快速入门指南

vShield Zones 1.0

CN-000166-00

vmware®

您可以在 VMware 网站上找到最新的技术文档，网址为：

http://www.vmware.com/cn/support/

此外， VMware 网站还提供最新的产品更新。

如果对本文档有任何意见或建议，请将反馈信息提交至以下地址：

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

目录

关于本文档

*快速入门指南*提供有关将 vShield Zones 安装到 VMware® Virtual Infrastructure 环境中的信息。

目标读者

本文档是为需要安装或使用 vShield Zones 的人提供的。本文档的目标读者是熟悉虚拟机技术和数据中心操作且具有丰富经验的 Windows 或 Linux 系统管理员。此外，本文档假设读者熟悉 VMware Virtual Infrastructure，包括 vCenter Server 4.0、 VMware ESX 4.0 和 vSphere Client。

文档反馈

VMware 欢迎您提出宝贵建议，以便改进我们的文档。如有任何意见或建议，请将反馈发送到 docfeedback@vmware.com。

VMware Infrastructure 文档

vShield Zones 文档集包括下列文档：

- 《vShield Zones 管理指南》
- 《vShield Zones 快速入门指南》
- 《vShield Zones 简介》

此外，您还应该了解 vCenter Server 和 ESX 文档集。

技术支持和教育资源

下列各节介绍为您提供的技术支持资源。请通过下列网站访问本文档和其他文档的最新版本：http://www.vmware.com/cn/support/pubs。

在线支持和电话支持

要通过在线支持提交技术支持请求、查看产品和合同信息以及注册您的产品，请访问 http://www.vmware.com/cn/support。

客户只要拥有相应的支持合同，就可以通过电话支持，尽快获得对优先级高的问题的答复。请访问 http://www.vmware.com/cn/support/phone_support。

支持服务项目

要了解 VMware 支持服务如何帮助您满足业务需求，请访问 http://www.vmware.com/cn/support/services。

VMware 专业服务

VMware 教育服务课程提供了大量实践操作环境、案例研究示例，以及用作作业参考工具的课程材料。这些课程可以通过现场指导、教室授课的方式学习，也可以通过在线直播的方式学习。关于现场试点项目及实施的最佳实践， VMware 咨询服务可提供多种服务，协助您评估、计划、构建和管理虚拟环境。要了解有关教育课程、认证计划和咨询服务的信息，请访问 http://www.vmware.com/cn/services。

安装 vShield Zones

vShield Zones 提供防火墙保护和流量分析来保护 VMware vCenter Server 虚拟基础架构。已对大多数虚拟数据中心自动执行 vShield Zones 虚拟设备安装。

本章包含下列主题：

要求

在安装 vShield Zones 之前，您必须具备以下条件：

- 运行 vCenter Server 4.0 或更高版本的系统
- 至少一个安装了 ESX 4.0 且正常运转的系统
- 一台使用 vSphere Client 的个人计算机
- 添加和启动虚拟机的权限
- 对存储虚拟机文件的数据存储的访问权限，以及将文件复制到该数据存储的帐户权限
- vShield Manager 和 vShield OVF 文件
- 供安装的每个 vShield 实例的管理接口使用的静态 IP 地址
- 供 vShield Manager 管理接口使用的单一静态 IP 地址
- 在 Web 浏览器中启用 Cookies 以访问 vShield Manager 用户界面

vShield Zones 组件

vShield Zones 解决方案包括下列组件：

- vShield Manager：管理所有分布式 vShield 实例的 vShield Zones 管理中心。为监控、配置 vShield 及对其进行软件更新而提供。
- vShield：vShield Zones 的活动安全组件，该组件检查流量并提供防火墙保护。在每台要保护的 ESX 主机上安装 vShield。在流量路径内安装 vShield 以监控所有流入和流出 ESX 主机的流量，以及主机上虚拟机之间的流量。

安装 vShield Zones 之前评估 ESX 网络配置

在 vCenter Server 环境中安装 vShield Zones 之前，请考虑 ESX 主机的网络配置。作为最低要求，每台主机需至少包含一个关联的物理网卡和一个 vSwitch，用于承载 VMKernel、服务控制台和虚拟机。在更稳定的环境中， ESX 主机可能具有多个专用物理网卡和多个 vSwitch，以将 VMKernel 和服务控制台与虚拟机分隔开。

vShield Zones 设备作为虚拟机安装在 ESX 主机上。但是，安装 vShield 需要进行规划。可以在任何具有专用网卡的 vSwitch 上安装 vShield。 vShield 安装将虚拟机从其原始 vSwitch 移动到克隆的 vSwitch。vShield 随后在原始 vSwitch 和克隆的 vSwitch 之间安装，以捕获进出虚拟机的所有流量。原始 vSwitch 保留该网卡，但新 vSwitch 与网卡无关联。因此，如果您的 ESX 主机带有多个承载多个虚拟机的 vSwitch，则每个 vSwitch 都需要有一个 vShield。任何连接到未安装 vShield 的 vSwitch 的虚拟机都不受 vShield Zones 保护。

