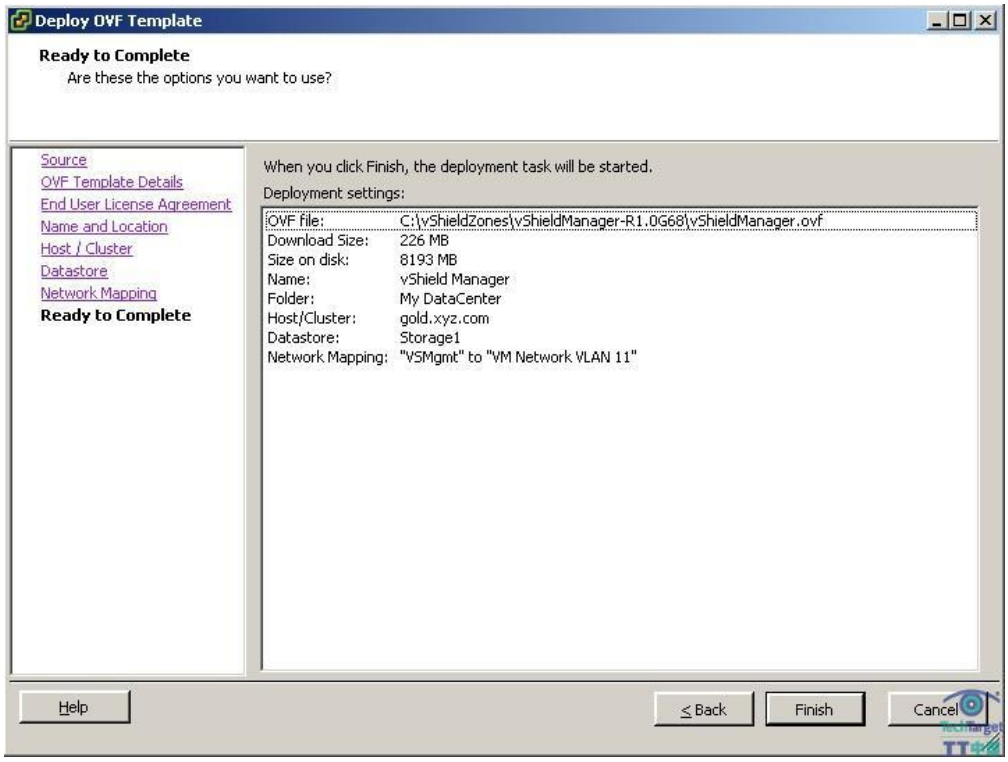
准备工作完成后，请遵循以下步骤开始安装 vShield Zones：

一、从 VMware 官网下载 ISO installation file 文件，大小为 759MB。vShield Zones 和 VMware Date Recovery 打包在同一个 ISO 镜像中。（如果你有 vSphere DVD 介质安装盘，其中包含 vShield Zones，无需下载。）

二、然后选择把下载的镜像文件刻录到 DVD 光盘上或者用虚拟光驱软件加载。安装向导将自动启用，按照向导提示选择 vShield Zones 安装的相关信息。安装程序将从 455MB 大小的 VMware-vShieldZones.exe 文件中解压 Open Virtualization Format（OVF）格式的/VMDK 文件和 PDF 文件到您选定的文件夹中。

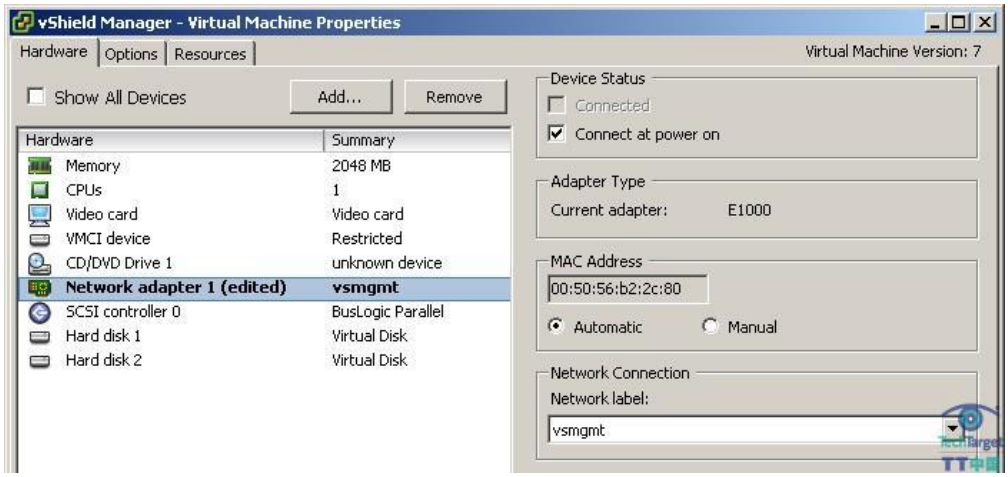
三、解压完成后，可以启用 vSphere 客户端程序在宿主机系统上创建 vShield Manager 虚拟机应用。

