在 Win2003 安装 VMware

在 Win Server 2003 上安装 VMware

VMware Server 提供了一个免费的并且比较容易进入的服务器虚拟化方法，不过部署它的几个方面——尤其是配置，可能很棘手。即使这个产品是免费的，可如果在安装和安全化进程中出了错误，也将会付出很高的代价。本指南提供了 VMware Server 在安装、配置（主要注重高安全性）以及如何成功运行于微软 Windows 2003 服务器等方面的说明。

VMware Server 工作原理及组件回顾

VMware Server 是一个寄居性的虚拟化解决方案。它不是直接地安装到裸机服务器上。VMware Server 必须安装到一台服务器现有的操作系统上，比如说微软的 Windows 系统或 Linux 系统。VMware Server 由安装在主机操作系统之上的三个主要组件组成。它们分别是注册服务组件、授权服务组件和用户界面管理组件。

- VMware Server 的工作原理
- VMware 组件的回顾及准备主机服务器

配置和保护 Windows Server 2003

安装 Microsoft Windows Server 2003 是很简单的，多数 IT 部门对此也已经有了自己的标准方法。在本部分里，我们将着眼于 Microsoft Windows Server 2003 的配置、一些安全性问题以及关于安装 IIS 的要点、如何启用邮件日志和保护邮件服务器和关于更多的 VMware Server 配置技巧。

- 如何为 VMware 安装和配置 Windows Server 2003
- 如何保护 Windows Server 2003 和安装 IIS
- 如何启用邮件日志和保护邮件服务器
- VMware Server 配置指南

创建虚拟机和安装 OS

本部分学习如何创建虚拟机和安装客户操作系统。

- 如何在 Windows Server 2003 上创建虚拟机
- 在 Windows Server 2003 上为 VMware 安装客户操作系统

VMware Server 的工作原理

VMware Server 提供了一个免费的并且比较容易进入的服务器虚拟化方法，不过部署它的几个方面——尤其是配置，可能很棘手。即使这个产品是免费的，可如果在安装和安全化进程中出了错误，也将会付出很高的代价。本指南提供了 VMware Server 在安装、配置（主要注重高安全性）以及如何成功运行于微软 Windows 2003 服务器等方面的说明。

这一系列文章共分为八部分。在这一部分中，TechTarget 中国的特约专家 Andrew Kutz 主要为大家提供其部署和调配方面的指导以及对其工作原理的描述。在随后的几部分中，还将介绍其配置、安全性、客户系统的安装等等。

这一系列文章将会成为大家了解 VMware Server 在 Windows Server 2003 运行相关知识的一个捷径。而它于我个人对 VMware 虚拟服务器部署体现出来的优缺点的认识也将是一种升华。此外，VMware 自身配有 214 页的使用手册，我在本指南中经常参考这个手册。

当创建本指南时提出的一些假设：

首先，假设 VMware Server 正被安装在一台全新的或是另有用途的服务器上。VMware 可以被安装在一台现有的、而你却又希望其一些额外资源能够被更好地利用的服务器上，而本指南更强调确保 VMware Server 和主机操作系统（OS）的高效性和安全性，因此我所说的每一步都是基于一个现有的操作系统。

根据你的具体情况，如果本指南中所介绍的某一步骤无法实现，把它标记下来等待将来的部署，跳过它继续向前。有些步骤需要重新调整现有的配置，如涉及到在 Windows 上确保 IIS(Internet Information Server)安全性的部分。还有，你可以根据自身情况，选择执行我的建议或跳过它们。

我还假设你会将最高安全列为首要议程。因为 VMware Server 搭载有众多虚拟服务器，安全性是头等重要的。本指南将帮读者建立一个安全性极高的“堡垒主机”。

虚拟化经常被用来为虚拟网络服务器服务，所以我设想这类服务器将需要连入公共互联网。端口转换和网关设备（像一个 Netscaler 一样）是可以被限制的，特别是如果你想让若干个虚拟网络服务器同时分享 80、433 端口，而不是像 Netscaler 一样每个工作区都可以负担一个网管设备。我在后边将对此假设的两个例外情况进行论述。

我猜想大多数系统管理员都有坚实的 Windows 知识。本指南主要服务于那些新接触 VMware Server 的 IT 管理员，而不是新接触 IT 管理的人群。你可能将从中找到一些确保

Windows 安全的方便技巧和窍门，但是我不会告诉你磁盘阵列控制器代表什么，或者是在哪里配置 Windows 页面文件等等这类基础问题。

VMware Server的工作原理

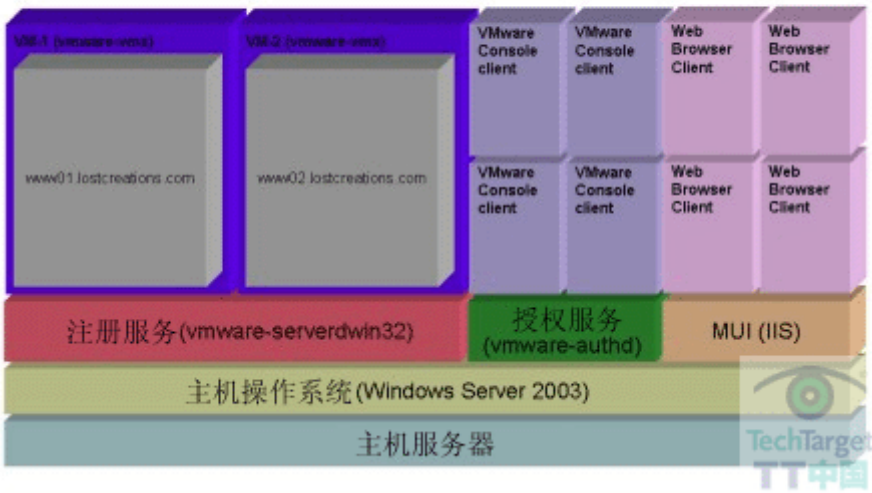
VMware Server 是一个寄居性的虚拟化解决方案。它不是直接地安装到裸机服务器上。VMware Server 必须安装到一台服务器现有的操作系统上，比如说微软的 Windows 系统或 Linux 系统。这与另一个 VMware 的服务器虚拟化产品——ESX，以及开放源代码虚拟化解决方案——Xen 形成了鲜明的对比。

现有操作系统的输入、输出任务是 VMware Server 的沉重负担，因此它也不如裸金属系统管理程序那样高效。在另一方面，它却有广泛的驱动程序兼容性，因为 VMware Server 能使用任何一个可与主机系统兼容的硬件设备。而一个裸机系统管理程序通常只支持有限数量的设备，因为其控制系统的核心程序和许多设备驱动程序没有形成汇编（目的是为了保持核心程序的简练和快速）。

Xen 比较特殊，它虽然是一个裸机系统管理程序，但它与其它硬件设备具有广泛的兼容性。这主要依赖于驱动域操作系统来实现（通常是 Dom-0 操作系统），而并不需要提供设备驱动程序。

这里是 VMware Server 工作原理的概述：

Windows主机上的VMware Server概况



位于此构架最底部的是物理主机服务器。位于裸机以上的那层是主机操作系统，在这种情况下选择的一般是 Windows 2003 Server 标准版。

VMware Server 由安装在主机操作系统之上的三个主要组件组成。他们分别是注册服务组件、授权服务组件和用户界面管理组件。注册服务组件负责虚拟机的启动和停止以及其客户连接。授权服务组件负责对从 MUI（Windows 多语版）和 VMware Server 控制台引入的连接进行验证。MUI 允许用户通过一个 Web 界面对虚拟机进行管理。

在本系列的第二部分，我将描述VMware Server最重要的部件和服务。

（作者：Andrew Kutz 译者：王霆 来源：TT 中国）

VMware 组件的回顾及准备主机服务器

只有 IT 天才可以不需做一些基础功课就直接跳转到基于 Microsoft Server 2003 的 VMware Server 的部署。不过，如果他们真的那么聪明，他们就将会意识到正确地安装这个免费的虚拟化平台和计算圆周率一样复杂。

这一系列文章的第一部分提供了关于VMware Server工作原理的一个基本指导方针和简短介绍。沿此继续往前，本部分将揭示VMware Server内部的重要组件及服务，以及如何准备主机服务器。后面的部分包括Windows安装、VMware Server的安全性等更多内容。

VMware Server组件

让我们来看看 VMware Server 最重要的组成部分，包括用户账号和群组、服务以及可执行文件。

用户账号和群组

在对 VMware Server 进行安装时，它会在服务器上创建一个名为“_vmware_user_”的用户账号。这似乎是从 VMware GSX Server 时代继承来的，又似乎已经被 VMware 授权服务所取代。

VMware Server 还会在服务器上创建一个名为"__VMware__"的群组。"__VMware_user__"是这个群组的成员。这个群组的成员拥有 "SE_INTERACTIVE_LOGON"用户权限，使他们能够在本地登录。使用这个群组是有好处的，它可以授权无管理权限账号对 VMware Server 进行远程连接。

服务

VMware Server 主要有以下服务组件：

- **VMware授权服务组件**负责侦听从本地以及VMware Server控制台应用程序引入的连接。它在 902 端口对这些引入的连接进行侦听。此外，该服务组件还负责验证用户。
- **VMware动态主机配置协议（DHCP）服务组件**负责给搭载在NATD服务器或私人网络服务器上的虚拟机供应IP地址。
- **VMware网络地址转换服务**允许搭载在NATD网络上的虚拟机与公共网络之间进行沟通。
- **VMware注册服务**用来启动和关闭虚拟机并负责管理它们的连接。

可执行文件

VMware-cmd.exe 程序可以用来从命令行控制 VMware Server 和虚拟机。要了解更多关于这个命令的知识只需键入以下命令提示符——"%ProgramFiles%\VMware\VMware Server\VMware-cmd.exe".此外，关于这个命令的更多信息可以在 www.vmware.com/support/developer 上找到。

VMware-vmx.exe 是宿主实际虚拟机的进程。这个命令运行的安全环境是非常重要的，稍后我们将对其进行讨论。

用户管理界面

由于在 VMware VI3 中被弃用，现在的 MUI（Windows 多语种版）已成为一个通过网络浏览器与 VMware Server 进行互动的途径。这通过 http://%HOSTNAME%:8222/和 athttp://%HOSTNAME%:8333/上的超文本传输协议是很容易实现的。而加密套接字协议层（SSL）是默认执行的。

准备主机服务器

在开始之前，将服务器的以太网电缆从网络端口上拔掉。大多数服务器之所以被黑客攻击是因为它们被安装在不安全的状态下。安全地断开服务器的网络连接，稍后再重启其网络连接。

如果服务器只有一个网络端口，可以安装一个 PCI（外设部件互连标准）以太网卡来提供一个额外的网络端口。这可以为虚拟机分别提供一个私人管理网络接口和一个公共网络接口。

多数为私人管理网络接口提供方便的措施将在这篇关于远程桌面协议、防火墙和 VMware 的文档中被论述，但有一步是现在就可以实现的。断开服务器上所有可用的网卡，将其中一个网卡的以太网电缆接入私人网络。此网络甚至不需要访问公共互联网，其唯一目的是给服务器管理员提供使用服务器的权限。

如果由于某种原因而使这一步不能完成，不必担心，使用 Windows 提供的工具也有可能可以创建一个私人管理网络接口。一个真实的、物理的私人网络只是对安全性的一个良好补充。

独立磁盘冗余阵列（Redundant Array of Independent Disk）

在配置应用程序时一个经常被忽略的部分是其磁盘的输入、输出要求。比这更频繁的，是在虚拟机出错时，我们总是会忽略磁盘访问速度过慢的问题，反而去猜疑 CPU 和内存。

有一个办法可以确保尽可能地给服务器的独立磁盘冗余阵列容器配置最佳的磁盘输入、输出。服务器中可用的磁盘数量应该决定独立磁盘冗余阵列的配置。这有一个可以方便你使用的列表：

—2 个磁盘—1 个容器，RAID-1(镜像)
—3 个磁盘—1 个容器，RAID-1（制作热备份）
—4 个磁盘—1 个容器，RAID-10
—5 个磁盘—1 个容器，RAID-10 或 2 个容器，RAID-1(系统)，RAID-1 制作热备份（数据）

RAID-5 通常不被使用，因为虽然它是受欢迎的，可会有一个处罚性的表现，就是在每次写入时要进行奇偶计算。

然而，每个人都有他自己的独立磁盘冗余阵列配置偏好，之前所作的尝试是为了给大家介绍一些配置方案，以实现在不牺牲冗余的情况下尽可能地提供最好的磁盘读写速度。标签“系统”和“数据”显示的是操作系统应该被安装到哪个容器中，此外，数据（在这种情况下指虚拟机）应该被分别存放。

在第三部分，TechTarget中国的特约专家Andrew Kutz将讨论如何安装Windows和它的组件。

(作者：Andrew Kutz 译者：王霆 来源：TT 中国)

