
# 保护 VMware 环境安全

# 保护 VMware 环境安全

VMware 安全非常关键，因为 VMware 是优秀的服务器虚拟化平台。在 TechTarget 的 2009 年虚拟化采购意向调查中，72.4%的受访者使用的是 VMware 作为他们的服务器虚拟化基础。

选择虚拟化市场领导者带来好处的同时（例如丰富的第三方产品和信息资源），也面临着风险。例如，VMware 有大量安装基础，这样的环境成了黑客的首要目标。因此，VMware 代码任何漏洞被发现的话，就很容易受到攻击。

不用担心！有许多方法可以消除 VMware 安全隐患和禁止访问 VMware 环境。在本手册中，我们将提供 VMware 安全工具、第三方产品和 VMware 安全实践的信息。

## 网络与驱动安全

在各种融合网络环境下运行 VMware 容易导致数据混合，如果有错误的数据混合进来就会出现问题。该如何防止呢？如何控制驱动的相互作用以及如何远离 VMware 后门程序引起的安全风险？

- 如何在 VMware 虚拟融合网络中防止安全漏洞？
- 如何预防 VMware 虚拟机错误和安全漏洞？
- 如何预防由 VMware 驱动和后门程序导致的系统故障（上）
- 如何预防由 VMware 驱动和后门程序导致的系统故障（下）

## ESX 和 ESXi 安全

如果用户在隔离区（DMZ）内配置 VMware ESX 或者 VMware ESXi 宿主虚拟机的话，需要格外注意网络问题。什么是 Tripwire ConfigCheck？如何使用 Tripwire ConfigCheck 审计 VMware ESX 的安全性？

- 如何防止在隔离区出现 VMware ESX 和 ESXi 网络安全漏洞？
- 使用 TripWire ConfigCheck 评估 VMware ESX 服务器安全

## 安全工具 vShield Zones

vShield Zones 是 VMware 的安全产品，有了 VMware 的 vShield Zones，你可以监控虚拟环境里的网络流量，并通过在网络上细分用户和敏感数据以确保法规遵从。本系列文章详细介绍 vShield Zones 工作原理、安装、配置与管理信息。

- VMware vShield Zones 如何有助于虚拟机安全监控？
- 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）

## 更多 VMware 环境安全资源

ESX 是性能比较稳定的虚拟化产品，但是也存在一些安全漏洞。ESXi 是 VMware 免费嵌入式 hypervisor，它也存在安全缺陷。对于这两款产品，我们该如何安全地管理它们？本指南将从网络和管理方面入手，提供一些实用技巧。

- ESX 与 ESXi 安全管理

# 如何在 VMware 虚拟融合网络中防止安全漏洞？

在各种融合网络环境下运行 VMware 容易导致数据混合，尽管从直观上看这种混合并没有坏处，但是如果有错误的数据混合进来的话，就会出现问题了。之所以出现融合网络是因为并不是很多人都完全利用 10Gb 以太网网络带宽，甚至很多人都没有充分利用 1Gb 的以太网连接。融合网络的目的就是让网络的其他方面充分利用未使用的带宽，这是由于缺少网卡（NIC，即 Network Interface Card），部署新的电缆不太可能，并且时间成本和资金成本也比较高。

最简单的解决方案就是在同一条光缆上不仅仅传输一类数据信息，这就是所谓的数据混合。只要所有的数据具有同样的安全等级和安全区域，在数据混合中就没有必要考虑安全问题。然而，如果同一条线路上传输的数据不属于相同的安全等级或者安全区域的话，数据融合就会成为一个比较令人头疼的问题。

安全等级定义不同主体可以访问同一传输线路上的不同数据，而安全区域指的是传输线路所连接的区域，也可能包括对其如何使用。例如，与称为生产的安全区域相比，一个 DMZ（隔离区）很有可能是一个敌对环境。两个区域的数据融合将会提高系统正常风险级别，正常风险级别是指在一个融合网络中没有数据混合的情况下的风险级别。

对每一台 VMware ESX 主机来讲，使用虚拟化的话，至少有四种可能的网络：服务控制台或者管理设备、存储网络、VMware VMotion 或 Storage VMtion 网络和虚拟机网络。另外至少有四个不同的安全区域：管理程序（Hypervisor）、虚拟机、存储和管理。

**如何合理地融合网络和安全区域？**

选择要融合网络和安全区域取决于很多方面，但是为了简化问题，我们这里忽略硬件限制。沿着当前的思路往下走：为什么各种各样的安全区域和网络需要保持隔离？这并不表示我不喜欢虚拟局域网（VLAN），但是 VLAN 确实不能保证安全性。VLAN 是一个网络中（物理的或者虚拟的）确保一个数据包传送到合适端点的工具，但并不是一种保护网络的方法。

最近在 VMware 社区，“Secured with VLANs”这个词谈论得非常热。RFC（Request for Comment）802.1q 中并没有提及到安全问题。VLAN 并不保证安全性，但是可以被安全地使用。然而，为了确保安全地使用融合网络，有一些问题还是需要注意的：

- 直接（vmkernel 虚拟网卡）或者间接地（管理设备与应用）通过网络连接对 Hypervisor 的任何访问都必须受到严格的控制。因为取得对 Hypervisor 的访问控制权限就会带来对 VMware ESX 主机或 VMware ESXi 主机内任何信息取得访问控制权限的风险。

- 对 VMotion 网络的任何访问也会带来风险：由于正在使用的内存信息以明文方式在线路上传输，虚拟机内的证书和身份数据很容易暴露。
- 通过一台虚拟机、备份服务器，或者是间接地通过 Hypervisor 和管理工具对存储网络的访问控制必须受到严格的控制。由于可以对存储网络信息以明文的方式访问，对虚拟存储网络的访问可能会带来暴露虚拟机内虚拟硬盘上内容的风险。

**最好的实现方式**

鉴于所有的上述信息，对于使用融合网络的虚拟网最好的建议是什么呢？理想的情况就是不融合 VMware ESX 主机和 VMware ESXi 主机内的任何网络，但是这个似乎有点不太现实。用户可以选择不融合从 VMware ESX 主机和 VMware ESXi 主机到物理网关的网络，但是如果这样的话，虚拟网就会形成集群来穿越整个公司交换结构中的其它物理网关。

交换结构中的薄弱环节实际上可能是物理网络，因为虚拟网关可以防止当前来自 VLAN 第二层攻击，尽管攻击不是来自第三层。不过也不是所有的物理网关都可以阻止来自第二层 VLAN 的攻击。

人们通常混合来自同一条线路上 VMware ESX 主机和 VMware ESXi 主机管理设备的数据和 VMotion 的数据，因为他们认为这两者应该是和其它任何网络一样具有同样的风险程度。VMotion 是具有最高风险的网络，然而如果有恶意用户可以攻破 VMware ESX 主机和 VMware ESXi 主机管理设备的话，就可以获得对所有磁盘数据的访问控制权限，然而未必是 VMotion 数据。但是如果这两者在通一条线路上传输的话，风险就比较高了。

其它经常混合的数据是存储数据和虚拟机数据。换句话说，虚拟机可以和 ESX 主机访问到同样的存储空间。如果虚拟机不是一个存储管理节点或者形式的管理节点，也可能导致虚拟环境中安全漏洞出现的高风险性。

当前没有减轻这个问题的好方法。VMware ESX 和 VMware ESXi 现在都不支持 IPsec（Internet Protocol Security）。IPsec 使用预置共享密钥和一个很好的公钥密码体系可以对融合网络上的所有数据完成强加密，加密过程基于不同数据来源使用不同的密钥体系。这个方法可以在很大程度上降低整体风险性。