- 登陆 vShpere 客户端并且链接到 vCenter Server（不要直接链接到 ESX 或 ESXi 主机）
- 从顶端菜单栏选择 File 菜单，然后选择 Deploy OVF Template 选项
- 选择 Deploy From File 选项，点击 Browse 按钮，选择需要解压的目标文件夹路径。vShield Manager 样本在 vShieldManager-R1.0G68 子文件夹中（vShield-R1.0G68 文件夹中存放的是 vShield agent）
- 选中 vShieldManager.ovf 文件
- 点击 Next 创建一个带有 8GB 虚拟硬盘的虚拟机，此时虚拟机样本的详细信息将显示出来。
- 继续按照提示选择新虚拟机的目标主机、数据存放地点以及目标网络（点击 Destination Networks 后可以配置相应的参数）
- 点击 Finish 完成新的 vShield Manager 虚拟机的创建

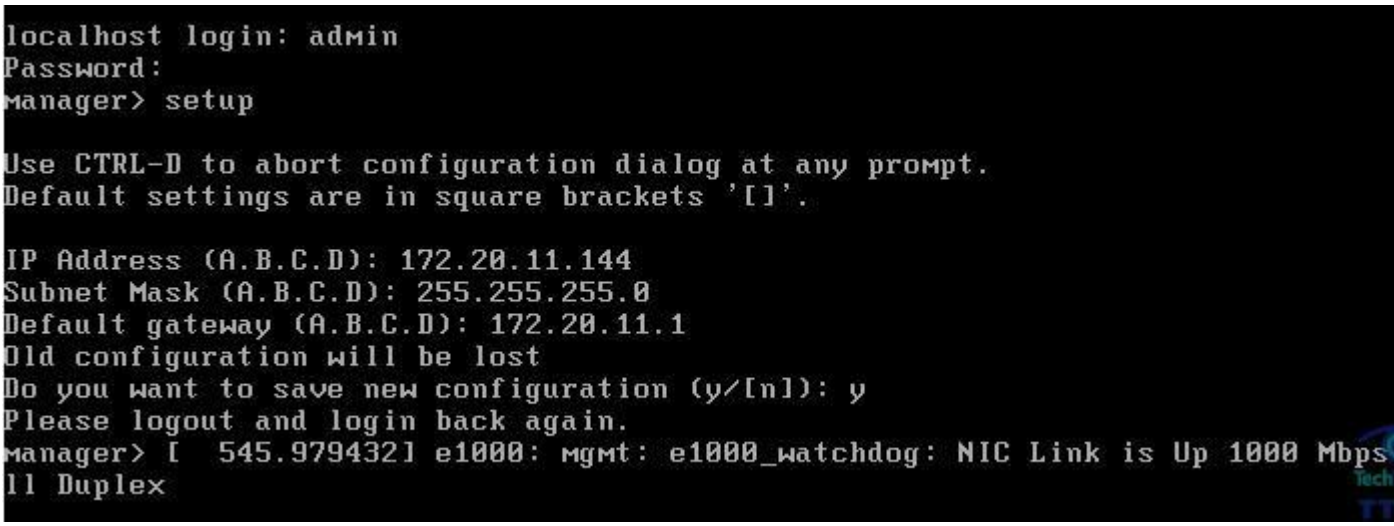


（点击图片就能放大）

四、然后，配置 vShield Manager 虚拟机连接的 vSwitch。增加一个名为 vsmgmt 的新端口，如果需要为它分配 VLAN ID。这是一个用于被 Shield agents 识别的特殊端口组，防止安装的 vShield Manager 虚拟机被移除。完成 vShield Manager 虚拟机的配置之后，选择 network adapter，把 network label 修改为新创建的 vsmgmt。