如何为 VMware 安装和配置 Windows Server 2003

安装 Microsoft Windows Server 2003 很简单，但要将它正确地安装到 VMware Server 却会遇到一些特殊的挑战。在这篇关于在 Windows 上使用 VMware Server 的入门知识的系列文章中，TechTarget 中国的特约专家 Andrew Kutz 将对这些安装和配置的基本要点进行论述。

这一系列文章的第一部分对于VMware Server的工作原理提供了基本的指导方针和简单的研究。第二部分回顾了VMware Server内部重要组成部分和服务，以及如何准备主机服务器。接下来我们来看看如何为其安装Windows Server。

Windows Server及其组件的安装：

安装 Microsoft Windows Server 2003 是很简单的，多数 IT 部门对此也已经有了自己的标准方法。唯一的例外可能是磁盘分区。为操作系统和数据创建单独的分区（如果相关选项可用的话，将其创建在不同的 RAID——独立磁盘冗余阵列容器中）。这种配置方案既快速又安全。

当安装完成，操作系统启动时，请继续进行数据分区。在本指南的剩余部分中，我们将假定系统驱动是 C 盘驱动；数据驱动是 E 盘驱动。

既然系统驱动器和数据驱动器都已可用，就是该配置系统页面文件的时候了。将系统驱动页面文件参数设置为静态值 768，数据驱动页面文件的参数设置为机器 RAM（随机存取存储）值的两倍，或是机器所允许的最大值这样一个静态值。选择应用这些更改并重新启动计算机。

接下来设定系统的网络设置。如果机器有多个网卡，请务必给它们全部指派有效的网络设置。最好是将其中一个网卡配置到专用网络，这样的设置更有利于安全。

IIS（Internet Information Server）,SMTP(简单邮件传输协议)以及 Network Tools 重启之后，还有一些额外的 Windows 组件需要配置——IIS，SMTP 以及 Network Tools。IIS 对于 VMware Server MUI 来说，IIS 是 VMware Server MUI 所需的，最好还要有一个邮件服务器。

Network Tools 是一个并不常见的安装组件，但是它包含了非常方便的网络监控器——一个在网络协议标准上进行调试时很有用的工具。（因为是几个虚拟机分享一个共同的网络接口，有些时候可能有必要对接口的通信状况进行细致的检测）。

配置提示

你需要对一些设置进行调整以实现最佳的安全性和性能。

安装补丁

通常来讲，确保 Windows 安全性的第一步是给服务器安装补丁程序。那么你也许会问为什么在安装完成后没有将此作为第一步来实施。其实，并不是所有的补丁程序都应该在那时被安装，因为还有一些附加的组件尚未安装。还因为服务器是与网络断开的，在安装补丁程序前安装那些附加配置也不会损害到机器。

在安装完 Windows 及其附加配置后，再安装最新的服务包和补丁程序。因为此时并没有连接到网络中，要完成这一步需要从另一台安全的、无病毒的计算机 Microsoft Windows update（从 Windows 更新目录）那里下载所有最新的服务包和补丁程序，将其刻录到一张 CD 或是存到一个闪存盘上，然后从便携式媒体将其安装。

除非说该闪存盘有一个物理的写保护开关，可以在文件被拷进去后将其关闭。否则的话，CD 盘将是最安全的传输媒介。

网络设置

如果服务器有两个或两个以上的网络接口，将其中一个设为专门的管理界面（dedicated management interface）。

打开网络连接文件夹。如果一个网卡被放置在专门网络，选定这个网卡。如果没有的话，选定任何一个网卡。将这个连接重命名为“Private”。将其它连接重命名为“Public”（公共连接）；对于多于一个的连接，在“Public”后附加 01、02、03 等等，依此类推。

远程桌面

远程桌面服务应该监听专用管理界面上引入的连接。点击“开始”按钮，再点击“运行”选项，键入"tscc.msc /s"然后选择返回。在左侧，单击标记为“Connections ”的文件夹，在右侧，右击标记为"RDP-Tcp"的文件夹然后选择“Properties”。

这时会弹出一个新的窗口。单击标记为"Network Adapter"（网络适配器）的标签，你会看到一个标记为"Network Adapter"的下拉菜单。选择"All network adapters configured with this protocol"（所有配置到此协议的网络适配器）。这意味着机器上所有的网卡都会监听 3389 端口（默认的 RDP 远程桌面协议端口）上引入的远程桌面客户连接。

而这并不是我们想看到的结果。我们要限制远程桌面协议，使其只听从一个在专用网卡上引入的连接。

选择已被指定为专用管理界面的那个网卡。

如果此服务器在 DNS（域名解析服务器）中被注册，它的 DNS 名是不会回应 RDP 连接的，除非该服务器的 DNS 登陆程序指出了已被指定为专用管理界面的那个网卡的 IP 地址。

你还需要将 DNS 登陆程序注册到专用管理界面的 IP 地址，然后再创建另一个到专用管理界面 IP 地址的登陆程序。或者，你也可以让服务器管理员给他们的客户机创建一个已经直接指向专用管理界面的 RDP 捷径。最后这项选择也是最安全的，因为对于一个对它试图攻击的 DNS 服务器名称有疑问的攻击者来说，它是不会得到那个揭示了服务器 RDP 端口的登陆程序的。

磁盘高速缓存

使 E 盘实现高速缓存可以提高 VMware Server 的性能，因为虚拟磁盘镜像文件将会被存到这里(VMware Server 管理手册第 153 页)。这个选项应该已经被启用了，但是为了对此进行核对，请点击“开始”按钮，单击“运行”选项，然后键入"compmgmt.msc"，选择返回。

在左手一侧点击“Storage”，然后点击“Disk Management”。右击包含有 E 盘驱动（也可能是磁盘 1）的硬盘并且选择“Properties”。

此时将会出现一个标记为"Local Disk (E:) Properties"（“本地磁盘(E:) 属性”）的窗口。单击标记着"Hardware."（硬件）的标签。键入"Disk drives"（磁盘驱动）选择第一个磁盘驱动器。点击"Properties"（属性）按钮，将会出现一个新的窗口。单击标记为"Policies"的标签。

确认标记为"Optimize for performance"（优化性能）的选项被选中并点击该选项，然后再次点击"OK"（确定）按钮。现在可以关闭“计算机管理”应用程序并继续下一步了。

磁盘碎片整理

由于受到存储虚拟磁盘的文件夹尺寸所限，虚拟磁盘的分裂和破碎会导致磁盘性能的严重退化。VMware 建议运行磁盘碎片整理程序来降低磁盘分裂和破碎程度。Microsoft Windows Server 2003 装载有一个磁盘碎片整理程序工具，但实际上还有一个更好的可以

用。尽管说不是免费的，但是要想在磁盘碎片整理方面击败 O&O Defrag（磁盘整理工具）几乎是不可能的。

在作者写这篇文章的时候，O&O Defrag V8.5 Server 一个单一用户许可的费用是 219 美元。此外，它还提供一个三十天的试用期。谨慎地讲，这毫无疑问是一个唾手可得的、作者使用过的最好的磁盘破碎文件整理工具软件

在第四部分中我们将着眼于一些安全性问题以及关于安装IIS（Internet Information Server）的要点。

（作者：Andrew Kutz 译者：王霆 来源：TT 中国）

如何保护 Windows Server 2003 和安装 IIS

一旦启动和运行 Windows，我们应该如何保护它以及怎样安装 IIS（Internet 信息服务器）呢？

前面几个部分的文章已经讨论过 VMware Server 如何工作、如何准备主机服务器以及如何安装 Windows。在本文中，TechTarget 中国的特约专家 Andrew Kutz 将讨论如何保护 Windows Server 2003 和安装 IIS。

Windows安全性

下面介绍几种让 Windows 更加安全的方法。

伪造管理员帐户

创建伪管理员帐户是一个摆脱某些爱管闲事的人的好方法。虽然这并不能防止真正的黑客企图，但是加密至少还会让诚实的人保持诚实，对吧？

给管理员帐户重新命名，如“lucy”，然后断开之后重新连接。连接之后，立刻创建一个新的帐户，命名为“Administrator”。剪切（不要复制）原管理员帐户的描述（现在叫“lucy”）粘贴到伪管理员帐户的描述中。把新管理员帐户的密码设置得很长很长（密码的复杂性并不那么重要，尽管安全专家 20 年前就说过密码应该复杂），用 50 个或更多字符，然后禁用这个帐户。这只是“深入防守”的一个实例。

保护数据区

接下来，在 E 盘创建如下文件夹层次：

```
DATA
 \var
 \log
 \mail
 \vms
 \tmp
```

有人可能会发现它和标准*NIX 文件夹名有相似之处。短目录名简明扼要，如果它不名一文，就不要用了。

在 var 目录下设置安全性，只允许 SYSTEM 帐户和 Administrator 帐户组享有完全控制权。移除 var 文件夹的所有其它许可，在子文件夹中，用适用于 var 的许可替换所有现有许可。

事务日志

现在，打开注册表编辑器，设置以下一些值：

- HKLM\SYSTEM\CurrentControlSet\Services\Eventlog\Application\File - "e:\var\log\applog.evt"
- HKLM\SYSTEM\CurrentControlSet\Services\Eventlog\Security\File - "e:\var\log\seclog.evt"
- HKLM\SYSTEM\CurrentControlSet\Services\Eventlog\System\File - "e:\var\log\syslog.evt"

重启计算机，以便新的事务日志设置生效。

防火墙

重启之后，打开 Windows 防火墙设置，为所有连接开启防火墙，打开远程桌面端口（3389 号端口，远程管理），902 号端口（VMware Server 远程控制台），8222 号端口和 8333 号端口（分别是 VMware 网站为 HTTP 和 HTTPS 使用的端口）。

在防火墙属性窗口打开后，配置防火墙的日志文件设置是个不错的想法。设置防火墙日志文件地址为“e:\var\log\pfirewall.log”。最好把防火墙日志文件的默认大小增加一些，如 10M。

服务禁用

还有一种确保服务器安全的方法是禁用服务器不需要运行的一些服务。下面一些服务可以放心的禁用，VMware Server 仍会工作：

Alerter - ClipBook - Computer Browser - Distributed File System - Distributed Link Tracking Client - Distributed Link Tracking Server - File Replication - Indexing Service - Messenger - NetMeeting Remote Desktop Sharing - Network DDE - Network DDE DSDM - Remote Access Auto Connection Manager - Remote Access Connection Manager - Removable Storage - Telephony - Uninterupptable Power Supply - WinHTTP Web Proxy Auto-Discovery Service

IIS

现在，我们把注意力转向一些配置 IIS 的策略。

限制 MIME（多用途互联网邮件扩展）类型

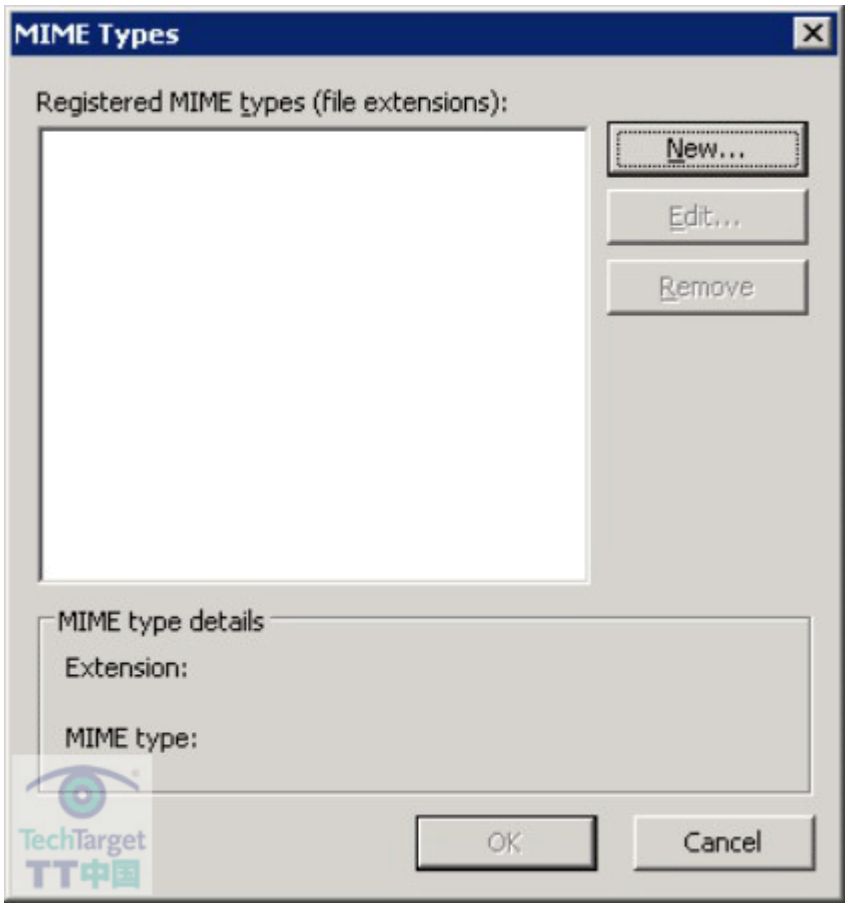
重要提示：如果这是个现成的 Web 服务器 ，一定要非常小心这一步。它可能导致 Web 服务器完全停止所有服务内容。所以，要小心谨慎。