选择融合何种网络需要对要传输的数据有一个很详尽的了解，如这些数据传送的目的地、传送方式、加密的可能性以及数据传输错误带来的风险等。

*（作者：Edward L. Haletky 译者：王越 来源：TechTarget 中国）*

原文标题：如何在 VMware 虚拟融合网络中防止安全漏洞？

原文链接：http://www.searchvirtual.com.cn/showcontent_26136.htm

## 如何预防 VMware 虚拟机错误和安全漏洞？

仅仅是由于你确保了运行在 VMware ESX 或 VMware ESXi hypervisor 上的操作系统的安全，这并不意味着你的虚拟机就不会出现错误和漏洞。VMware 管理员也需要考虑到虚拟机和 hypervisor 受到影响的更多抽象的虚拟化“层”。

在本文中，TechTarget 中国的特约作者 Edward L. Haletky 将讨论由准虚拟化驱动、普通驱动和 VMware 用于执行命令的工具所组成的虚拟化层。无论哪里有一个相互作用层，黑客都将开发和研究安全漏洞。我们将在本文中学习如何控制驱动的相互作用以及如何远离 VMware 后门程序引起的安全风险。

### hypervisor 和虚拟机之间的相互作用

尽管准虚拟化驱动、一般驱动和 VMware Tools 有各种不同的威胁，每个实体都应该减少发生安全漏洞的机率。

准虚拟化驱动：准虚拟化驱动知道它们运行在虚拟机里，也使用带外通信设备（可能是通过 VMware 后门程序、专用于 VMware 虚拟机的一个 I/O 端口），或者利用设备使用的虚拟化主机在用的具体代码。例如在 VMware 子机里，vmxnet 驱动是准虚拟化的。这样的驱动能获取性能优势。VMware 建议的虚拟机接口（VMI）使为 Linux 写入准虚拟化驱动更容易更透明。

不过同时，错误写入的准虚拟化驱动能导致崩溃，试图避开 hypervisor 里的虚拟机。虽然目前不可能发生，最好在使用准虚拟化驱动之前先诊断它们。大体上只使用来自已知资源（如 VMware）的准虚拟化驱动。

普通驱动。普通驱动不知道它们运行在 hypervisor 上，通常需要 hypervisor 翻译到正在使用的下层硬件。这些驱动只与子操作系统内核交互作用，然后子操作系统内核通过普通方法与 hypervisor 作用。一些情况下，hypervisor 不知道由驱动发送或发送到驱动的命令，并将在 per-VM vmware.log 里显示错误。虚拟机可能发现不到这个问题。在其他情况下能导致虚拟机崩溃。例如，VMware 的 hypervisor——vmkernel 不执行每个 SCSI 指令或可用的命令。一些秘密命令能导致错误，并显示在 vmware.log 文件里。

VMware 后门程序。VMware 后门程序能泄露版本数据，从而引起其他攻击。后门程序给了一个到 hypervisor 的备用路径，用于提供虚拟机与 hypervisor 之间的带外通信。VMware 后门程序主要用在 VMware Tools。不过如果你在虚拟机里创建了一些简单的设置，就能保护这个程序。

任何用户使用都能使用 VMware Tools，因此用户能发送许多通过 VMware 后门程序运行的 VMware Tools 命令。一般用户不需要访问 VMware Tools 以执行命令，因为 VMware

Tools 访问在子机中应该受到管理员的限制。不幸的是，任何人都能使用 VMware 后门程序，并且现在不能从所有子操作系统中关闭它们。

### 确保 VMware 后门程序的安全

确保 VMware 后门程序安全的主要方式是禁用 VMware 的高级配置设置功能。目前的每个安全标准都建议设置所有不同独立选项的子集。下面是关于如何更改虚拟机的设置，能在 Advanced Options（或者直接添加到每台虚拟机的.vmx 文件里）下找到。

#### ESX 的 DISA STIG

- 禁止从虚拟机的远程控制台复制到 workstation：isolation.tools.copy.enable => false
- 禁止从 workstation 粘贴到远程虚拟机控制台：isolation.tools.paste.enable => false
- 禁止更改屏幕分辨率和深度：isolation.tools.setguioptions.enable => false

#### CISecurity ESX Benchmark

- 禁止从虚拟机的远程控制台复制到 workstation：isolation.tools.copy.enable => false
- 禁止从 workstation 粘贴到远程虚拟机控制台：isolation.tools.paste.enable => false
- 禁止更改屏幕分辨率和深度：isolation.tools.setguioptions.enable => false
- 禁止 VMware Tools 作出配置更改的能力：isolation.tools.setinfo.disable => true

#### VMware VI3.5 指导

- 在虚拟机到 vmware.log 的过程中禁用登录的一些选项。这能最大程度上减少登录，不过不能完全移除它。这有助于解决磁盘 I/O 问题。
  isolation.tools.log.disable => true
- 在每个指定字节检查 vmware.log，否则 vmware.log 文件增长得很大。
  log.rotatesize => 100000
- 只保持 vmware.log 文件的具体数量，不然会保存无穷大的数量，这会占用大量磁盘空间。在 VMFS 上，能迅速达到 32K 的极限。log.keepold => 10
- 限制发送到 VMware Back 后门的数据量。tools.setinfo.sizeLimit => 1048576
- 禁用从穿过 VMware 后门程序的虚拟机里设置一些信息的功能。
  isolation.tools.setInfo.disable => true
- 禁用通过虚拟硬件能连接或断开（软盘、CD-ROM 和网络等）这些方面的 VMware 后门程序为虚拟机设置连接状态的功能。

isolation.tools.connectable.disable => true
isolation.tools.diskshrink.disable => true

- 禁用虚拟机通过 VMware 后门程序调用 diskwiper routines 的功能。
  isolation.tools.diskwiper.disable => true

**预防措施**

取决于安全需求，所有这些选项都应该设置，因为它们确保了子机与 VMware 远程控制台主机之间交互的安全，也确保了子机与虚拟机、hypervisor 和文件系统的交互安全。这些设置都能预防由于缺少空间而导致的 hypervisor 错误。

保护 VMware 的后门程序非常重要，因为我在这里着重强调。最好适当地限制对工具而不是驱动的访问。同样，诸如对子机操作系统里的 WindowUser Access Control (UAC) 和 SELinux 执行强制性访问控制，这样来限制对 VMware 后门程序的访问。

虚拟机的安全主要在于子机操作系统里，不过虚拟硬件的设置同样也不同。经常参照当前的指南、基准和一缆表帮助适当地保护虚拟机。

*(作者：Edward L. Haletky 译者：唐琼瑶 来源：TechTarget 中国)*

原文标题：如何预防 VMware 虚拟机错误和安全漏洞？

原文链接：http://www.searchvirtual.com.cn/showcontent_26301.htm

# 预防由 VMware 驱动和后门程序导致的系统故障（上）

尽管有大量的受访信息显示，运行 VMware ESX 和 ESXi 的操作系统是非常安全的；仍不排除一些由于 VMware 管理程序（hypervisor）和子操作系统之前的交互机制所带来的安全隐患。这种交互通常由三种渠道实现：半虚拟化驱动程序、常规驱动程序和 VMware 工具。这样，当系统管理员希望构建一个安全的 VMware 环境时，有两个部分需要关注：

**第一部分是管理程序（hypervisor）和虚拟机（VM）之间的交互**。虚拟化层通过组成 VMware 工具的半虚拟化驱动延伸到子操作系统（guest OS）之中，对于之前不太关注这部分内容的人，这是一个全新的命题；**第二部分就是子操作系统本身**。每个子操作系统都有需要遵循的安全加固脚本、向导和基准。然而这些脚本、向导和基准事实上都无法完全取代虚拟化层和子操作系统之间的交互，所以一般来讲第一个部分会直接影响到第二个部分。总之，您可以参考下面的这些设置，来确保 VMware 管理程序和建立在它之上的虚拟机之间的交互更加安全：

### 加固子操作系统

本篇本章文将不会对子操作系统的加固问题展开讨论，如果您需要对子操作系统做加固，如下这些链接的相关内容将对您有所帮助

- Repository of Defense Information Systems Agency (DISA) Security Technical Information Guides (STIGS)
- CISecurity benchmarks
- Bastille-Linux