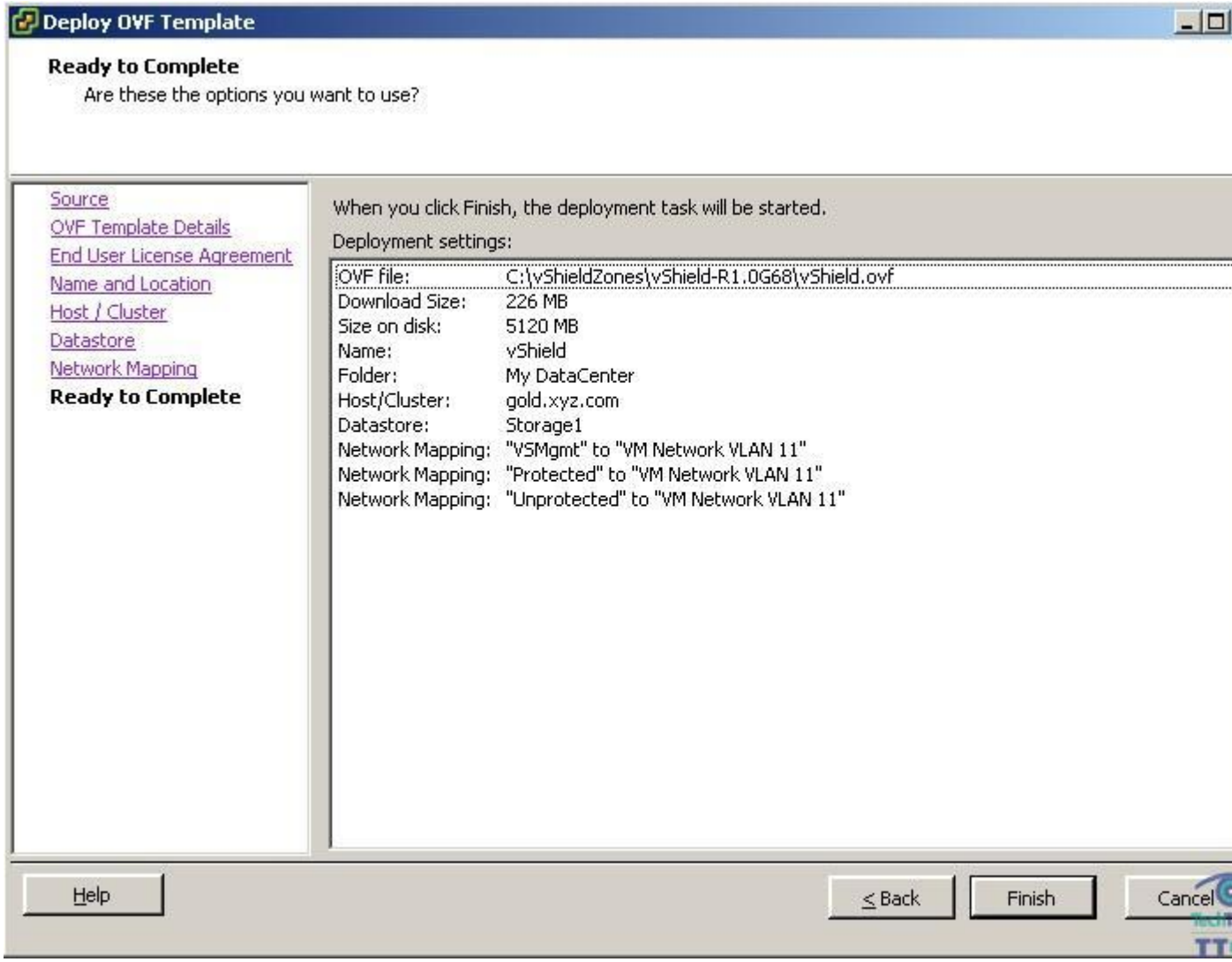


五、启动 vShield Manager 虚拟机。启动完成后，使用默认的用户名“admin”，密码“default”登陆。一旦登陆后，就进入管理向导界面，选择“setup”运行命令行界面的提示向导来配置网络设置。输入 IP 地址信息。完成后，选择“y”保存配置。系统将提示退出并重新登录，这个步骤并不是必须的，这时，你可以运行 ping vShield Manager 来确认网络连接是否正常。完成后选择“quit”退出。



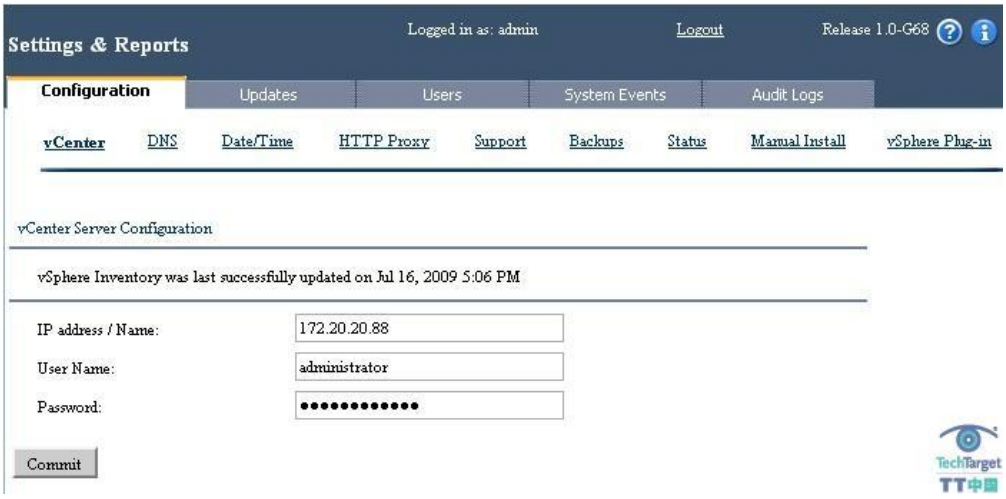
六、接下来需要从 vShield Agents OVF 文件创建一个虚拟机，并且把它保存为一个样本，方便后续 vShield Agents 的创建。为了完成这步操作，仍然需要使用 vSphere Client。