MIME 类型会告诉 IIS 如何根据文件的扩展名处理各种类型的文件。例如，.exe 扩展名的 MIME 类型是“application/octet-stream”，IIS 就知道它是一个二进制文件了。

这一步会移除 IIS 能识别的所有 MIME 类型。这似乎比较过激，但是你可以这样考虑：如果一个新的 IIS 漏洞被发现，而且它依赖于 IIS 能够服务扩展名为“ida”的文件，由于 IIS 不识别这个 MIME 类型而不能服务这个文件，那么会发生什么？答案是什么都不发生。这个文件将不会被服务，服务器就不会受到这个特定的漏洞利用的威胁。

打开 IIS 管理器，右击本地电脑，点击属性，然后点击“MIME 类型”按钮。现在，点击第一个条目然后按下 SHIFT 键。展开下拉卷轴，点击最后一个条目。

如果正确完成，会选择整个列表（CTRL-A 在这里无效）。点击“移除”按钮，确定警告提示。这时，列表中就应该没有 MIME 类型了。

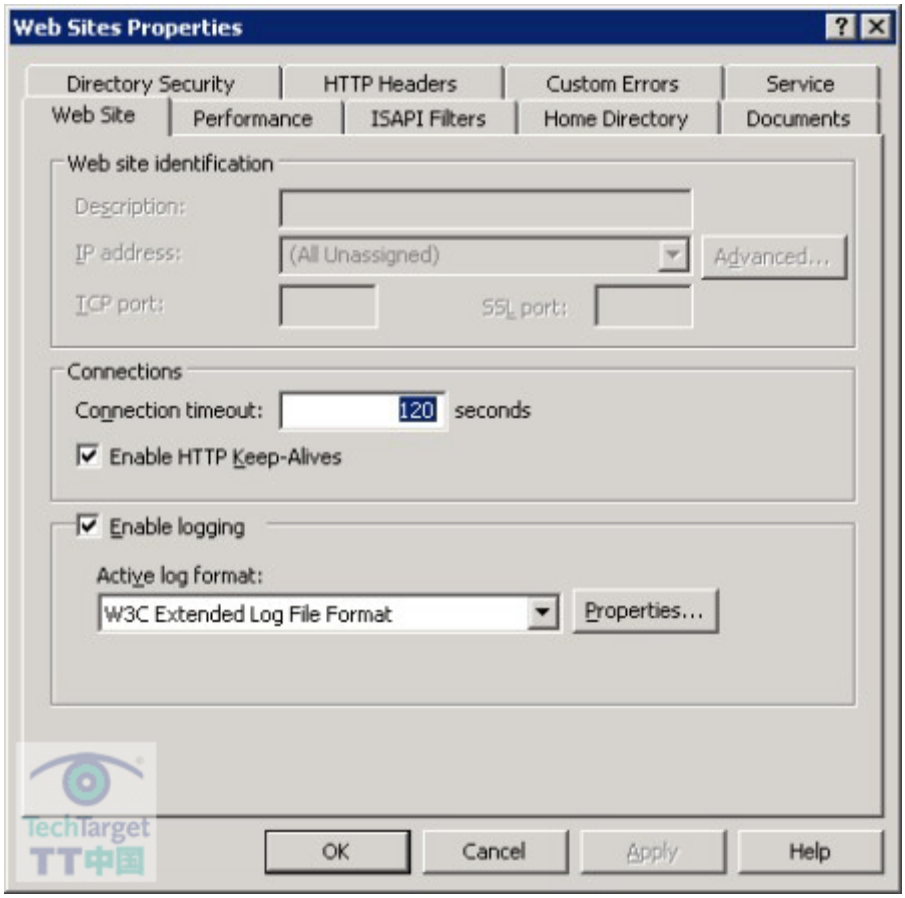


点击“确定”，然后再次“确定”。

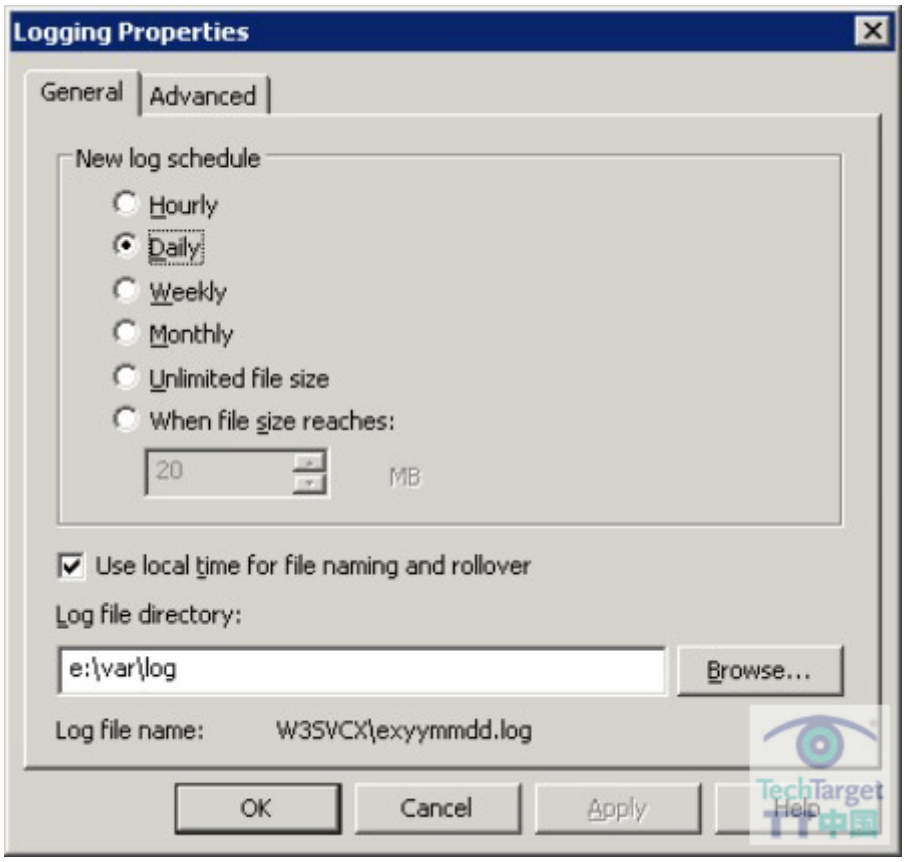
这一步限制了 IIS 服务任何非系统 MIME 类型。但是 IIS 需要能够服务某些文件，如扩展名为.html 的文件。这个问题将在下文中解决。

IIS日志

在 IIS 管理器中，右击“网站”文件夹，选择属性，会出现一个窗口，默认选择的是“网站”标签。确保选中“启用日志”复选框。



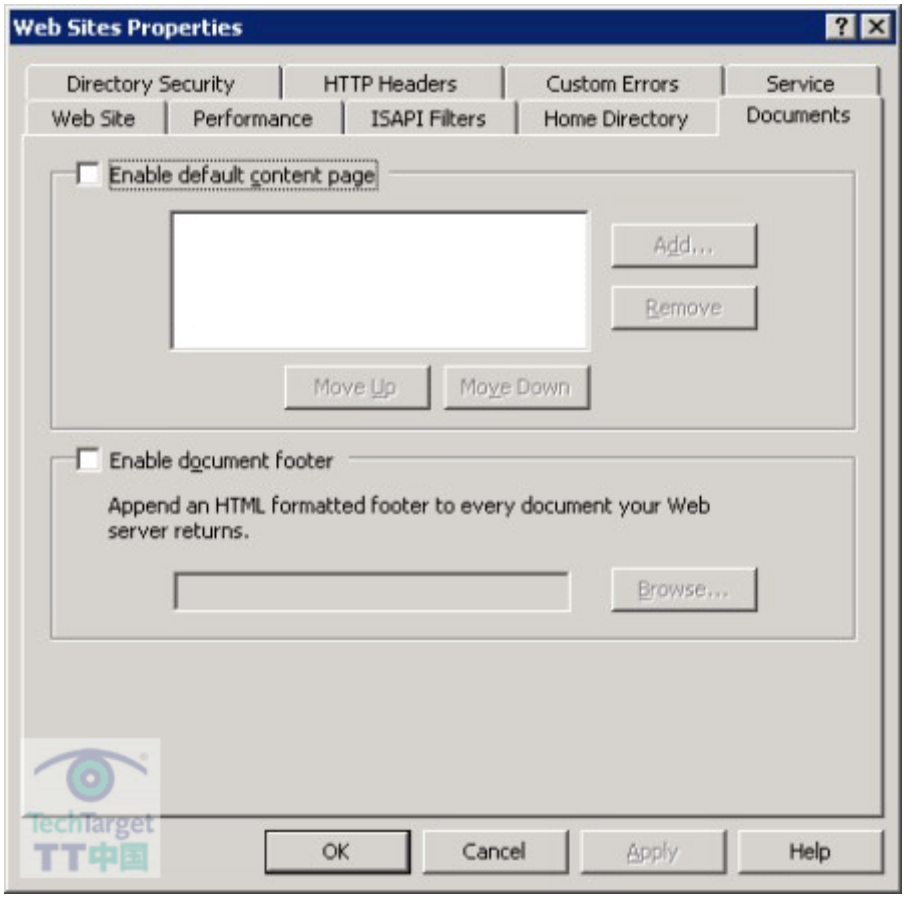
点击“属性”标签，选中“文件命名和 rollover 使用本地时间”复选框，设置“日志文件目录”为“e:\var\log”。



点击“高级”选项，确保选中所有扩展的选项，然后点击“确定”。

默认内容页

点击“文档”选项，移除所有默认的内容页，然后退选“启用默认内容页”复选框。现在，这个窗口应该是这样的：

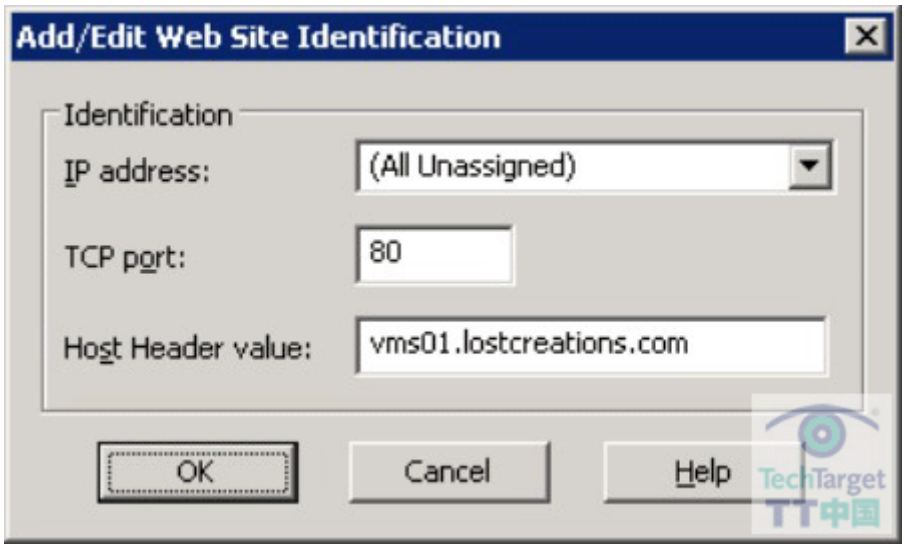


点击“确定”。

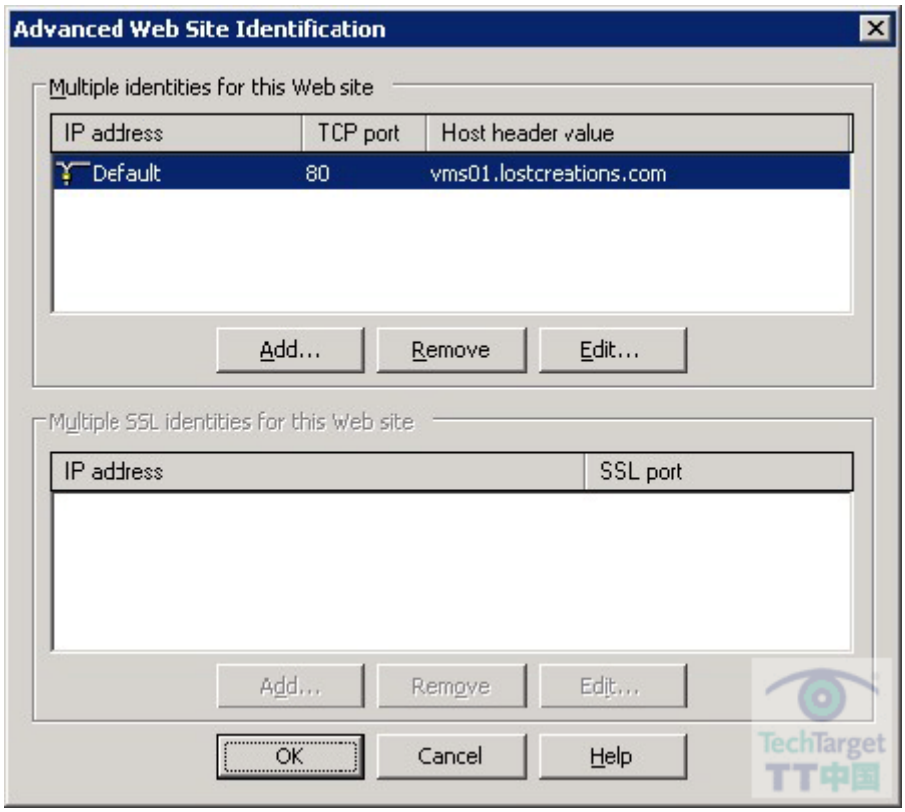
默认网站和默认应用池

有一个避免受攻击的方法是设置主机头名（host header value）。这可以使从 Web 服务器 80 号端口对 IP 地址的直接攻击完全失效，当设置主机头名后，如果 HTTP 请求向服务器提供所设置的主机标头字段，这个请求才有效。