请在您的虚拟机环境中遵循其中的一项或者所有的基准和向导。同时谨记 vSwitch 并不包含内置的防火墙，所以一旦子操作系统接入网络环境，它就需要加强自身的防护工作。

### 管理程序和虚拟机之间的交互

管理程序和虚拟机之间的交互通过三种渠道：半虚拟化驱动、常规驱动和 VMware 后门程序。

半虚拟化驱动程序知晓自身运行于虚拟机中，通过带外通讯机制和硬件设备交互（也可能是通过 VMware 后门程序），或者利用虚拟主机使用的特殊的指令交互。例如，在 VMware 子系统中，vmxnet 驱动就是半虚拟化驱动程序。因为虚拟机界面（VMI）可以在 Linux 下几乎透明地写入半虚拟化驱动，所有它有很好的性能优势。如果写入半虚拟化程序的过程很困难，程序会试图避开虚拟机直接跟管理程序交互，这个过程可能会直接导致系统崩溃。因此，为了避免这种情况发生，最好的办法就是在使用半虚拟化程序之前确保

他们它们都是经过验证的。通常我们只使用那些来自已知来源（如：VMware）的半虚拟化驱动。

常规驱动程序并不知道自身运行于虚拟机管理程序之上，它和底层硬件之间的交互通常需要管理程序的转发。这些驱动程序仅仅和子操作系统内核之间交互，然后子操作系统内核通过普通方式和虚拟机管理程序之间交互。在某些情况下，管理程序可能并不能识别驱动所发出的（或者是发往驱动）指令。这种结果下，程序会返回错误值写入到每个虚拟机内部的 vmware.log 中，程序所需的功能将无法实现，这个过程多数时候对虚拟机的影响并不明显。有些时候，这种情形会直接导致虚拟机的崩溃。例如，VMware 的管理程序 vmkernel，并不能有效执行每个 SCSI 指令，一些特殊的指令将导致在 VMware.log 中写入错误日志。或在一些情况下，虚拟机会瘫痪。

**VMware 后门程序**

关于 VMware 的后门程序是一个让人困惑和，并被许多人诟病的问题。一般来说，通过一些虚拟机内部的简单设置就可以保护 VMware 后门程序安全。后门程序是一种旁路通讯方式，提供了管理程序和虚拟机之间的另外一条交互通路，通常情况下 VMware 后门程序是供给 VMware 工具来使用的。

VMware 工具可以在所有的用户权限下运行，因此每个用户都可以通过虚拟机后门程序运行一些 VMware 工具命令行。通常普通用户并不需要经常通过 VMware 工具来执行命令行指令，所以在 VMware ESX 环境中，VMware 工具应该被严格限制给系统管理员使用。不幸的是，VMware 后门程序是对所有用户开放的，并且不能在子操作系统内通过设置来关闭。

在本文的下半部分中，我们将继续介绍如何确保 VMware 后门程序的安全性。

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

原文标题：如何预防由 VMware 驱动和后门程序导致的系统故障（上）
原文链接：http://www.searchvirtual.com.cn/showcontent_26632.htm

# 预防由 VMware 驱动和后门程序导致的系统故障（下）

在本文的上半部分中，我们介绍了如何加固子操作系统以及 VMware 后门程序。现在我们来看看如何确保 VMware 后门程序的安全性。

## 确保 VMware 后门程序的安全性

通常用来保护 VMware 后门程序的方式是在 VMware 高级设置来配置更改一些选项。现在通用的安全标准都不建议使用最小化配置，而是通过建立一些不同配置的子集来管理。这里提供了一些设置方式，可以在 Advanced Options 下设置虚拟机配置来保证 VMware 后门程序更高的安全性（或直接添加到每个虚拟机的.vmx 文件中）：

DISA STIG for ESX

- 禁止从虚拟机的远程控制端向工作站拷贝：

```
isolation.tools.copy.enable => false
```

- 禁止从工作站向虚拟机远程控制端粘贴：

```
isolation.tools.paste.enable => false
```

- 禁止改变屏幕分辨率和色度：

```
isolation.tools.setguioptions.enable => false
```

CISecurity ESX Benchmark

- 禁止从虚拟机的远程控制端向工作站拷贝：

```
isolation.tools.copy.enable => false
```

- 禁止从工作站向虚拟机远程控制端粘贴：

```
isolation.tools.paste.enable => false
```

- 禁止改变屏幕分辨率和色度：

```
isolation.tools.setguioptions.enable => false
```

- 禁止 VMware 工具进行配置更改的功能：

```
isolation.tools.setinfo.disable => true
```

VMware VI3.5 加固指导

- 禁止某些情况下对 vmware.log 文件的访问登陆。在允许访问的情况下极大减少了访问量，可以减轻磁盘的 I/O 压力：

```
isolation.tools.log.disable => true
```

- 使 vmware.log 文件按照设定的字节循环滚动保存，避免 vmware.log 文件变得非常的庞大：

```
log.rotatesize => 100000
```

- 只保存设定数量的历史 vmware.log 文件，避免重复保存的该文件占用大量磁盘空间。在 VMFS 系统中，这个文件可以迅速达到 32K 的文件大小上限。

```
log.keepold => 10
```

- 限制可以发送给 VMware 后门程序的数据量：

```
tools.setinfo.sizeLimit => 1048576
```

- 禁止通过后门程序直接对虚拟机内部的一些配置信息做修改：

```
isolation.tools.setInfo.disable => true
```

- 禁止虚拟机通过 VMware 后门程序直接设置虚拟机硬件设备（软驱、光驱、网卡等）的连接状态（断开或连接）：

```
isolation.tools.connectable.disable => true
isolation.tools.diskshrink.disable => true
```

- 禁止虚拟机通过 VMware 后门程序直接调用 diskwiper 功能：

```
isolation.tools.diskwiper.disable => true
```

根据安全需求的不同，所有的选项可以被设置用来保证子系统和 VMware 远程控制主机之间以及在虚拟机、管理程序及文件系统之间交互的安全。这些设置可以防止一些非常有趣的（有时是让人迷茫的）由于缺少空间导致的管理程序故障。

对 VMware 后门程序的保护是非常重要的，必须强调的一点是最好适当限制使用 VMware 工具，而不是对驱动的访问。或者，执行集成在子操作系统内部的，像 Window UAC（User Access Control）或 SElinux 这样的强制访问控制工具也是一样的效果。通过这些来限制什么时候可以访问 VMware 的后门程序。

虚拟机安全最主要的部分是在子操作系统之内，但是虚拟硬件设置也会起到作用。尝试去掌握和练习那些用于加固虚拟机的指导方针、基准和检查清单，帮助您更加合理地保护您的虚拟机。

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

原文标题：如何预防由 VMware 驱动和后门程序导致的系统故障（下）

原文链接：http://www.searchvirtual.com.cn/showcontent_26633.htm

# 防止在隔离区出现 VMware ESX 和 ESXi 网络安全漏洞

如果用户在隔离区（DMZ：Demilitarized Zone）内配置 VMware ESX 或者 VMware ESXi 宿主虚拟机的话，需要格外注意网络问题。VMware 网络包括 VMotion 和存储 VMotion 网络、虚拟机网络、存储网络以及管理控制台所必需的网络。如果网络问题不能很好地处理的话，这些网络就会绕过现有的保护措施，而这些保护措施通常情况下用来阻止隔离区与外部通信。

在隔离区内部署 VMware ESX 和 VMware ESXi 的一个关键问题就是要意识到这是一个混合网络和混合计算资源，而不是一个单一操作系统或者应用设备。相应的，同时也应该评估一下在隔离区内是否应该有一台虚拟机。

很多安全管理员不允许在隔离区内实现多宿主系统，多宿主系统就意味着一个系统同时可以和很多网络建立连接。多宿主系统中，令人担心的问题就是这些系统会不自觉地成为安全区域和外部预定义的防火墙、路由器和网关通信的桥梁，其中这些防火墙、路由器、网关是安全部门早期建立的。