- 选择 File/Deploy OVF Template/Browse，在解压的安装文件中选择 vShield-R1.0G68 子文件夹，选中 vShield.ovf 文件。
- 点击 Next，可以看到样本的详细信息提示。新的虚拟机将分配 5GB 的虚拟盘。
- 按照向导步骤选择目标主机和数据存放地址。在 network mapping 界面，你可以看到多个网络适配器（vsmgmt，被保护的和未被保护的）。
- 无需担心目标网络地址已经改变，选择接受默认配置。
- 完成安装向导后，选择 Finish 创建 vShield Agents 虚拟机，虚拟机创建完毕后，暂时不要启动。
- 右键单击虚拟机，选择 Template，然后选择 Convert to Template。



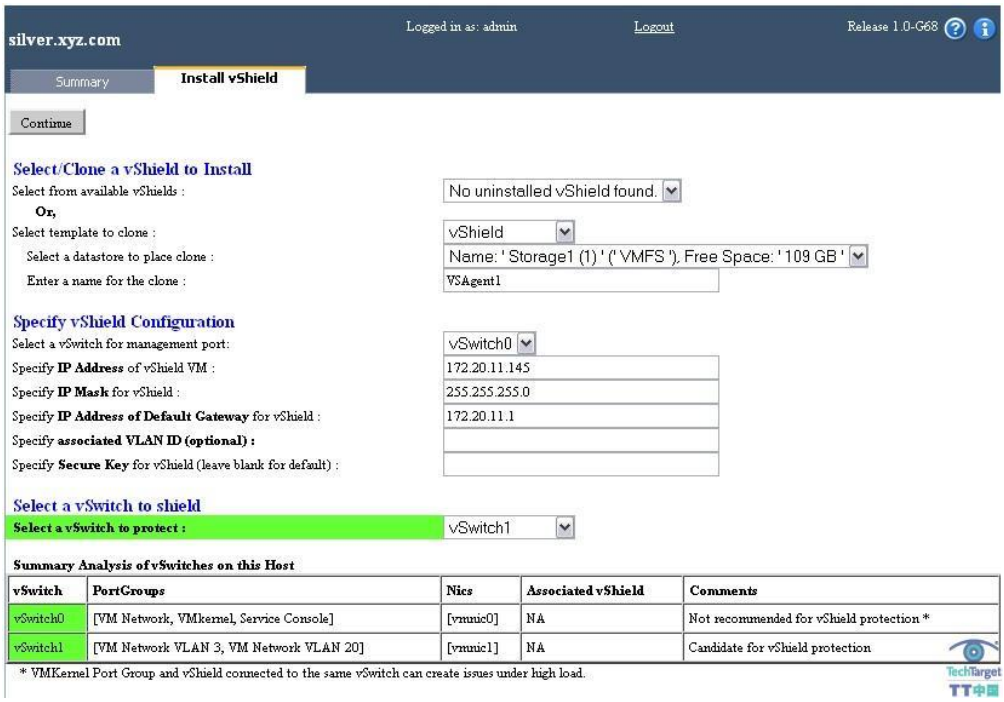
七、现在需要登录 vShield Manager 完成配置。

- 打开 Web 浏览器，输入地址 https://<vShield Manager IP Address>。将弹出登陆界面
- 用默认用户名“admin”和密码“default”登陆
- 登陆后，在面板右侧 Configuration 选项下，选择 vCenter，输入 IP 地址和 vCenter Server 的登录信息，点击 Commit 按钮登陆以后，面板左侧的目录和你的 vCenter Server 是一致的，你还可以通过 Configuration 选项下的链接查看和配置 DNS 和 Date/Time