要设置这个值，展开“网站”文件夹，右击“默认网站”，点击属性会打开一个新窗口“默认网站属性”。点击窗口右上方的“高级”按钮，会出现一个新窗口“高级网站鉴定”。选择有默认 IP 地址的条目，点击“编辑”按钮。设置主机头名为服务器 FQDN，点击“确定”。



现在，这个窗口应该像这样。



现在攻击者就不可能轻易地强迫“默认网站”使用服务器的 IP 地址了。倒不是说这非常重要，因为下一步是禁用“默认网站”和“默认应用池”。

展开“网站”文件夹。现在，右击“默认网站”文本，单击“停止”。接下来，展开“默认应用池”文件夹，右击“默认应用池”，单击“停止”。

因为 VMware Server 不适用默认网站，所以禁用默认网站和服务于它的应用池很安全。之所以禁用了网站之后还要设置主机头名，是为了防止万一系统管理员偶然启用网站。

之所以不删除默认网站和默认应用池，是因为默认网站在 IIS Metabase 中有特殊意义。它是唯一网站 ID 为 1 的网站，有些应用需要 IIS Metabase 中存在 ID 为 1 的网站，不然会出严重问题。

(作者：Andrew Kutz 译者：涂凡才 来源：TT 中国)

如何启用邮件日志和保护邮件服务器

启用邮件日志和保护邮件服务器是为 VMware Server 使用做准备的一个重要步骤。本系列的前面几部分已经讨论了 VMware Server 的各个组成部分、安装和配置 Windows 与 IIS，在本文中，TechTarget 中国的特约专家 Andrew Kutz 将讨论关于 SMTP 的问题。

首先，需要完成一些基本步骤以启用邮件日志和保护邮件服务器。

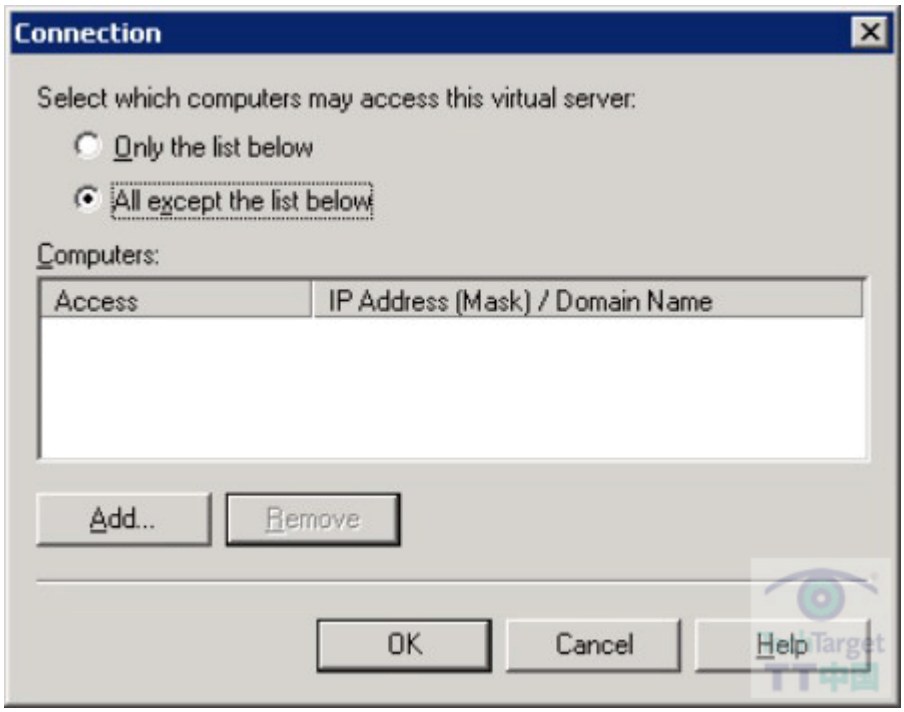
SMTP（简单邮件传输协议）日志

右击 “默认 SMTP 虚拟服务器” 文本，然后点“属性”。接下来选中“启用日志”复选框，然后点击右下角的“属性”按钮。弹出的窗口你应该很熟悉，它和前面设置的网站文件日志属性窗口是一样的。

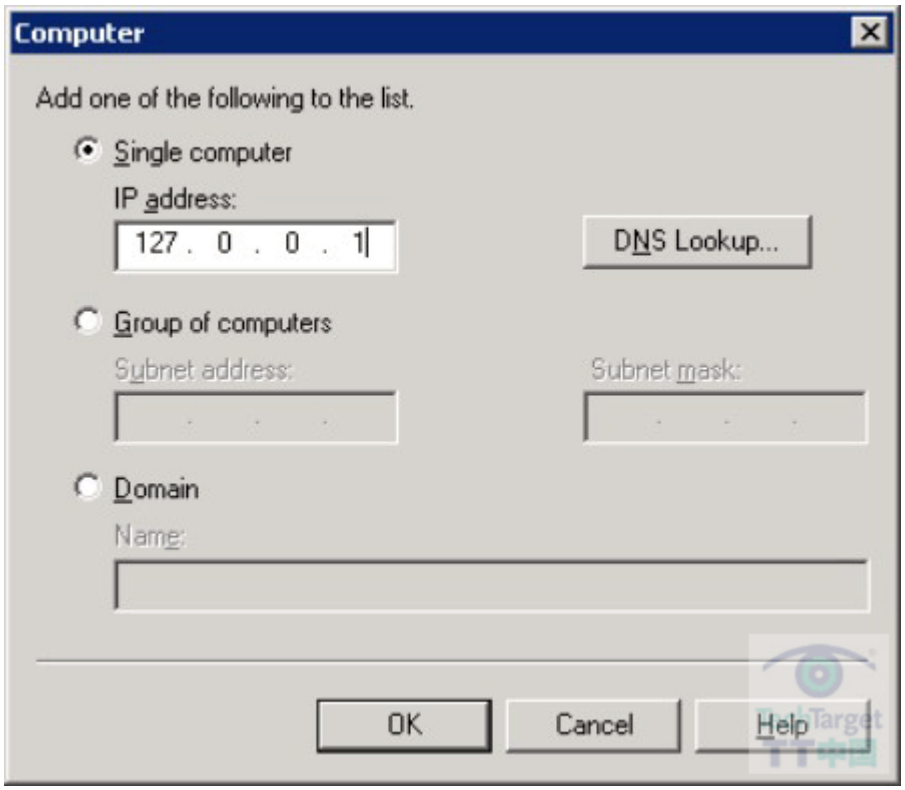
确保选中“文件命名和翻转（rollover）使用本地时间”复选框，然后点击顶部的“高级”标签。确保选中“扩展日志选项”下面所有的复选框，然后点击“确定”。

访问控制

控制 SMTP 服务器的访问权限很重要。点击“访问”，然后点“连接”，会出现如下“连接”窗口：

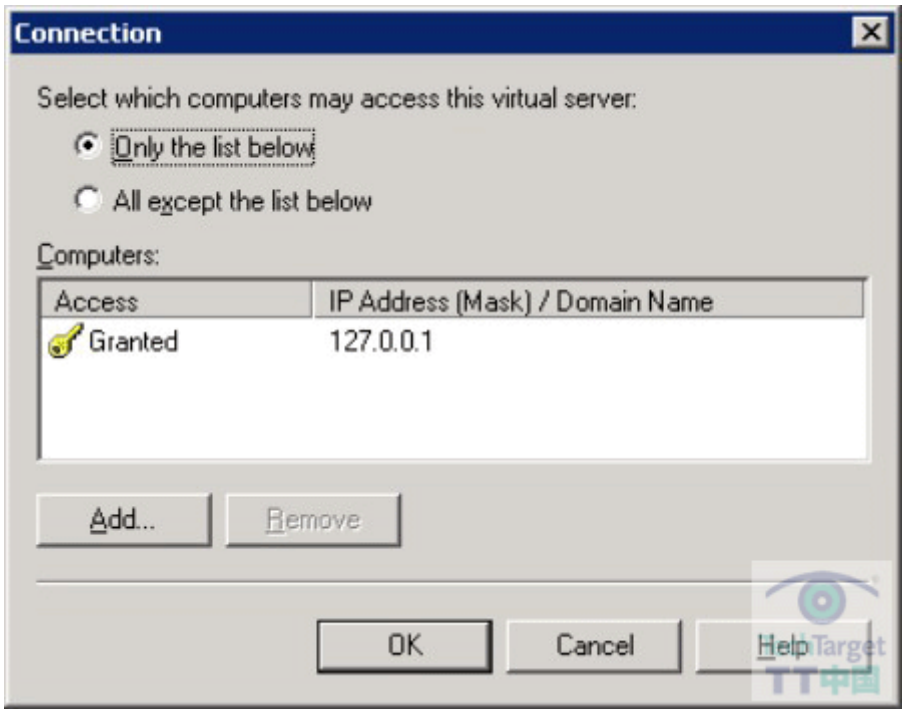


应该设置只允许本地主机连接到 SMTP 服务器。首先点击“只允许如下列表访问”，然后点“添加”，会出现一个新窗口“计算机”。在标题 “单个计算机”下面输入“127.0.0.1”，本窗口如下所示：