使用 VMware ESX 或者 VMware ESXi 的话，情况就不会是这个样子。在 Hypervisor 内部的 Layer 2 虚拟网关使用起来同 Layer 2 物理网关一样简单。鉴于这些虚拟网关的存在并且这些虚拟网关不能相互通信（除非是和不同的物理网关），所以存在一些系统可以为此建立连接。VMware ESX 或者 VMware ESXi 不会作为这样一个桥梁，但是却可以维持虚拟网关作为其自身的一个实体。虚拟机被连接到虚拟网关的 portgroups 上，这个虚拟网关作为一个 VLAN，其实并不必需。虚拟网关之间不能直接通信，不同 portgroups 的虚拟机也不可以直接通信。除非是 ID 为 4095 的 VLAN portgroups 内的虚拟网关，这是因为 ID 为 4095 的 VLAN 是供安全软件和控制 VLAN 的虚拟机使用的。

对于每一个 VMware ESX 主机来讲有四个可能网络：服务控制台或者管理设备、存储网络、VMware VMotion 或者存储 VMotion 网络和虚拟机网络。前三个网络是关键性网络，不能部署在隔离区内。最后一个网络是唯一个可以部署在隔离区内的网络。

很多人都认为最好的实现方式就是不要把前三个网络部署在隔离区内，但是却没有合适的理由。以下是我的理由：但都是基于这样一个假设，在持续威胁和可能性攻击情况下，隔离区可以会成为一个恶意网络环境。它一旦被攻破，就会成为对保护的网络进一步攻击的枢纽。

### 服务控制台

服务控制台或者管理设备是虚拟网关上的 portgroups 的门户，并且部署在它们自身虚拟网关上的 portgroups 内。所有的管理性的工作都在这个网络上完成，所谓管理性的工作通常包括登录每一个系统的认证信息。这个网络一般通过 SSL 得到保护，访问这个网

络可以给予攻击者从最基本的层次渗透到虚拟环境中的可能性，悄无声息地窃取数据的机会也会有很大增长（所谓的数据，我这里是指虚拟磁盘文件及其内容）。进一步来讲，这也就提供一个直接攻击 VMware ESX 主机和 VMware ESXi 主机上账户的机会，也就等于是给了攻击者访问所有信息的权限。

**存储网络**

存储网络是另外一个经常部署在其自身虚拟网关内部的重要网络。当前所有负责存储的协议在物理线路上都以不加密形式传送数据。攻击者获得访问这个网络的权限就可以访问虚拟磁盘数据。进一步来讲，如果使用的是 iSCSI，就会有另外一种攻击服务控制台或者管理设备的可能，这是因为服务控制台或者管理设备也参与 iSCSI 网络。

**VMotion 和存储 VMotion 网络**

VMware VMotion 和 Storage VMotion 网络通常情况下在其自身的虚拟网关上，一般以明文方式在物理线路上传送虚拟机的内容和磁盘信息。由于攻击者可以获得虚拟机内存和磁盘内容的信息，所以这个网络是不安全位置中最危险的一处。通过这些信息，攻击者可以得到访问认证信息的权限。通过收集到的认证信息，这个网络也就成了攻击用户网络的枢纽。

**虚拟机网络**

获得虚拟机网络访问控制权限不会带来获得其它三个网络访问控制权限同样的风险。

有必要进一步阅读 VMware 其它文档，因为我发现在一个隔离区内开始部署 VMware ESX 主机和 VMware ESXi 主机之前，阅读这些文档是相当重要的。列举部分如下：

- VMware whitepaper on virtual networking concepts
- VMware whitepaper on VMware ESX 802.1q VLAN solutions
- VMware whitepaper on iSCSI design and deployment
- VMware whitepaper on placing a VMware ESX host within a DMZ

*(作者：Edward L. Haletky 译者：王越 来源：TechTarget 中国)*

原文标题：如何防止在隔离区出现 VMware ESX 和 ESXi 网络安全漏洞？

原文链接：http://www.searchvirtual.com.cn/showcontent_26152.htm

# 使用 TripWire ConfigCheck 评估 VMware ESX 服务器安全

审计 VMware ESX 是一个好主意，尤其是如果你的架构受制于几个不同的法规标准。人工增强 VMware ESX 机器的安全性有许多最佳做法，不过由于是手动调节而容易忽视。甚至一名管理员从头开始建立了一台 ESX 机器，这台机器仍然会在 ConfigCheck 安全测试中的 77 检查点里有 45 个存在问题。TripWire ConfigCheck 是一个免费的应用，能帮助识别安全漏洞，并为修改安全漏洞提供使用说明。在本文中，TechTarget 中国的特约虚拟化专家 David Davis 将说明如何获得 ConfigCheck 以及怎样运行它。

## 为什么评估 VMware ESX 安全性？

由于网络和服务器，包括 VMware ESX Servers 受制于支付卡行业、SOX（萨班斯—奥克斯利法案）、健康保险可移植性和问责法的法律要求，因此一些组织需要确保 VMware ESX 机器的安全。另外一些组织只是想确保 ESX 主机的安全。

最小程度上，每个服务器和网络管理员应该想知道他们的服务器和网络从根本上说来是安全的。为了确保安全性，许多管理员从头配置服务器并自己安装操作系统。不过确保操作系统如设计的那样保护自己本身仍然是个好主意。

## 什么是 Tripwire ConfigCheck？

Tripwire 以其在配置更改时监控服务器或网络设备的审计和评估产品而闻名。随着虚拟化的流行，Tripwire 也通过添加 VMware 虚拟化审计产品进入虚拟化环境。它提供了两款产品，Tripwire ConfigCheck（我们将在本文中演示）和评估 VMware ESX 的 Tripwire Enterprise。

根据 Tripwire 的说法，ConfigCheck 能审计和评估 VMware ESX 主机，并以如何解决问题的说明书形式提供补救帮助。用于 VMware ESX 的 Tripwire Enterprise 能够评估和审计 ESX 的遵从性，能审计子操作系统，并提供报告、通知和对帐功能。

## 如何下载、安装和运行 Tripwire ConfigCheck？

要下载 Tripwire ConfigCheck，去到 ConfigCheck download 站点，填写一个简单的登记表。下载这个 10MB 的应用并解压。

ConfigCheck 是一个 Java 应用。这意味着安装 ConfigCheck 包括运行叫做 ConfigCheck 的 Windows 命令文件，即运行 Java Archive（JAR）文件。因此，安装的先决条件是 Java Runtime。在运行应用之前，将出现如下窗口。


点击放大

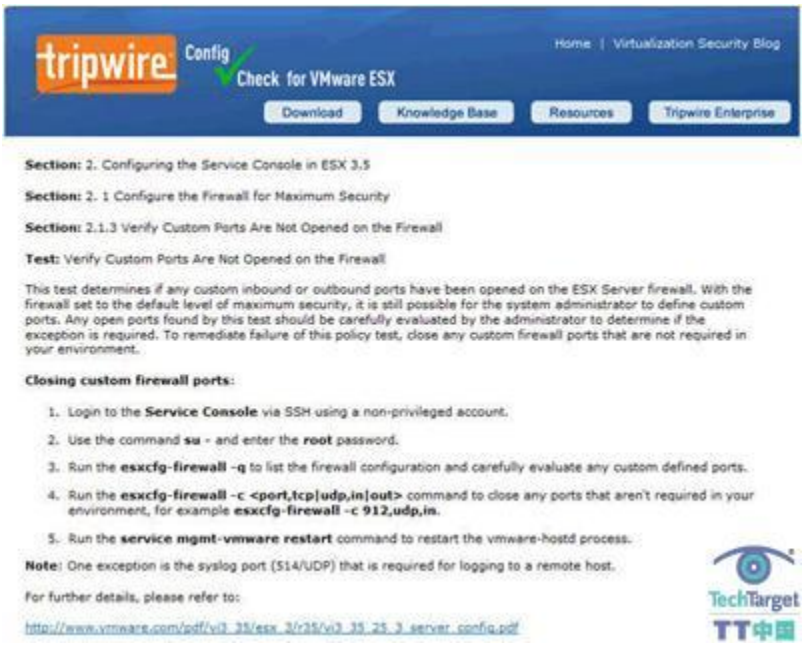
ConfigCheck 是一个简单的应用。上面的图就是 ConfigCheck 的样子。