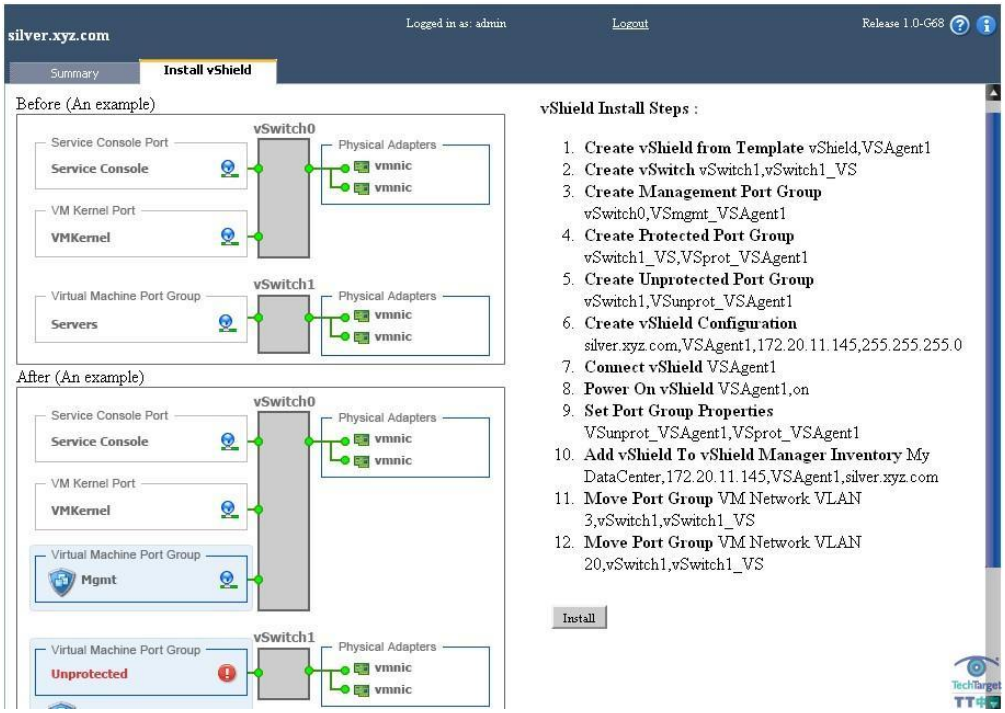


八、现在 vShield Manager 已经安装和配置完成，接下来需要部署 vShield Agents。

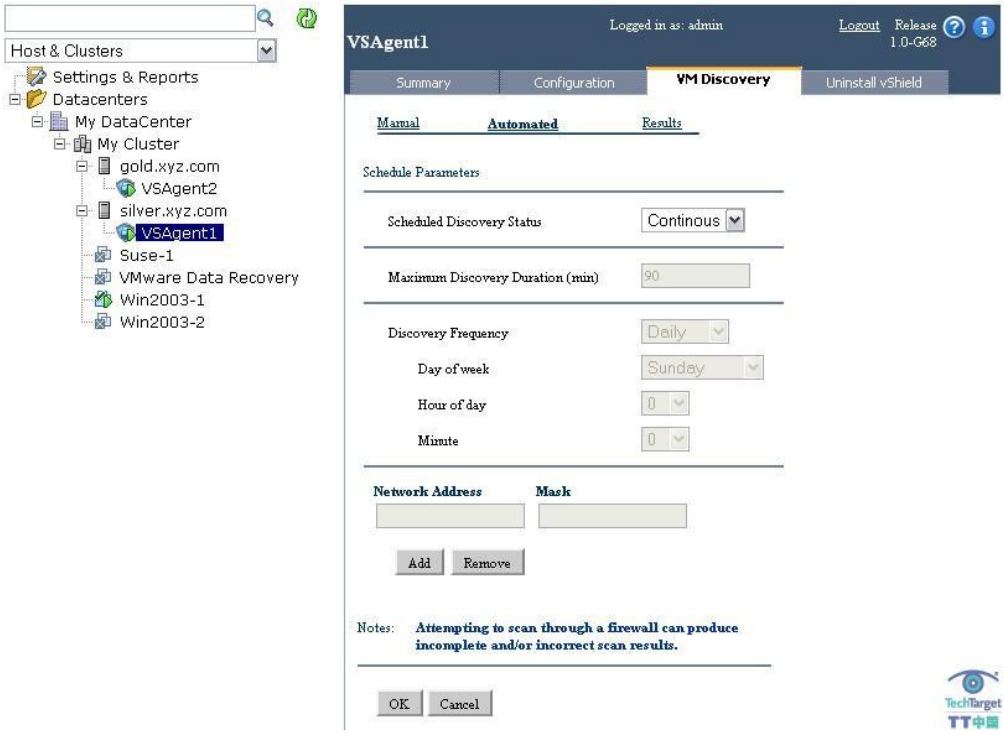
- 在左侧面板中选中你要添加保护的 ESX 主机
- 在面板右侧，选择 Install vShield 选项
- 选择 Configure Install Parameters 链接，显示页面中列举了新克隆的 vShield Agents 虚拟机，IP 地址和保护的 vSwitch 等相关信息。这里可以选择克隆已经存在的 vShield Agents 或者从之前保存的模板来创建
- 选择新 agent 虚拟机的数据存放地址，并为它指定唯一的名称
- 选择一个 vSwitch 作为 vShield 管理程序接口（vsmgmt），并且输入它的 IP 地址。在底部从下拉菜单中选择要添加保护的 vSwitch。分析结果将显示所有存在的 vSwitch 并且提供是否可以添加 vShiled 保护等相关信息。
- 所有信息输入完成后，点击 Continue 开始安装过程



九、下一个页面将显示在安装 vSwitch 前后变化的示例情况以及安装步骤。点击底部的 Install 按钮，开始安装，我们可以在 Web 浏览器中或者通过登录 vSphere Client，从创建的任务中跟踪整个安装进程。