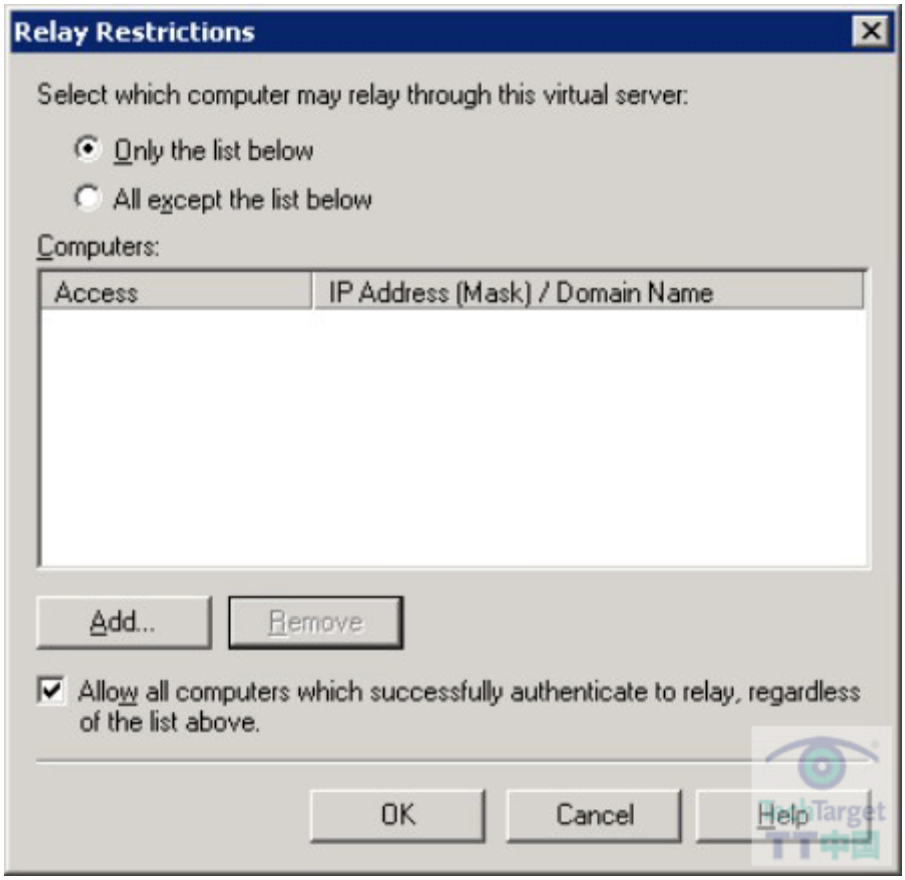


点击“确定”。

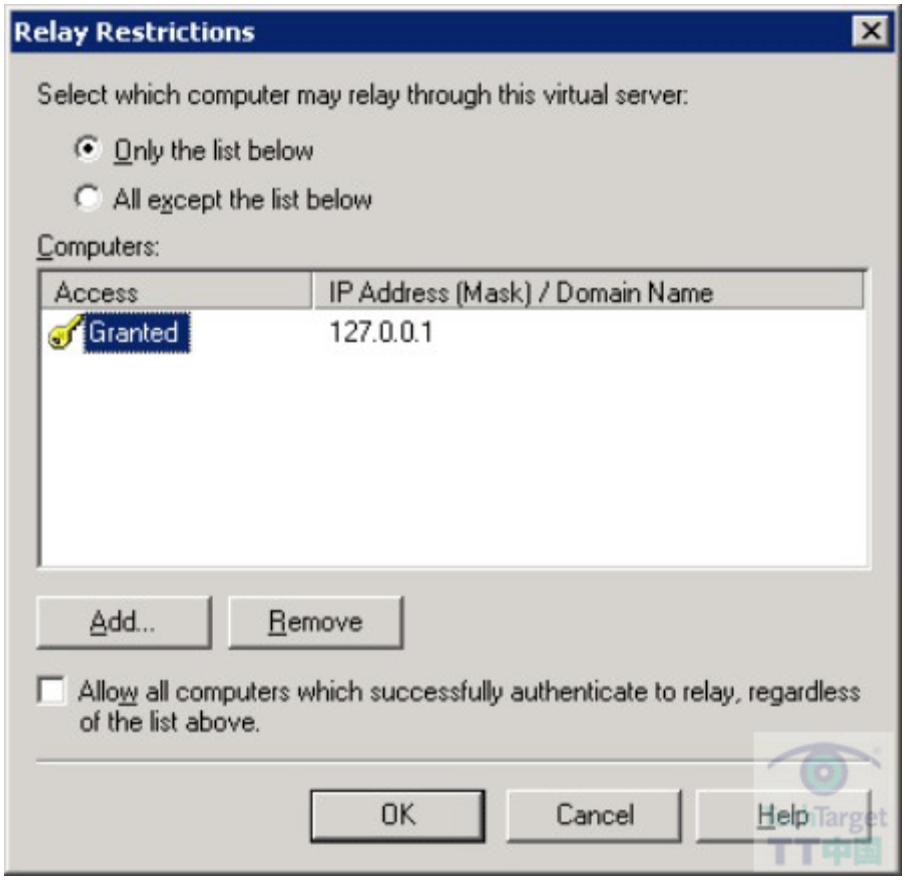
现在，“连接”窗口应该是这样子的：



点击“确定”。然后点“中转”按钮，会出现一个这样的“中转限制”窗口：



点击“添加”按钮，会出现一个新的“计算机”窗口，和前面出现的那个差不多。重复原来那个操作，即在“单个计算机”下面输入“127.0.0.1”，然后点“确定”。现在，退选“允许所有获得证书的计算机中转”复选框，不要管上面的列表。这个窗口应该是这样的：



点击“确定”。

邮件目录

现在，应该重新设置邮件目录以保护数据区。点击“消息”，在“垃圾邮件目录”标题下面输入“e:\var\mail\badmail”。如果此目录还不存在，没有关系，这个过程会创建一个。点击“确定”。

现在，点击“默认 SMTP 虚拟服务器”旁的加号（+）以增加它的大小。点击“域”文本框。

在屏幕右方应该是“域名”栏下的服务器名条目。右击此条目，然后点击“属性”会出现一个“%HOSTNAME%属性”新窗口。在“drop 目录”下输入“e:\var\mail\drop”并点击“确定”。

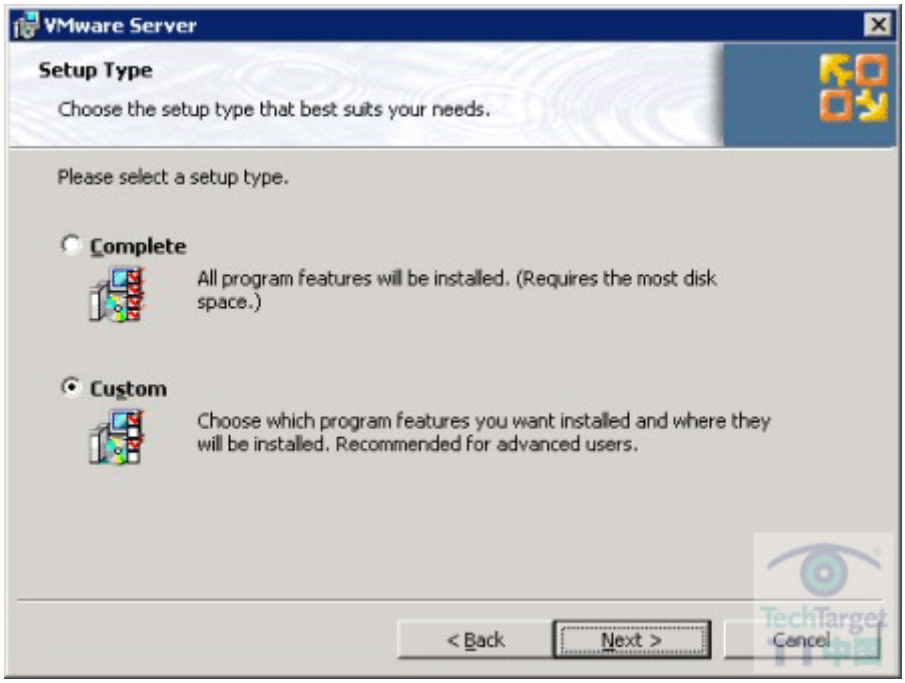
现在，就可以关闭 IIS 管理器了。

安装VMware Server

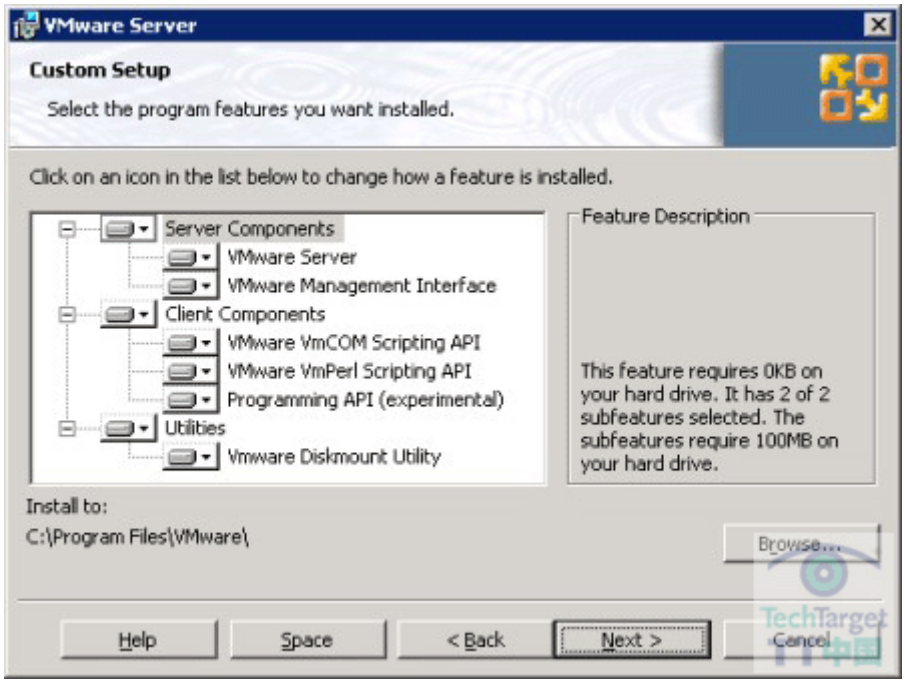
虽然需要一点时间，但现在是时候安装 VMware Server 了。

首先，从一台安全的计算机上下载最新版本的 VMware Server，通过刻录 CD-ROM 或带有物理只读开关的闪存盘将其转到服务器上。

双击安装程序。安装程序步骤很简单，只需按照屏幕说明一步一步操作，直到出现如下窗口：

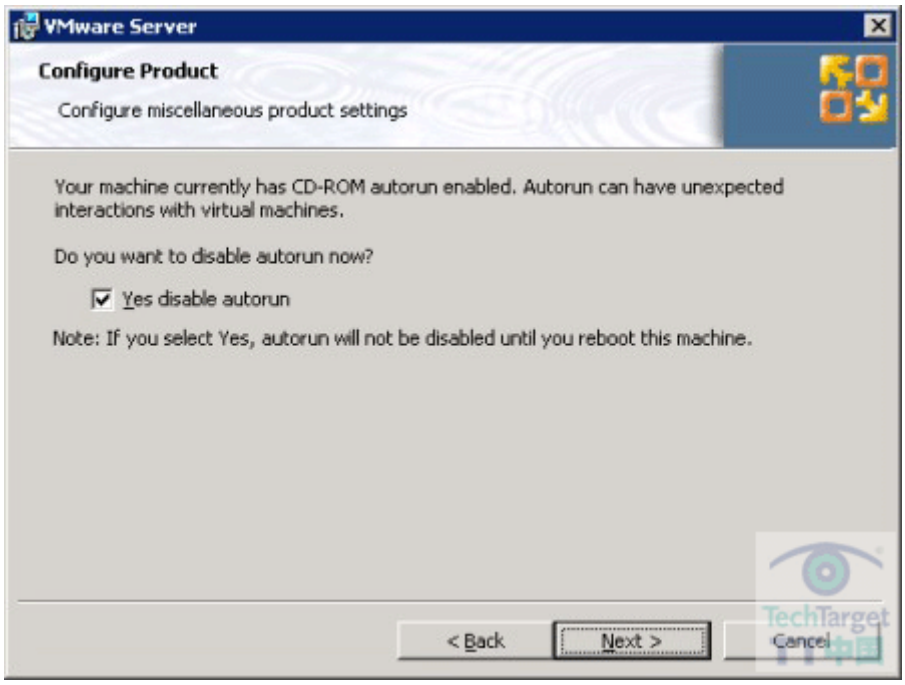


选择“自定义”，然后点击“下一步”。所有的选项都默认选择：

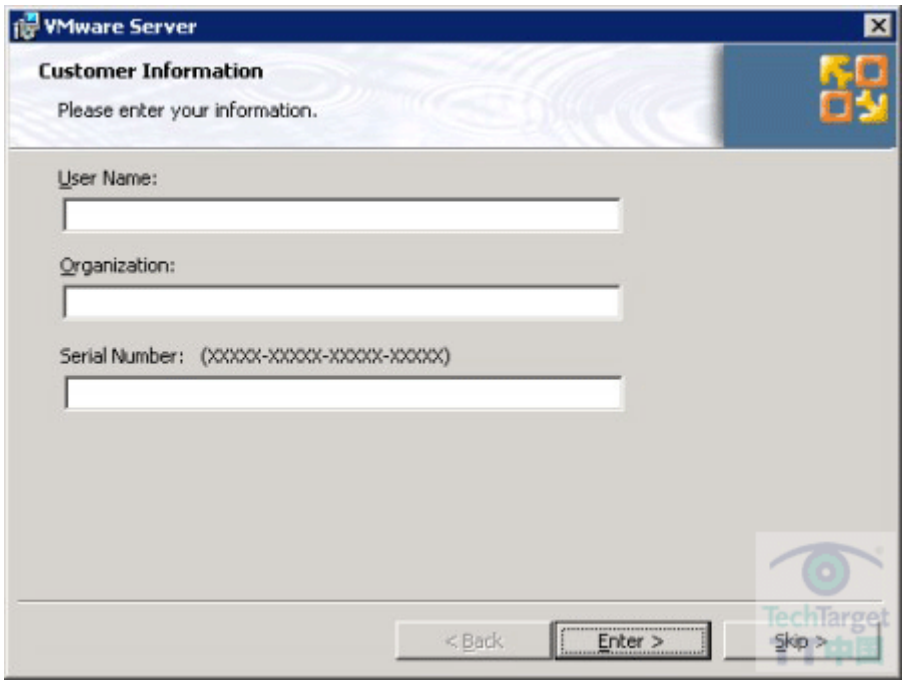


这和“完全”安装选项的设置是一样的，但是这个方法可以查看即将安装的所有组件。

点击“下一步”，会询问是否禁用“自动运行”。选中此复选框，如图所示：



点击“下一步”。然后点击“安装”以继续进行安装。安装完成后，会询问一些信息，特别是 VMware Server 序列号。



要获得 VMware Server 免费序列号，登陆 VMware 网站的这部分，点击“现在注册”。输入序列号，然后点击“下一步”。

现在VMware Server就可以运行了。在本系列的下一篇文章中，我们将讨论如何设置和保护VMware Server。

(作者：Andrew Kutz 译者：涂凡才 来源：TT 中国)

VMware Server 配置指南

VMware Server 的安装只是第一步，不过，它的配置却是一个全新的整体。

如果你是按照我们的系列做下来的，那么你知道我们已经讨论过各个组件、安装步骤和主机服务器上的 Windows 配置，包括一些安全性调整。然后我们讨论了 VMware Server 安装。在本文中，TechTarget 中国的特约专家 Andrew Kutz 将讨论 VMware Server 的配置。