要使用 ConfigCheck，输入 ESX 主机名、用户名、密码和根密码，并点击 Check Configuration。这个应用立即扫描 77 个潜在的安全漏洞，在 10 秒内完成。


点击放大

我在 VMware ESX 3.5 服务器上运行 Configcheck。这台服务器通过了 32 个检查点，失败了 45 个。所检查的名目基于 VMware 的 VMware Infrastructure 3 Security Hardening Guide。由于 ConfigCheck 的检查基于 VMware 的向导，可以采用来自 VMware 的官方安全最佳策略。

如果你点击每个失败的测试，将被带去一个 Tripwire 站点，提供了补救安全问题的说明。Tripwir 也提供一个完整的有 129 页的“虚拟化安全补救指南”。下图显示的是补救说明类型的一个例子。




点击放大

在补救说明书里有大量的非常好的安全技巧的步骤。例如，上面的说明建议管理员：

- 运行 esxcfg-firewall -q 以打开防火墙端口并评估自定义端口。
- 运行 esxcfg-firewall -c <port，tcp|udp，in|out>以关闭自定义端口。
- 然后运行 service mgmt-vmware restart 重新启动 vmware-hostd 过程。

当我收到上面的说明时我很惊讶，因为我以为有个默认的 ESX 安装。ConfigCheck 指出在 ESX 防火墙里有一些自定义端口。在想了想之后，我模糊地回忆起在几个月前我作测试时，为某个应用开启了一些自定义端口。

一台默认的 VMware ESX 服务器没有我以前所给的那样的安全。考虑到有 31 页的安全指南和 129 页的 Tripwire 安全补救手册，我的默认版本的 VMware ESX Server 在 77 个检查点里有 45 个有问题，这个事实是个警钟。

*(作者：David Davis 译者：唐琼瑶 来源：TechTarget 中国)*

原文标题：使用 TripWire ConfigCheck 评估 VMware ESX 服务器安全

原文链接：http://www.searchvirtual.com.cn/showcontent_26244.htm

# VMware vShield Zones 如何有助于虚拟机安全监控？

## 什么是 vShield Zones？

有了 VMware 的 vShield Zones，你可以监控虚拟环境里的网络流量，并通过在网络上细分用户和敏感数据以确保法规遵从。vShield Zones 是 VMware 的安全产品，其技术基于 VMware 在 2008 年 10 月收购的 Blue Lane Technologies。

如许多公司需要为其物理服务器创建隔离区（DMZ）一样，vShield Zones 允许为虚拟服务器创建安全区域。vShield Zones 的附加好处在于公司公司能收到大量的网络流量监控、分析和报道。

## vShield Zones 如何工作？

vShield 执行封包主动侦测检验技术（SPI），并追踪 FPT 这样的动态链接。更好的是，vShield 了解你的虚拟架构，并与 vCenter 追踪虚拟机与事件之间的流量，还有与 VMotion 相关的流量。

有了 vShield，你可以创建各种级别的管理员权限，并分配给网络层和 VMware 管理员。

通过使用单个虚拟机作为 vShield 管理站点，VShield Zones 就可以工作。vShield 开始监控虚拟机，然后部署到监控每台 ESX 服务器上的每个虚拟交换机。每个受监控的 vSwitch 都经克隆，并且 vShield 监控器链接到克隆的 vSwitch 和原始 vSwitch 之间。所收集的数据返回到 vShield 管理站点。你可以在管理站点创建策略以监控虚拟架构网络流量，并报道允许和拒绝的网络流量。

在六个版本的 vSphere Editions 中，有三个版本提供 vShield Zones：Advanced、Enterprise 和 Enterprise Plus。另外，需要 VMware 的 vCenter。可以在 SearchVMware.com 网站上查看 vShield Zones 介绍。

更多信息请参看 VMware's vShield Zones 产品页合 vShield Zones 1.0 FAQ 的 DPM。

*(作者：David Davis 译者：唐琼瑶 来源：TechTarget 中国)*
原文标题：VMware vShield Zones 如何有助于虚拟机安全监控？
原文链接：http://www.searchvirtual.com.cn/showcontent_33367.htm

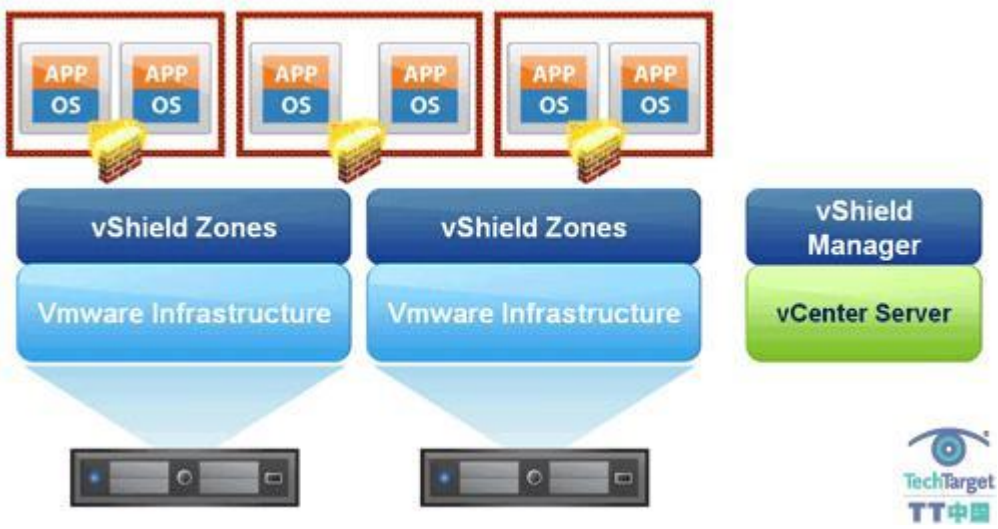
# VMware vShield Zones 组件及其工作原理介绍

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。

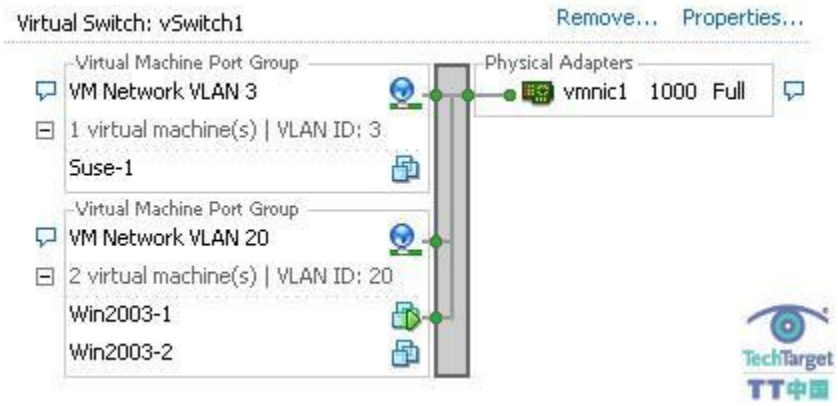
试想原来有一组可以通过公路到达的房子。为了保护这些房子，使得只有被允许的访客可以进入，我们首先把这些房子搬迁到一个独立的小岛上。所有试图进入小岛的客人，都必须跨越一座唯一的小桥。在小桥的入口处放置一个守卫（vShield 客户端 ），他只允许出现在访客列表上（防火墙规则）的客人通行。同时，警卫会监控和管理所有通过小桥的人流来排查任何可疑的情况（流量分析）。