十、安装完成后，右侧的界面中列举了主机中所有部署了 agent 的虚拟机名称。如果选中 agent 并点击 VM Discovery 选项，可以对虚拟机的扫描进程做配置。扫描进程分析虚拟机的流量并启动端口扫描来识别开放的端口。我们可以选择手工指定 IP 地址的一次性扫描或者建立周期性（或连续的）扫描计划。



访问 VM Wall 和 VM Flow 选项

所有的安装和配置完成后，我们可以打开 VM Flow 和 VM Wall 选项来进行流量分析和防火墙规则设置。当你在左侧选择 data center, cluster, resource pool 或 virtual machine 这些选项时，这些选项会显示在面板右侧。

如果点击 VM Wall 选项，可以看到默认的防火墙规则下，对于任意的源和目标 IP 地址或源和目标端口都设置为“any”。这时允许所有的访问通过 vShield Agents。在你添加了防火墙规则之后，可以发现源和目标的选择并不仅仅针对 IP 地址设置，同样可以是 vCenter Server 中的组件，如 data center 和 cluster。你可以通过点击页面顶部的按钮或者直接在前面的 VM Flow 分析界面中，创建附加的 VM Wall 规则。

Application	Sessions	Packets	Bytes	VMWall
ALLOWED	1320	12,755	1,770,070	
TCP	359	10,961	1,645,012	
UDP	961	970	118,638	
INCOMING	348	348	31,320	
CATEGORIZED	348	348	31,320	
NBNS-Broadcast	348	348	31,320	
Win2003-1(172.20.20.115)	348	348	31,320	
172.20.20.88	95	95	8,550	
172.20.20.90	253	253	22,770	
UNCATEGORIZED	0	0	0	
OUTGOING	9	18	2,003	
CATEGORIZED	9	18	2,003	
DNS	9	18	2,003	
172.20.3.50	9	18	2,003	
Win2003-1(172.20.20.115)	9	18	2,003	
UNCATEGORIZED	0	0	0	
INTRA	0	0	0	
INTRA_HOST	0	0	0	
ICMP	0	107	6,420	
ARP	0	717	0	

流量监视程序（VM Flow）可以在基于 data center, cluster, port group, VLAN, 或 virtual machine 层面来使用，防护程序（VM Wall）被限制在 data center，cluster 和 VLAN 层面。在面板左侧，可以对不同的层面设置不同的访问规则，同时可以监控该层的流量分析结果。VM Wall 的规制是分级的，data center 上设置的规则相比下面的 cluster 层的规则拥有更高的优先级。

如果想达到熟练和正确的配置使用 vShield Zones，需要一些时间来逐渐适应。vShield Zones 管理员指南提供了一些关于设置和使用 VM Wall 和 VM Flow 组件的细节建议。稍后，在这个系列的最后一章中，我将提供一些实用的技巧。

（作者：Eric Siebert 译者：李哲贤 来源：TechTarget 中国）

管理 vShield Zones 的最佳技巧（上）

如果你选择使用 vShield Zones，那么你应该注意到了它的使用局限；例如，它没有产品 VMware Data Recovery 那样好，新接触 vSphere 的管理员将需要具备许多领域的技巧。在本文中，TechTarget 中国的特约虚拟化专家 Eric Siebert 将列出目前为止所发现的技巧，以便你轻松使用目前版本的 vSphere。

这是 vShield Zones 系列文章的最后一部分。如果你一路追随，应该知道我们第一部分概述了 vShield Zones，第二部分讲安装和配置 vShield Zones。

VMware Tools

vSphere Client 将报告 VMware Tools 没有安装在 vShield Manager 和代理虚拟机上。不要尝试在这些虚拟机上安装 VMware Tools，因为没有必要，并且 VMware Tools 提供的性能优化已经内置在 vShield Zones 虚拟机里。

内存与 CPU 预留

代理不是真正的有特权的虚拟机，但是应该看成是。虽然默认下它们有内存预留，但不是用于 CPU。考虑使用共享或预留保证代理的 CPU 资源。

VMkernel 与服务控制台

VShield Zones 的建立用于保护虚拟机，不是 VMkernel 与服务控制台。不要在服务控制台或 VMkernel vSwitch 上安装代理。

预安装的网络接口卡

不要从 vShield Manager 或者代理虚拟机移除预安装的网络接口卡（NIC）。如果你要在 vShield 代理上移除并添加 NIC，必须卸载 vShield Zones 代理并重新安装。如果你从 vShield Manager 移除 NIC，可能必须重新安装整个 vShield Zones 以确保 vShield 代理和 vShield Manager 之间的通信。不要重新配置硬件或减少分配给 vShield Zones Manager 或代理虚拟机的资源，因为它们已经被 vCenter Server 优化。