配置

VMware Server 可能是安装了，但是它的 MUI 现在还是用不了。因为当 IIS 受保护时，所有的 MIME 类型都已从 IIS 根目录下删除了。

在初始安装时，如果在文件夹级别进行设置，让 VMware Server 网站的每个文件夹只能服务于它内部的文件，而不是添加许多 MIME 类型到 IIS 根目录或者 VMware Server 网站，这样难道不会更安全吗？当然，这将更加安全。但是这个设置过程将会非常单调乏味。除非你已经有一个执行这个操作的脚本。

事实上，这样的脚本是存在的，你可以从这里下载：http://www.lostcreations.com/~akutz/chmt.wsf.zip。编者提示：你需要一个zip文件管理器打开这个文件，如Winzip。Chmt.wsf表示“改变MIME类型”。它通过给定的网站标识符列举网站，然后通过网站内容的物理文件夹和文件重新出现。在脚本运行时，它会限制IIS metabase中的相应文件夹只能服务于物理文件夹中存在的MIME类型。

要获得 VMware MUI 网站 ID，打开 IIS 管理器，点击“网站”文件夹。在屏幕右边有一个“VMware 管理界面 1.0.1”条目，在它的“标识符”下面有一个号码，这就是你要的 ID。

运行这个脚本还要求服务器上存在 IIS 管理脚本“adsUtil.vbs”。IIS 管理脚本一般在“c:\inetpub\adminscripts”。

下面是 chmt.wst 脚本的使用实例：

```
C:\Inetpub\AdminScripts>cscript chmt.wsf
 Microsoft (R) Windows Script Host Version 5.6
 Copyright (C) Microsoft Corporation 1996-2001. All rights reserved.
```

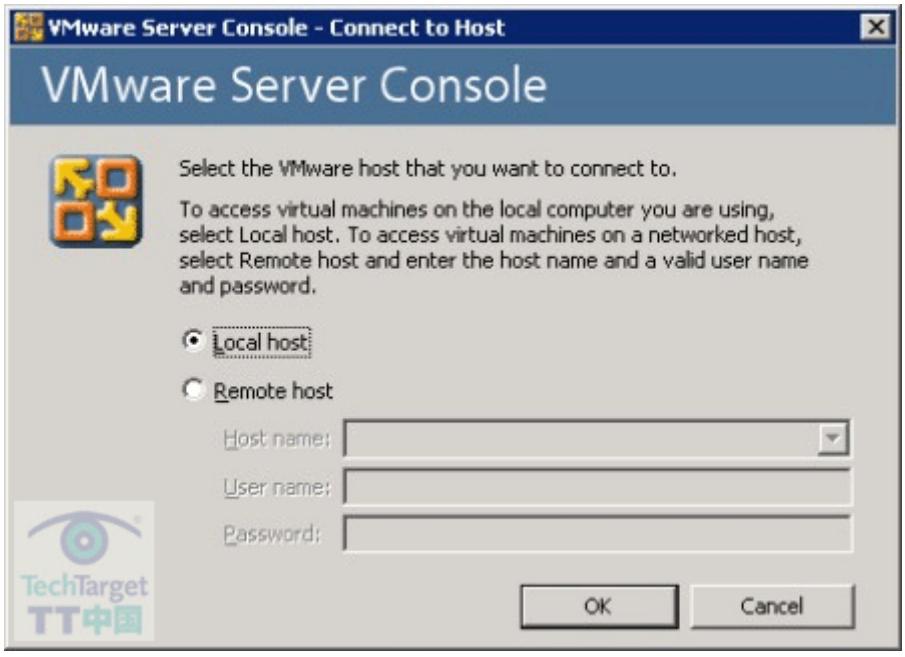
```
Usage: chmt.wsf /w3svcID:value [/webRootPath:value] [/adsUtilPath:value]

Options:

w3svcID : The IIS ID of the website.
webRootPath : The path to the directory of the web root.
adsUtilPath : The path to the adsUtil.vbs file.
```

“WebRootPath”选项默认为“%ProgramFiles%\VMware\VMware Management Interface\htdocs”，“adsUtilPath”选项默认为“c:\inetpub\adminscripts\adsutil.vbs”。

虚拟机位置

设置 MIME 类型之后，点击“开始”按钮，装载 VMware Server 控制台客户端。依次点击“所有程序”、“VMware”、“VMware Server”，然后点击“VMware Server 控制台”。

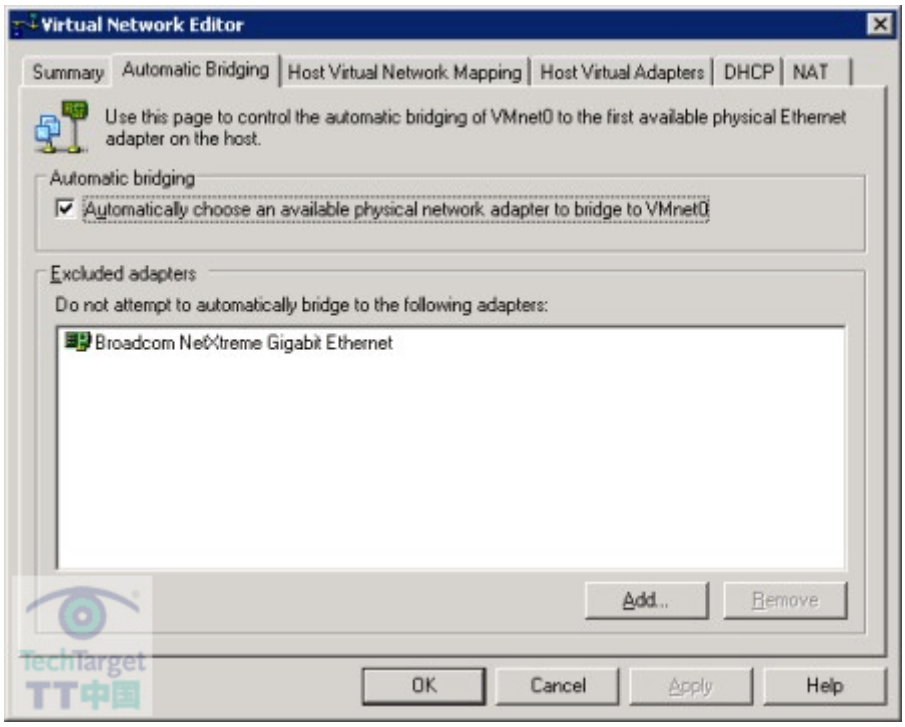
控制台打开时在大窗口上会有一个小窗口。小窗口叫做“VMware Server 控制台-连接主机”。



点击“确认”连接，然后点击“主机”菜单项的“设置”。更改“虚拟机默认位置”为“e:\var\vms”。这个地址是前面设置过受保护的，这样就只有“SYSTEM”帐户和“Administrators”组的用户可以访问虚拟机。

网络共享

下一步是防止VMware Server使用服务器管理专用的网络。点击“主机”菜单项，然后点击“虚拟网络设置”，会弹出一个窗口“虚拟网络编辑器”，点击“自动桥接”。窗口会是这个样子：



点击“添加”按钮，添加前面为管理界面所选的网络接口，这个接口还会监听 RDP 通信。在截图中，它是“网卡驱动”界面。

这一步会防止 VMware Server 在桥接模式下通过虚拟机操作接收或发送网络通信。

点击“确定”按钮退出此窗口。现在，可以关闭 VMware Server 控制台了。

安全性

在保护 VMware Server 日志之前，启用 VMware 证书服务日志。默认下，此服务是关闭的，但是在用 VMware Server 调试某些问题时，此服务是非常有用的。

要启用日志，只需在文件“%ALLUSERSPROFILE%\applicationdata\vmware\vmware server\config.ini”中添加如下代码行即可：

```
vmauthd.logEnabled = TRUE
log.vmauthdFileName = "vmauthd.log"
```

打开命令提示符，输入如下命令：

```
net stop vmauthdservice
 net start vmauthdservice
```

这会重启 VMware 证书服务，并启用日志。

保护

通过限制如下位置的许可，可以使“SYSTEM”帐户和“Administrators”组拥有完全控制权并删除其它所有许可，从而保护 VMware Server 日志：

%SystemRoot%\system32\vmauthd.log - this is the VMware authorization servicelog

%ProgramFiles%\VMware\VMware Management Interface\mui.log——这是 VMware Server MUI 日志。

这些不是所有日志文件的地址，仅仅是系统服务运行的日志文件。还有与用户和虚拟机相关的日志文件在其它位置。更多 VMware Server 日志文件信息，请见 VMware Server 管理操作手册第 22 页。

SSL证书

VMware Server MUI SSL 证书存放在“%ProgramFiles%\VMware\VMware Management Interface\SSL”。默认下，这个目录是不受保护的。删除此目录的继承，复制现有的许可。除了“SYSTEM”帐户和“Administrators”组以外，删除此目录的所有其它许可。点击“确定”。

进入“SSL”目录，“mui.key”是MUI的SSL私钥文件。此时它应该继承其父级的许可和“SYSTEM”帐户和“Administrators”组的完全控制权，没有其它许可在这个文件中。这个设置对私钥文件来说太不安全了。直接从文件中删除继承，设置许可，让“SYSTEM”帐户和“Administrators”组对此文件只有读取许可。

监测

监测VMware Server有好几种方法，要看它如何工作，最简单的方法是在https://%HOSTNAME%:8333/访问VMware Server MUI。MUI会显示服务器运行虚拟机的使用统计数据。

另一种监测VMware Server的方法是用VirtualCenter 1.x.。它可以管理VMware Server主机，提供它们的部分数据。

最后，还可以用Microsoft Performance Monitor监测VMware Server。VMware Server安装了性能计算机，可以用于监测虚拟磁盘活动，内存使用和虚拟机网络通信。

备份

VMware Server没有与ESX相同的热备份能力，因此在备份虚拟机之前将其暂停是有必要的。VMware Server管理操作手册的第95页简要地说明了如何在主机上备份虚拟机和在虚拟机中配置备份代理。在这里逐字地重复VMware自己的说明没有意义，所以，这部分我们遵从官方指南。

在本系列的下一部分中，我们将讨论创建虚拟机的过程。

(作者：Andrew Kutz 译者：涂凡才 来源：TT中国)

如何在 Windows Server 2003 上创建虚拟机

缺少了虚拟机，虚拟化还有什么好处呢？

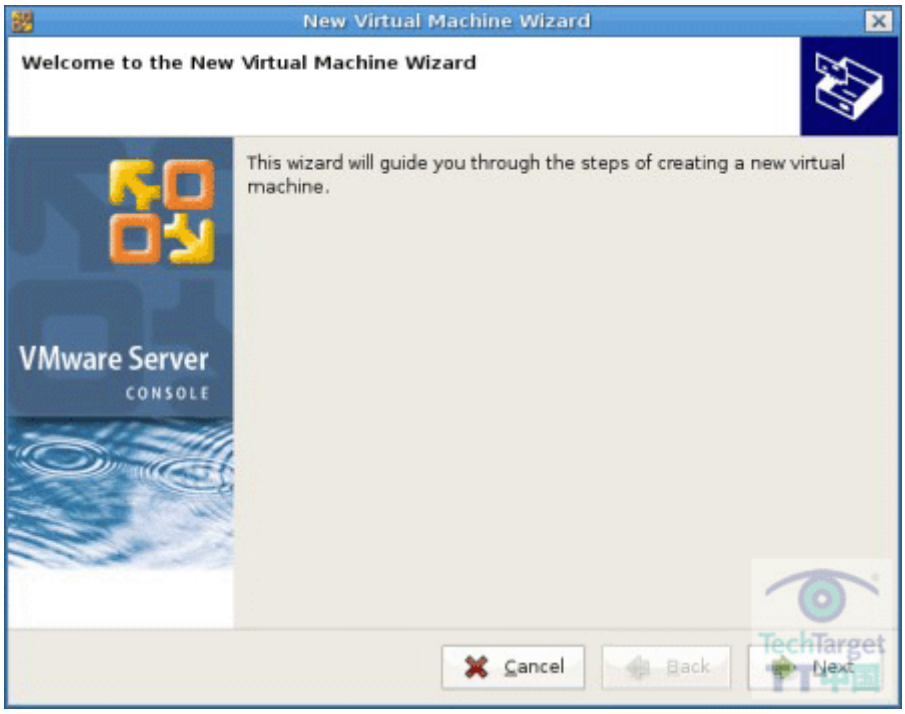
到目前为止，关于 VMware Server、服务器上 Windows 的安装与配置、VMware Server 本身的安装与配置、IIS（Internet Information Server）和 SMTP（简单邮件传输协议）的配置等部分已经在前面几部分文章中讨论过了。在本文中，TechTarget 中国的特约专家 Andrew Kutz 将讨论关于如何创建虚拟机的问题。

用 VMware Server 创建虚拟机非常容易。首先，点击开始按钮启动 VMware Server 控制台，接下来点击"所有程序"，再点击"VMware"，选择"VMware Server"，然后点击"VMware Server 控制台"。