接下来用技术术语说明部署 vShield 代理的步骤：

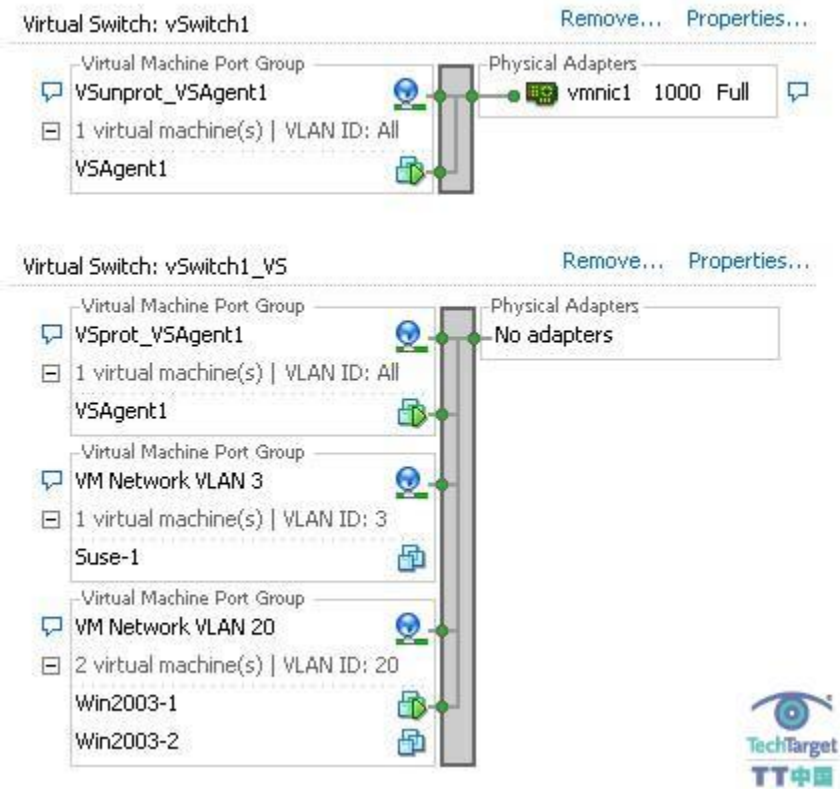
1. 根据样本为 vShield 客户端程序创建一个新的虚拟机。然后为虚拟机分配三块虚拟网卡（vNIC），一个用于跟 VShield Manager 之间的对话；一个连接到原有的 vSwitch（vSwitch1）接管未被保护的流量（入口），另一个连接到新创建的 vSwitch（vSwitch2）作为到达虚拟机的被保护流量通道（出口）。
2. 创建新的 vSwitch（vSwitch2）时不分配物理网卡。
3. 在 vSwitch 1 上创建一组新的端口用于未被保护的流量通过，在 vSwitch2 上创建一组新的端口用于被保护的流量通过。vShield agent 的虚拟网卡（vNIC）分别建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

原文标题：VMware vShield Zones 组件及其工作原理介绍

原文链接：http://www.searchvirtual.com.cn/showcontent_26647.htm

## 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。

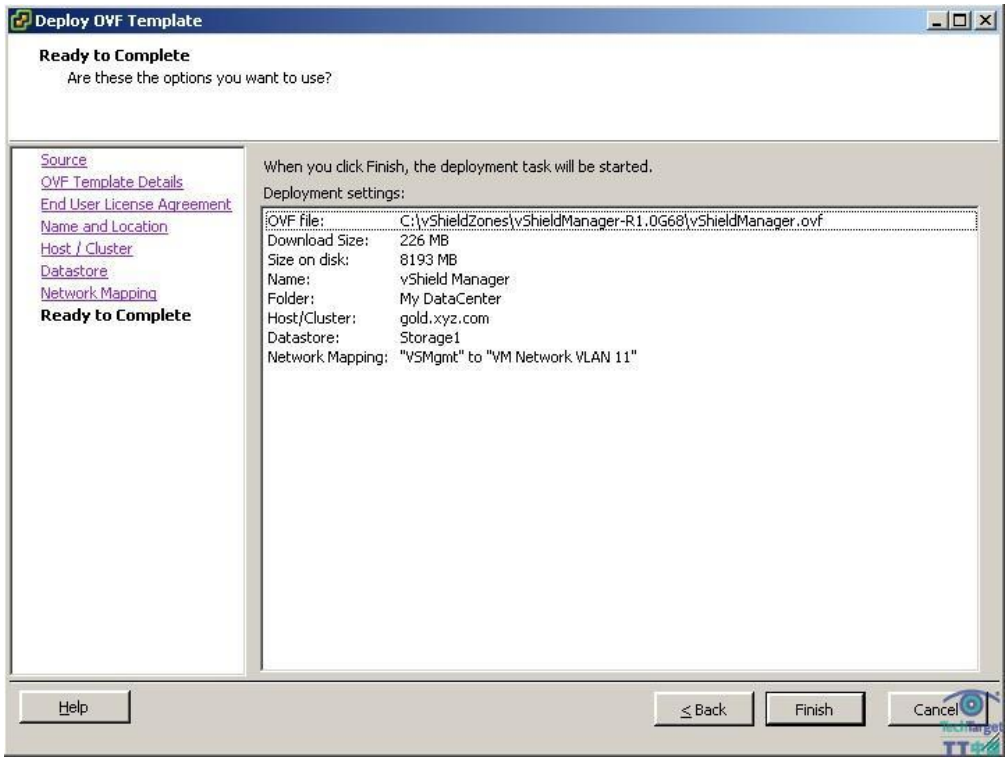
准备工作完成后，请遵循以下步骤开始安装 vShield Zones：

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。

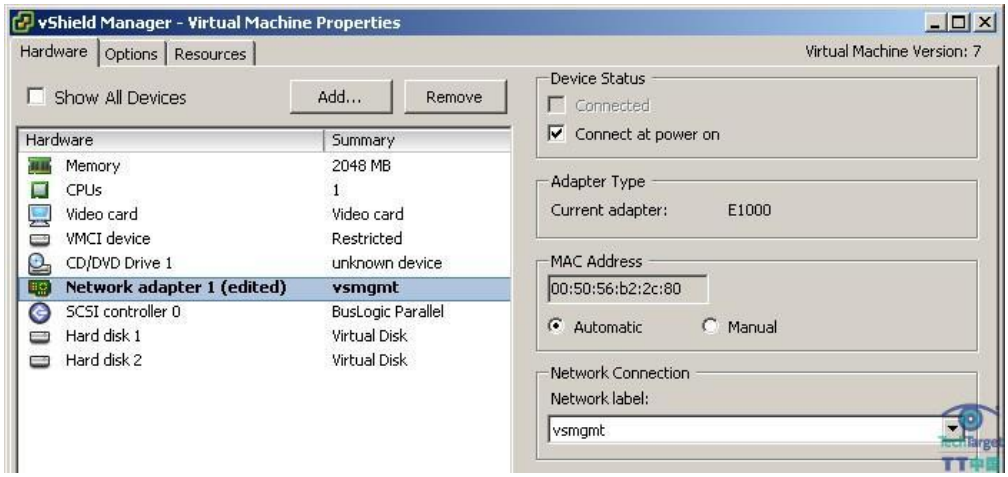
三、解压完成后，可以启用 vSphere 客户端程序在宿主机系统上创建 vShield Manager 虚拟机应用。