VMotion

由 vShield 保护的虚拟机受 VMotion 的支持，不过你首先必须确保在主机上拥有代理移动虚拟机，并且你的端口组有相应的配置。默认下你不能 VMotion 一台连接到内部（不是 NIC）vSwitch 的虚拟机，因此你必须通过编辑 vpxd.cfg 文件并添加

VMOnVirtualIntranet 参数配置 vCenter Server 允许这样做（更多细节参见 vShield Zones 管理员指导附录）。

VMotion 不支持 vShield 代理，但是支持 vShield Manager。你不想 vShield 代理移到其他主机，因此确保禁用单个 vShield 代理虚拟机上的 Distributed Resource Scheduler 和 High Availability (HA)功能。你不能在主机上使用运行 vShield 代理的 Data Protection Manager（更多细节参见 vShield 使用注意事项）。

本地与共享磁盘

vShield Manager 和代理虚拟机能安装到本地磁盘或者共享磁盘。尽可能安装在共享磁盘，这样能平衡 VMotion 和 HA。由于代理不能从主机移动，最好安装到本地磁盘。

VSwitch

当部署 vShield 代理时，你的虚拟机不会崩溃，因为它们从一个 vSwitch 移动到了另一个。在我的测试环境中，当在代理部署操作期间持续在虚拟机上 ping 时，只看见一个没有响应。

DMZ

当在主机上设计 DMZ 环境时，VShield Zones 提供了更多选项和保护。即将发布的 VMware 白皮书将包含架构选项，你可以在进行 DMZ 配置使用 vShield Zones 的时候用到。

更多技巧请点击下半部分。

（作者：Eric Siebert 译者：唐琼瑶 来源：TechTarget 中国）

管理 vShield Zones 的最佳技巧（下）

（点击回顾上半部分）

如果 vSheild 管理或代理被关掉……

如果 vShield Manager 断电，它不会影响 vShield 代理运营或受保护的虚拟机。如果 vShield Manager 某些时候不可用，每个 vShield 能排列数据并在 vShield Manager 能用的时候发送到 vShield Manager。不过如果 vShield 代理断电，在安全区域的所有虚拟机将丢失网络连接。最好限制在 vCenter Server 里谁能访问和控制代理虚拟机，并且设置当主机重启或启动时虚拟机自动启动。

VSphere Client 插件

有个用于 vShield Zones 的 VSphere Client 插件，不过它的功用就只是启动 Web 界面。

虚拟交换机与分布式虚拟交换机

VShield Zones 支持标准的虚拟交换机（也叫做 vSwitches）和分布式 vSwitches。代理安装将自动配置标准的 vSwitches，不过你必须手动配置 Distributed vSwitches。

更改默认密码

你应该尽快更改 manager 和代理的默认密码，这不会影响 manager 与 vCenter 或 manager 与代理之间的通信。注意，在 Web 用户界面的管理用户账户与命令行用户界面的用户账户是不同的。即使它们使用默认下的管理员用户名和密码，它们是独立的账户，以不同方式管理。

你能使用 Web 用户界面更改管理密码。详细信息参见“保护 vShield Zones CLI 用户账户和特权模式”手册。你也能使用 Web 用户界面添加用户到 manager。

备份

你能备份和恢复 vShield Manager 数据，这包括系统配置、时间和审计日志表。备份保存到 vShield Manager 能访问的远程地点。能在 vShield Manager UI 的 Configuration 表上配置备份。

时间集成

安装并初始化 vShield Manager 后，能配置成指向内部网络时间协议（NTP）服务器用于时间集成服务。默认下，vShield Manager 配置每个安装的 vShield 代理使用 vShield Manager 的 IP 地址实现 NTP 服务。你不能更改 vShield 代理的 NTP 服务器分配。

日志文件

为了检修问题，如果你需要访问日志文件，vShield Manager 和代理的日志文件可以使用 vShield Manager 用户界面下载，只需要选择 Configuration 表然后点击 Support 选项。当你点击启动按钮下载日志文件，这个日志是打包好的并下载在你的工作站。日志是压缩的，有专门的文件扩展.blsl（Blue Lane Support Log），能使用像 WinZip 这样的解压工具打开。

VShield Zones 版本更新

VShield Zones 版本更新是周期分布的。可以在 Update 表上使用 vShield Manager 用户界面使用。有了更新就可以下载到 PC，然后使用 vShield Manager 用户界面上传。首先应该更新 vShield Manager，然后是 vShield 代理。你将看见更新状态界面在安装更新后是否是 manager 还是 代理的重启。在重启任何代理之前确保首先重启 vShield Manager。

总结

vShield Zones 未来的版本将提供更好的集成和可用性，增加的功能能更好保护你的虚拟环境。将来的一些功能包括为 vShield 代理启用高可用性（HA）的能力，因此，如果代理崩溃，可以在相同主机上自动重启。此外，VMsafe 集成在 vSphere 里，你不再需要在 vSwitch 层使用在线代理，因此代理集成在每台虚拟机的虚拟 NIC 里。