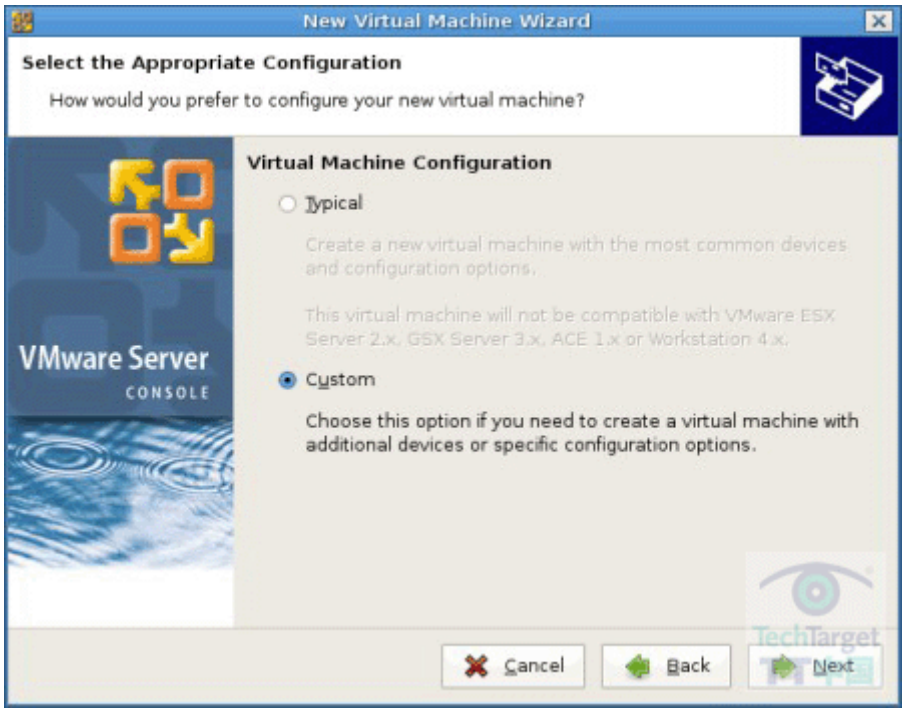
顺便说一下，安装程序本应该在桌面上创建一个 VMware Server 应用程序的快捷方式，但是如果你发现没有创建的话，请继续往下，并手动创建一个这样的快捷方式。这主要是考虑到该应用程序使用得非常频繁。

一旦 VMware Server 控制台加载成功，单击标有"文件"的菜单选项，然后点击"New"并选择"虚拟机"。有一个组合键也可以实现此任务——CTRL-N。此外，位于 VMware Server 控制台主屏幕中央的大按钮也可以用来创建新的虚拟机。

接下来就会出现一个标题为"新虚拟机创建向导"的窗口。点击"下一步"按钮。

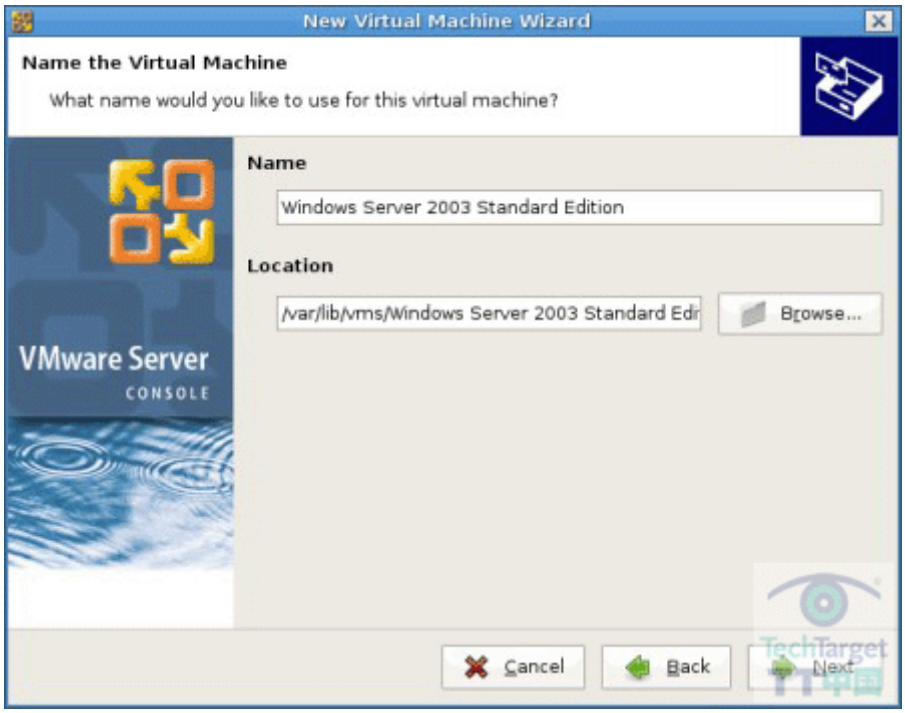


选择"自定义"选项，然后点击下一步"。

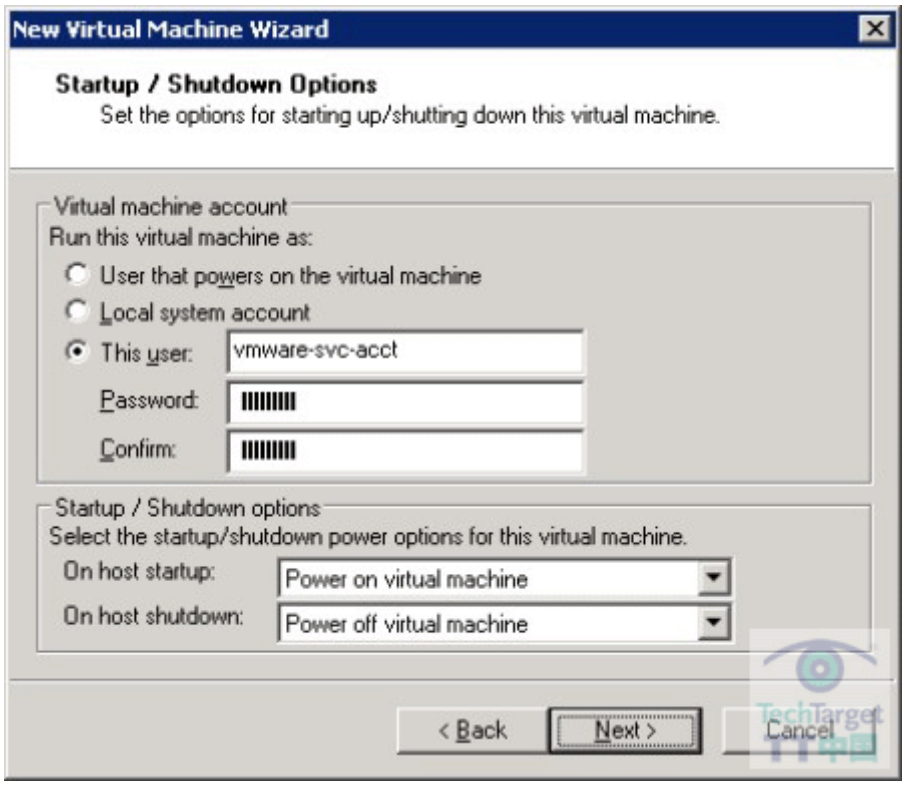


选择所创建虚拟机将要运行的子机操作系统并选择它的版本。在这种情况下，需要选择的是 Microsoft Windows Server 2003 标准版。点击“下一步”

为此虚拟机选一个名称。这将被自动填到虚拟机的地址栏中。点击“下一步”



取消勾选"Make this virtual machine private"。这样的话，获得该虚拟机的文件许可才可以访问该虚拟机。点击“下一步”



这一步非常的重要，因为它将会影响到在这台服务器上运行的每台虚拟机的安全性，乃至可能是整个计算机构架的安全性。

就像是在第二节中提及到的一样，VMware Server 以其特有的过程启动每台虚拟机。这种屏幕给我们提供了一个机会，可以配置运行该过程的用户帐户。默认情况下，一台虚拟机将会由启动它的那个用户来使用。这实际上非常的不安全。

假设此服务器是某 AD（活动目录）的成员之一。由于此服务器上的文件系统都已经被设置成允许该服务器的管理员访问虚拟机，除非此默认设置在其他地方被修改过。这意味着该活动目录“域管理员”群组内的任何成员都可以通过 VMware Server 控制台访问此服务器上的虚拟机。

如果一个域管理员启用某台虚拟机，这台虚拟机就将在该域管理员的安全监控下运行。目前，还没有已知的办法可以侵入一台正在 VMware Server 上运行的虚拟机。然而，我们猜想有这样的方法。（黑客不是愚蠢的，当他们显身的时候就是他们已经找到新的攻击载体的时候）。

以下情况可以很容易发生，如果某台虚拟机是被一个特权用户使用，黑客就可以摧毁整个活动目录。举个例子，域管理员"l.carroll"进入 VMware Server，启动名为

"jabberwocky"的虚拟机。虚拟机此时由"vmware-vmx.exe"进程支持运行，而且这个进程在域管理员"l.carroll"的安全监控下运行。在启动虚拟机之后，域管理员"l.carroll"就断开了与 VMware Server 的连接。而几个小时后虚拟机"jabberwocky"被黑客袭击了，因为作为一台服务器来说，这样的 IIS 设置明显不够（系统管理员本应该遵循这个指南）。

这不仅仅是危害虚拟机的任何黑客，也同样是发明了在虚拟机外面和主机服务器操作系统里面一直跟踪白兔的方法的黑客，。从这点来讲，改变活动目录里所有的密码并重建服务器的所有密码是完全有必要的。

当黑客突破防御通向另一方时，却发现另一方正在域管理员"l.carroll"的安全性监控之下。这就意味着黑客像域管理员一样运行代码，尝试访问系统。

通过这些情景，我们可以看到为什么说谨慎地选择启动虚拟机的帐户是那么的重要。

如果该服务器不属于某个活动目录，也可以选择使用本地系统帐户作为虚拟机帐户来使用。虽然说如果虚拟机被黑客袭击，活动目录并不会受到损害，但主机服务器乃至在主机服务器上运行的其它虚拟机都会有所损害。

安全性最高的方法就是创建一个低特权服务帐户，并将其作为虚拟机帐户来使用。此帐户唯一应该拥有的额外特权就是对文件夹"e:\var\vms"的完全控制。除此之外，普通用户特权就足够了。

另外，如果服务器是某活动目录内的一员，一个单一的低特权域用户帐户也可以让用来在所有 VMware Server 主机上运行虚拟机。

而对于一些十足的偏执人士来说，他们应该使用一个单独的低特权用户帐户来运行每一个单独的虚拟机。当然，所有的帐户也都应该有单独的、长一些的密码。这样，如果只是一个帐户被危及安全，其它所有的帐户应该不会有太大危险。

在点击“下一步”之前，请决定当服务器启动时这台虚拟机是否要随之启动。请适当地调整设置后然后点击“下一步”。

即使选择两个虚拟处理器同时运行很诱人，想想看：Windows Server 2003 无法支持处理器的删除。尽管说 Windows Server 2000 可以进行这样的操作，可不论什么原因，Windows Server 2003 就是不能支持。所以，虽然说稍后给虚拟机添加资源(现在这种情况是指 CPU)是小事一桩，可如果这个添加的 CPU 没有被使用的话，我们是不可能将其移去的。

因此，请选择"One"然后点击“下一步”。

尽管如今的大多数服务器最小也载有 1G 的内存，对于 Windows Server 2003 来说 384M 内存就足够了。为了安全起见，选择 512M。如果之后服务器需要更大的随机存储空间，我们可以通过给它多分配随机存储空间来满足其不稳定的欲望。点击“下一步”。

除非该虚拟机需要在专用网络或 NATD（网络地址转换实现形式之一）网络，否则的话请选择"使用桥接网络"。本指南将不会论述所有 VMware Server 上各种不同类型的网络设置，但是在不久的将来会提供一个关于高级网络和 VMware Server 的指南。

点击“下一步”

BusLogic 适配器是支持遗留系统处理的。选择"LSI Logic"，然后点击“下一步”。

选择"创建新的虚拟磁盘"，然后点击“下一步”。之后选择"SCSI"（小型计算机系统接口）并点击“下一步”。

Windows Server 2003 最好在 6G 空间内安装，所以对于磁盘大小，请选择“6”。

现在有问题产生了，我们是否为虚拟硬盘图像预先分配了空间呢？如果服务器上有 6G 的自由存储空间，那么一定要预先分配空间。这将有利于提升虚拟机的性能。预先分配存储空间也就意味着硬盘在今后将不能被压缩或者进行碎片整理。这些一定要记住。

选中相应选项旁边的复选框将磁盘分成 2G 的文件也是一个好主意。将来如果有必要将虚拟机的磁盘文件刻录成 DVD 或是在网络中转移文件的话，这个设置将使其变得容易些。在移动或者复制小量数据时，错误将很少有机会发生。

点击“下一步”。

给这个磁盘文件起一个容易记住的名字，比如说"%HOSTNAME%-system.vmdk"，然后点击“下一步”。

祝贺您，虚拟机创建完毕！在本系列的下一部分中，我们将讨论如何安装客户操作系统。

(作者：Andrew Kutz 译者：王霆 来源：TT 中国)