- 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

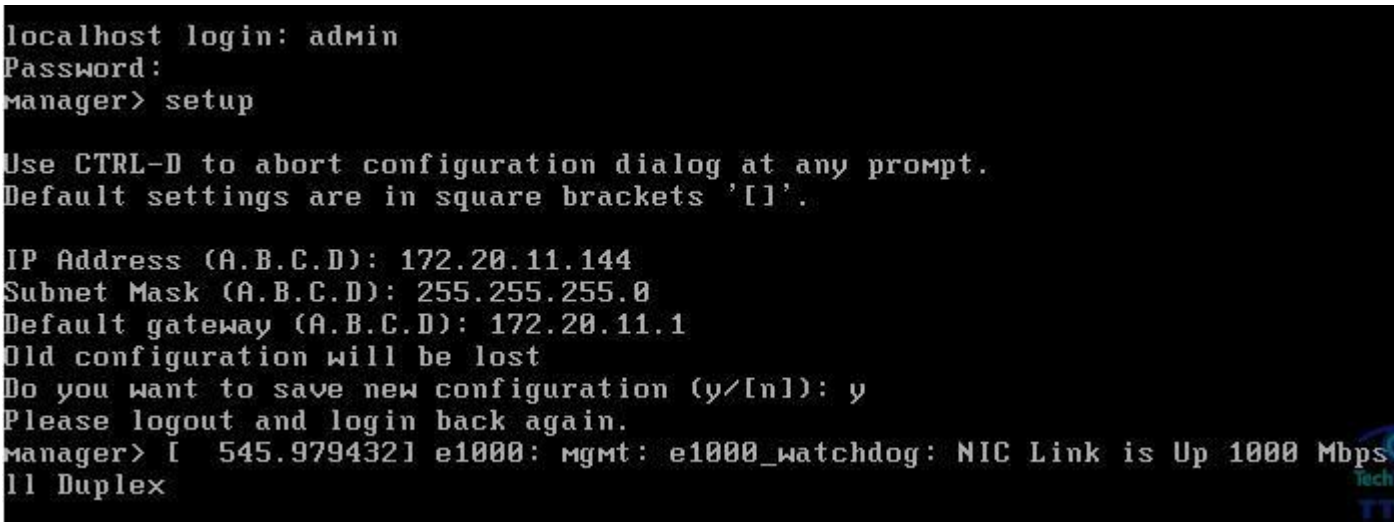



（点击图片就能放大）

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。

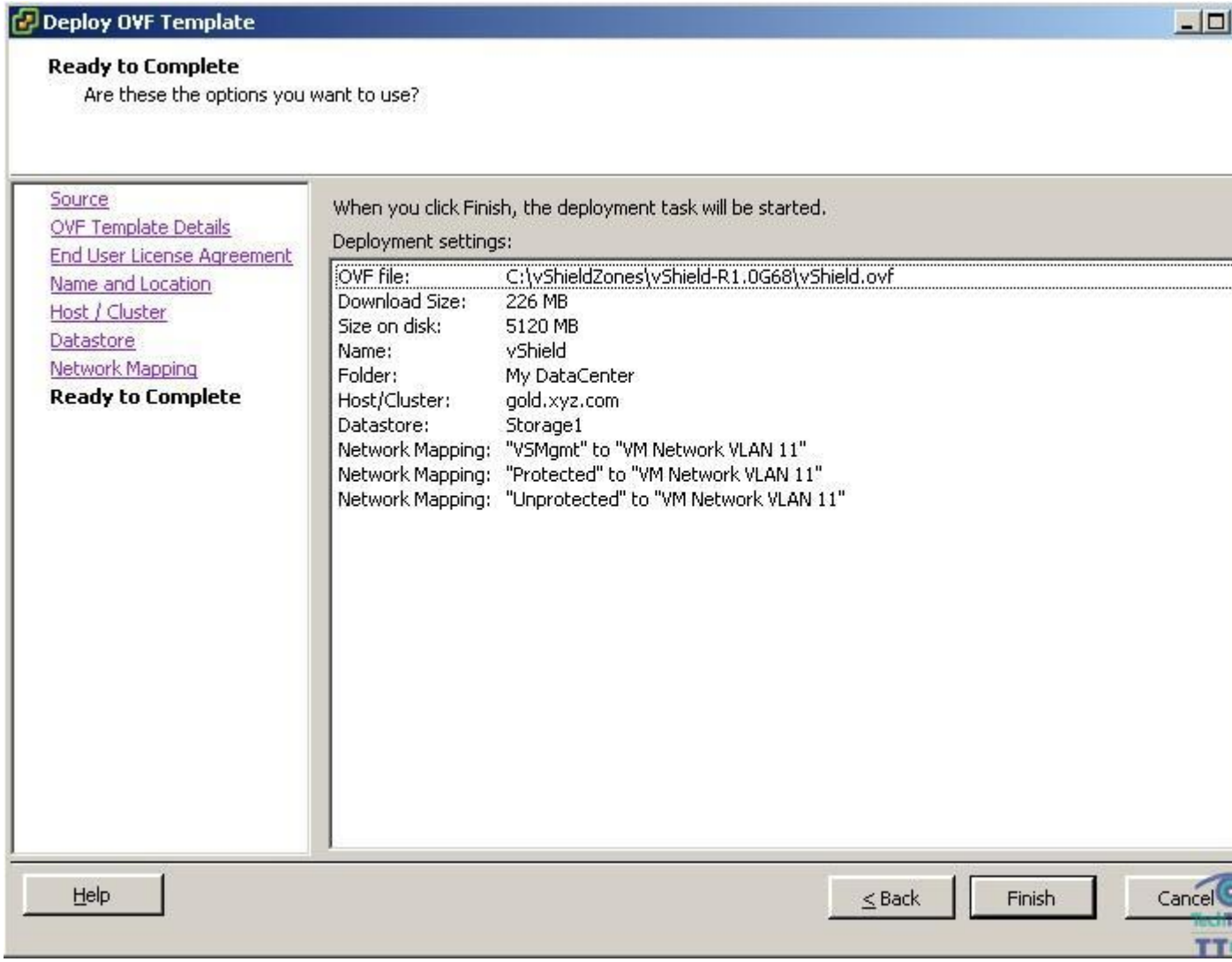


五、启动 vShield Manager 虚拟机。启动完成后，使用默认的用户名“admin”，密码“default”登陆。一旦登陆后，就进入管理向导界面，选择“setup”运行命令行界面的提示向导来配置网络设置。输入 IP 地址信息。完成后，选择“y”保存配置。系统将提示退出并重新登录，这个步骤并不是必须的，这时，你可以运行 ping vShield Manager 来确认网络连接是否正常。完成后选择“quit”退出。



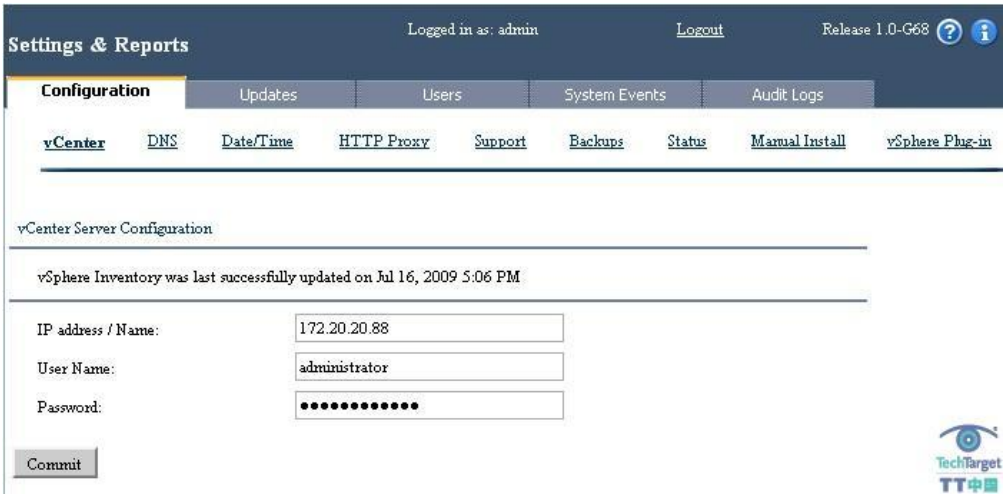

六、接下来需要从 vShield Agents OVF 文件创建一个虚拟机，并且把它保存为一个样本，方便后续 vShield Agents 的创建。为了完成这步操作，仍然需要使用 vSphere Client。