（作者：Eric Siebert 译者：唐琼瑶 来源：TechTarget 中国）

如何在数据中心中安全部署 VMsafe 虚拟设备？

虽然 VMware vSphere 4 版本已经集成了 VMware VMsafe，但是对于多数人来说，并不熟悉如何正确地部署 VMsafe。VMsafe 是一个应用程序接口，保护运行在虚拟机上的应用。

尽管 VMsafe（如思科的 Nexus 1000V 虚拟交换机）产品并不太多，但是为了能达到最佳的虚拟化安全、效率和性能，在您部署一款产品之前，需要了解清楚如何把这种虚拟机应用保护程序整合到您的数据中心环境中。

本文讨论在数据中心部署 VMware VMsafe 需要考虑的问题：VMsafe-aware 虚拟程序的位置、程序对主机的影响以及交互性问题。

Faster Path 和 Slow Path

VMsafe 应用有两种实现方式：第一种被称为 Faster Path，通过在 VMware vSphere ESX 4 主机系统上安装一个 vmkernel 驱动实现。Fast Path 方式的优点非常多。但它仅仅是一个驱动，此外经常被用来转发必要的信息给虚拟程序；第二种是组合虚拟程序和 vmkernel 驱动的方式，被称为 Slow Path。

因为多数 VMsafe 应用程序会使用虚拟设备，所以把这些程序放置在数据中心的哪里就变得很重要。从安全的角度出发，充分考虑 VMsafe 程序的作用及其对虚拟化数据中心的影响成为关键因素。VMsafe 虚拟程序具备直接访问处于虚拟化管理程序（hypervisor）中数据的能力,包括读写内存、存储和访问网络设备。在一些情况下，VMsafe 虚拟程序甚至可以改变从内存、存储设备或网络读取的数据。

这种访问存在重大的安全隐患。如果虚拟设备处于危险的环境中，如隔离区（DMZ）或可以直接访问 Internet 的环境，那么它就非常容易被攻击。一次成功的侵入将会对您的虚拟化数据中心造成灾难性的破坏。

在使用 VMsafe 虚拟设备前首先要考虑的问题是，VMware vSphere 不会自动保护虚拟设备，而是把这个任务留给用户和供应商，当供应商完善了自身的工作之后，VMsafe 虚拟设备的安全就成为用户的职责。

这里提供一些基本的准则：

- 不要把 VMsafe 设备安装在隔离区（DMZ）
- 不要赋予它们直接访问 Internet 的能力，设置成通过代理服务访问
- 不要安装在虚拟机网络层
- 不要安装在服务管理层和 IP 存储层

- 不要安装在 VMware VMtion 或 Fault Tolerance Logging 网络层

那么，在什么地方安装虚拟设备呢？

- 安装在防火墙保护的安全区域内，安全区可以是虚拟管理网络层的一部分，或者在一个单独安全区域。

伴随着 VMsafe，VMware 在虚拟网络层中强化了另外一种有效的安全区域：相比早期的 VM Infrastructure3（VI3）中的四个，在全功能的 Enterprise 或 Enterprise Plus 版本的 VMware vSphere ESX 主机自带有六个基本的安全区域。这样就增加了更多让人可以放心选择的虚拟网络。

在 VI3 中，通常认为 VMotion 和服务器控制台可以共享同一个 uplink（上行链路），现在我们可以考虑是不是让 VMsafe 也共享这块区域。或者应该把 service Console 跟 VMsafe、VMotion 以及 Fault Tolerance Logging 整合起来。答案是：这些都主要取决于用户的应用环境和性能方面要求。

VMsafe 对虚拟机性能的影响

从功能方面分析，VMsafe 设备能是资源密集型虚拟机。例如，如果你想做全面的深度包检测或内存分析时，VMsafe 应用性能开销是很大的。换句话说，这个进程将影响整个 ESX4 主系统上的所有的虚拟机性能。全面的深度包检测和内存分析对 CPU 的占用率也是很高的。

最后一点需要考虑的是不同厂商 VMsafe Vmkerner 驱动之间的交互问题。如果您计划使用多种 VMsafe 产品，就需要验证和测试各种 vmkernel 驱动间的互操作性问题。VMware 不会对这些交互的过程做测试，虚拟程序的供应商可能也不会做。考虑到这是一种第三方的 vmkernel 驱动，厂商会有一些兼容性方面的考量。

当您开始部署 VMsafe 设备的时候，就需要小心了（Cisco Nexus 1000V 也是 VMsafe 应用）。您需要：考虑在什么位置安装 VMsafe 虚拟程序；考虑虚拟设备可能对您的 ESX4 主机造成的影响；最后，考虑互操作性问题。在您的生产虚拟主机部署 VMsafe 之前，您还需要首先完成相应的计划、测试和评估工作。

（作者：Edward Haletky 译者：李哲贤 来源：TechTarget 中国）