在 Windows Server 2003 上为 VMware 安装客户操作系统

任何一台机器都需要一个操作系统，无论是虚拟机还是其它机器。幸运的是，安装操作系统是 VMware Server 起步阶段里最简单的一步。

在我们关于 VMware Server 起步阶段的系列文章的最后一部分，TechTarget 中国的特约专家 Andrew Kutz 将论述如何安装客户操作系统，也会得出一些关于整个安装过程的结论。之前，我们讨论了在 Windows 上安装 VMware Server 的整个过程，包括对于其组件的研究、Windows 的安装及其配置、安全性调整，和 VMware Server 的安装及其安全性调整。

客户操作系统的安装

这是所有步骤里边最简单的一步。考虑到这篇文章的写作意图，即将被安装的客户操作系统是 Windows Server 2003 标准版。

安装客户操作系统的第一步是将 Windows 2003 Server 标准版 CD 安装盘插入服务器的光驱里。

如果此操作系统会在虚拟机上频繁安装的话，那么就有必要给 CD 安装盘创建一个 ISO 图标。对 Windows 来说，有一个很不错的、名为"dd"的免费程序可以用来创建 ISO 图标。

在 VMware Server 使用 ISO 图标也非常简单。应该在 VMware Server 控制台上选中刚刚被创建的虚拟机。如果没有选的话，现在选中它。点击“VM”菜单选项，再点击"设置"。

一个新的名为"虚拟机设置"的窗口将和一个左侧列有虚拟机设备的菜单一起出现。选择设备"CD-ROM (IDE 1:0)"。右侧会出现一个标记着"使用 ISO 图标"的选项。选中这个选项，然后浏览所有使用 ISO 图标所必须的。虚拟机就会像对待已经插入服务器光驱里的 CD 盘那样对待它。

一旦 CD 安装盘已插入或 ISO 图标已被展开，就该是时候启动虚拟机了。虚拟机启动的那一刻，光驱是开机命令中唯一的设备，所以虚拟机上出现的任何与开机有关的 CD 或 ISO 图标都会被启动。其后每当虚拟机被启动时，光驱将不会出现在开机命令中（默认情况下），并且还需要从 CD 或 ISO 图标进行人工干预。在这里记一点笔记可能会避免将来的一些失败出现。

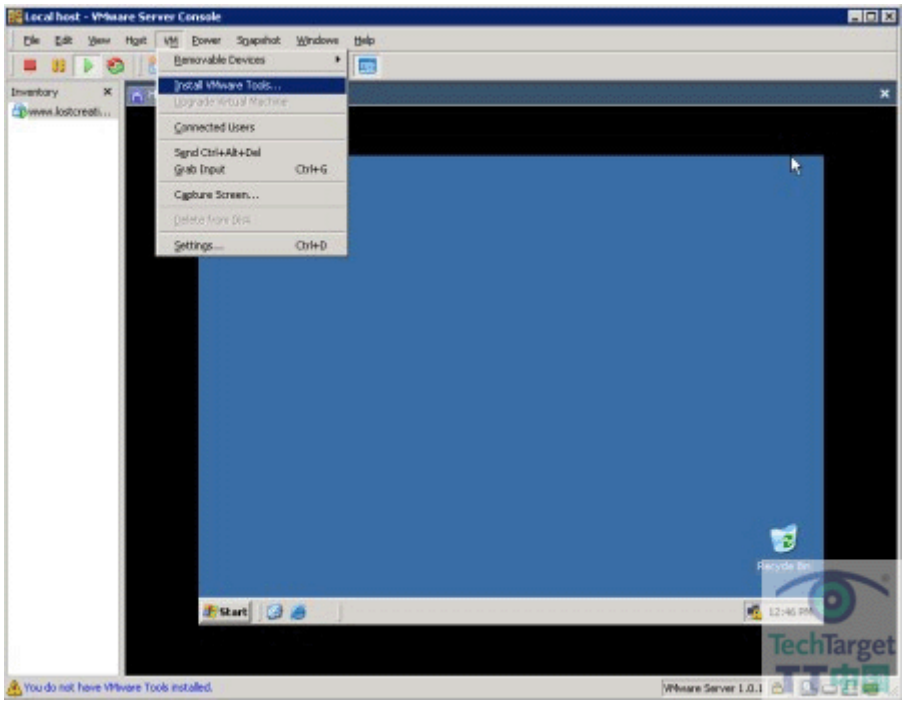
安装

CD 被导入以后，像平常一样继续安装 Windows。

VMware工具

安装完 Windows 以后，还要安装 VMware 工具。VMware 工具由一些能与 VMware Server 交互的特殊驱动器组成。

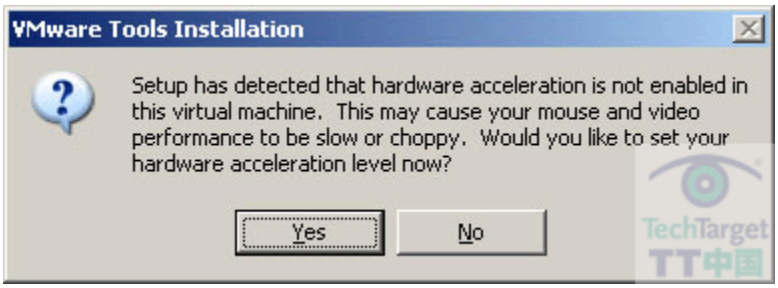
具体而言，VMware 工具将允许虚拟机有更好的屏幕分辨率和颜色深度、更快（千兆）的网络连接，以及更为智能化的内存管理。VMware 工具还提供了一些其它功能，想要全部阅读，请参看 VMware Server 虚拟机指南从 39 页开始对 VMware 工具的描述。



要安装 VMware 工具，先点击“VM”菜单选项，然后点击"安装 VMware 工具"。这时将会出现一个类似于下图的窗口。

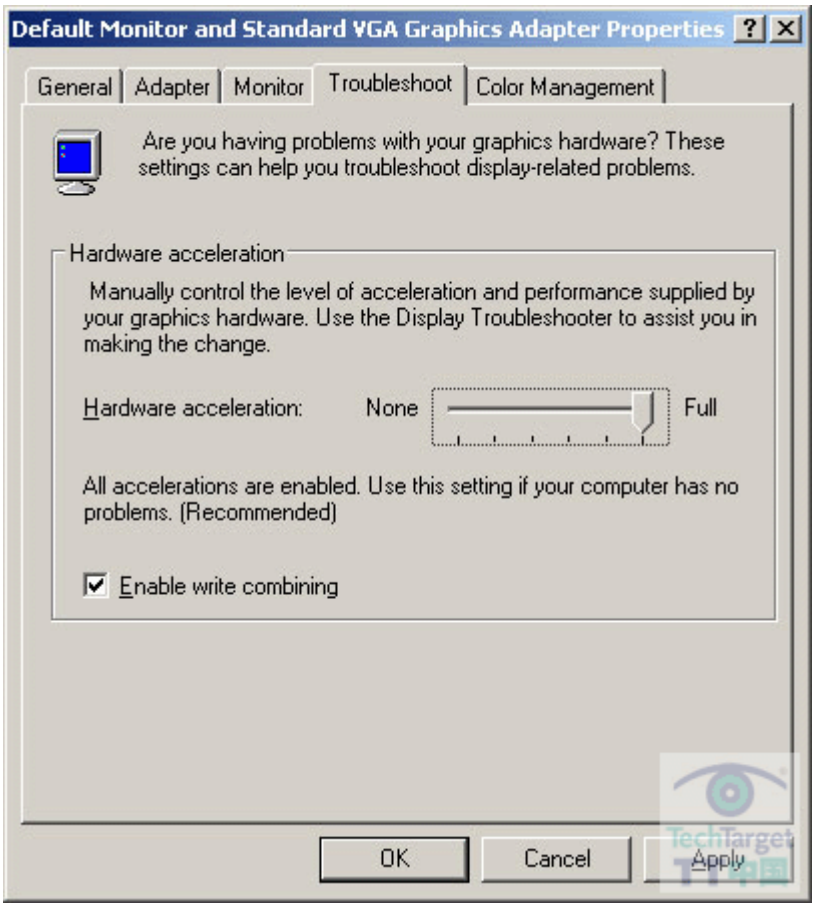
点击"安装"，从而使 VMware Tools ISO 图标能够像虚拟机里的 CD 一样被导入。剩余的安装程序将在虚拟机内部完成。此种安装方法非常易懂。看到提示后选择"完成"安装。

有些时候可能会弹出以下窗口：



既然 VMware 工具 SVGA 视频驱动已被安装，Windows 希望激活其硬件加速器。点击"Yes"按钮。

此时将会出现显示属性窗口。点击标记为"Troubleshoot"（调试）的标签，一直拖动"Hardware acceleration"（硬件加速器）滑块到提示"Full"。



点击"OK."。继续往下在 VMware Tools 安装窗口点击"Finish"按钮。重启机器，VMware Tools 安装完成。

安装技巧

这些技巧可以帮助安装程序运行得更流畅。

光驱检测

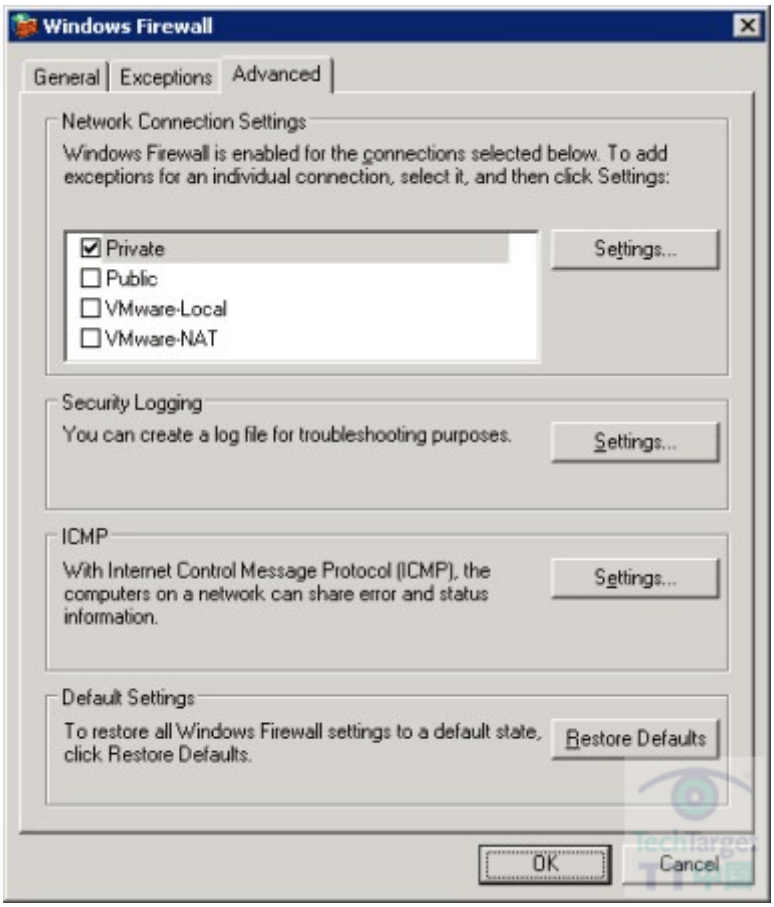
提升 Windows 客户性能的方法之一是关闭光驱检测。Windows 每隔几秒钟会检测光驱设备，检查是否有新 CD 的出现。当新 CD 被插入时会使主机操作系统暂停，也会导致其它设备反应缓慢。我们可以从微软官方网站上下载 TweakUI（Windows 系统增强工具）程序来关闭光驱检测。

客户操作系统指南

VMware 有一个相当不错的客户操作系统安装指南可用。关于 Microsoft Windows 2003 Server 的这章从 31 页开始。

防火墙

如果服务器配置了专门的管理接口，那么服务器的防火墙可能将无法用于其它所有接口，因为那些接口仅被用于 proxy VM 传输。打开 Windows 防火墙属性，点击"Advanced"选项。



勾掉所有没有被定制为专用管理接口的网络连接旁边的复选框。目前为止所有的网络接口中只有防火墙是专用网络接口，保持其它接口打开的状态，从而为通向虚拟机的数据传输提供充分自由。

现在可以安全地将以太网电缆插回服务器的网络接口端口了。

获得VMware Serve控制台

需要连接到 VMware Server 来管理虚拟机的用户可以从 https://%HOSTNAME%:8333/MUI（Windows 多语种版）下载 VMware Server 控制台。那里将会有一个包含有 Windows 和 Linux 版本 VMware Server 控制台的下拉列表。

组策略

如果此服务器是某活动目录的成员之一，那么许多本指南中应用到的设置就会被自动定制到组策略。这些设这包括安全性设置、时间日志文件定位、防火墙策略、Windows更新策略以及更多。

结论

本系列文章的目的是给系统管理员们创建一个安全的 VMware Server 提供一个向导或指南。

（作者：Andrew Kutz 译者：王霆 来源：TT 中国）