- 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。



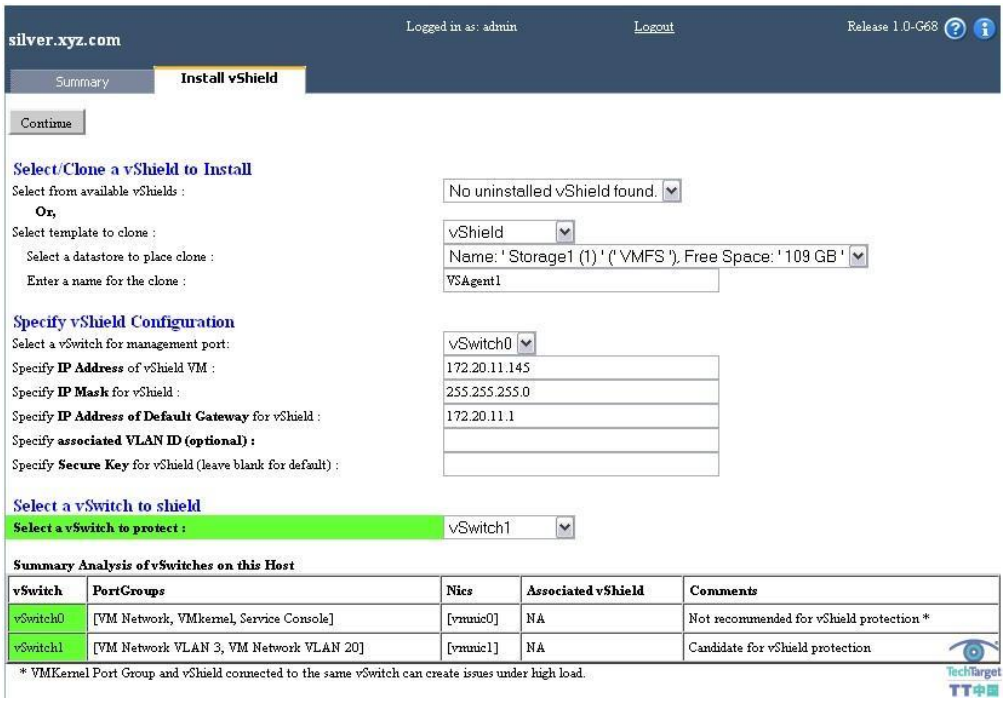

七、现在需要登录 vShield Manager 完成配置。

- 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

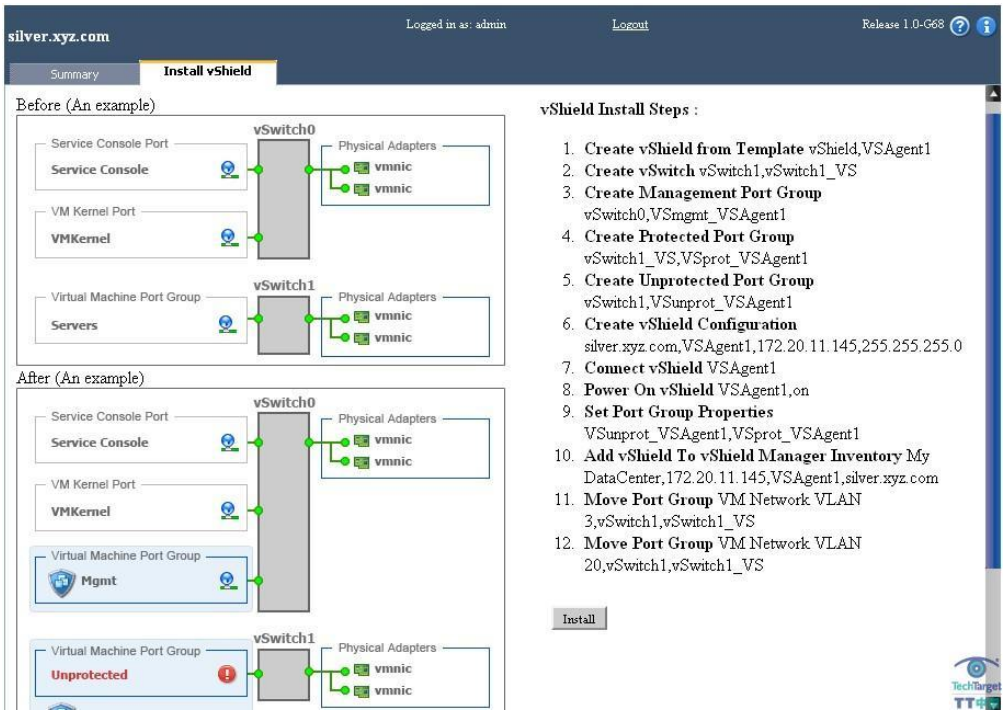



八、现在 vShield Manager 已经安装和配置完成，接下来需要部署 vShield Agents。

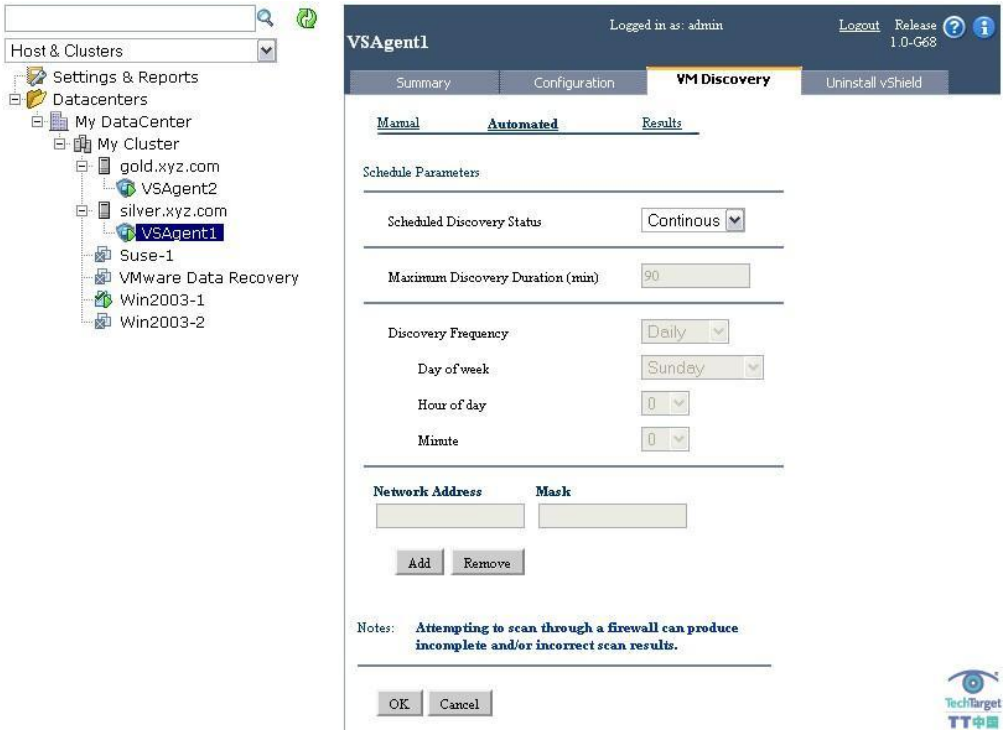
- 在左侧面板中选中你要添加保护的 ESX 主机
- 在面板右侧，选择 Install vShield 选项
- 选择 Configure Install Parameters 链接，显示页面中列举了新克隆的 vShield Agents 虚拟机，IP 地址和保护的 vSwitch 等相关信息。这里可以选择克隆已经存在的 vShield Agents 或者从之前保存的模板来创建
- 选择新 agent 虚拟机的数据存放地址，并为它指定唯一的名称
- 选择一个 vSwitch 作为 vShield 管理程序接口（vsmgmt），并且输入它的 IP 地址。在底部从下拉菜单中选择要添加保护的 vSwitch。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

原文标题：如何安装和配置 vShield Zones?

原文链接：http://www.searchvirtual.com.cn/showcontent_26652.htm

# 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)*

原文标题：管理 vShield Zones 的最佳技巧（上）

原文链接：http://www.searchvirtual.com.cn/showcontent_26650.htm

# 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)*

原文标题：管理 vShield Zones 的最佳技巧（下）

原文链接：http://www.searchvirtual.com.cn/showcontent_26651.htm