通过安装 vShield OVF，然后将原始 vShield 虚拟机部署为模板，简化了多个 vShield 的安装。此模板由 vShield Manager 引用，允许您将多个 vShield 从 vShield Manager 用户界面安装到 vCenter Server 环境。有关 vShield 安装过程的详细信息，请参见 “vShield 自动安装概览”（第 13 页）。

请注意 构建 vShield Zones 系统是为了保护虚拟机，而不是为了保护 VMKernel 或服务控制台。

安装 vShield Zones

vShield Zones 安装是多步骤过程。依次执行下列任务以成功完成 vShield Zones 安装。

获得 vShield Zones 虚拟设备

vShield Zones 虚拟设备是使用开放虚拟化格式 (OVF) 打包而成的。这种打包方式允许您使用 vSphere Client 将虚拟设备导入数据存储和虚拟机清单中，因而简化了安装。

请联系您的 VMware 客户团队以获取 vShield Zones 软件包，此软件包包含一个 vShield Manager 和一个 vShield。一个 vShield 虚拟设备可用于多个 vShield 安装。

获取软件包后，将其下载到安装了 vSphere Client 的个人计算机上。

使用 vSphere Client 将 vShield Manager 作为虚拟机安装

vShield Manager 虚拟机安装需要为 vShield Manager 创建端口组。

将 vShield Manager 作为虚拟机添加到您的 vCenter Server 清单中

1 登录 vSphere Client。

2 在清单面板中选择 ESX 主机。

3 转到 **[File] > [Deploy OVF Template]**。

此时将打开 “部署 OVF 模板”向导。

4 单击 **[Deploy from file]**，然后单击 **[Browse]** 找到个人计算机中包含 vShield Manager OVF 文件的文件夹。

5 完成此向导。

此时 vShield Manager 即安装到清单中。

6 在安装了 vShield Manager 的 ESX 主机上为 vShield Manager 创建名为 **[vsmgmt]** 的端口组。

每个已安装的 vShield 都能识别此端口组名称，该名称可在 vShield 安装期间阻止 vShield 移动 vShield Manager 虚拟机。

7 编辑 vShield Manager 虚拟机的设置以在启动时连接并为 vsmgmt 端口组设置网络标签。

a 右键单击 vShield Manager 虚拟机并单击 **[Edit Settings]**。

此时将打开 “vShield Manager - 虚拟机属性”对话框。

b 在 **[Hardware]** 选项卡下，单击 **[Network Adapter 1]**。

c 在 “设备状态”下，选择 **[Connect at power on]**。

d 在 **[Network label]** 下拉列表中选择 **[vsmgmt]**。

e 单击 **[OK]** 关闭该窗口。

8 启动 vShield Manager 虚拟机。

9 单击右窗格中的 **[Console]** 选项卡打开 vShield Manager CLI。

引导过程可能需要几分钟时间。

10 出现 `[manager login]` 提示后，使用用户名 **`[admin]`** 和密码 **`[default]`** 登录 CLI。

11 运行 `[setup]` 命令启动 CLI 设置向导。

CLI 设置向导会引导您完成为 vShield Manager 的管理接口分配 IP 地址并标识默认网络网关的过程。管理接口的 IP 地址必须可以由所有已安装的 vShield 实例以及用于系统管理的 Web 浏览器访问。

```
manager> setup

Use ctrl-d to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

Hostname [manager]:
IP Address [10.115.216.66/255.255.255.0]:
Default gateway [10.115.219.253]:
Old configuration will be lost, and system needs to be rebooted
Do you want to save new configuration (y/[n]): y
Please log out and log back in again.
```

此时无需注销。 vShield Manager 安装完成。

12 对默认网关执行 Ping 命令以验证网络连接。

```
manager> ping 10.115.219.253
```

13 在个人计算机中，对 vShield Manager IP 地址执行 ping 命令以验证 IP 地址是否可访问。

安装 vShield Image 并将其转换成模板

将 vShield 作为虚拟机安装并将其转换成模板。将 vShield 虚拟机转换成模板格式之后， vShield Manager 可以引用该模板进行多个 ESX 实例上的 vShield 安装。

将 vShield 添加到 vCenter Server 并将其转换成模板

1 登录 vSphere Client。

2 在清单面板中选择 ESX 主机。

3 转到 **[File] > [Deploy OVF Template]**。

此时将打开 “部署 OVF 模板”向导。

4 单击 **[Deploy from file]**，然后单击 **[Browse]** 在客户端计算机上找到包含 vShield OVF 文件的文件夹。

5 完成此向导。

此时 vShield 已安装到清单中。

警告 此时不要启动或编辑 vShield 虚拟机。此时启动或编辑虚拟机可能会导致网络问题，例如无限循环。

6 在向导完成安装之后，将 vShield 实例转换成虚拟机模板。

借助此模板，可以自动从 vShield Manager 用户界面安装多个 vShield 实例。

登录 vShield Manager 用户界面以配置系统

在安装 vShield Manager 虚拟设备并将 vShield Image 转换成模板之后，请登录 vShield Manager 用户界面并将 vShield Manager 配置为使用 vCenter Server 进行身份验证。此身份验证使 vShield Manager 可以显示您的 vCenter Server 清单、安装 vShield 实例并配置防火墙以保护您的资源。

登录 vShield Manager 用户界面

1 打开 Web 浏览器窗口并键入分配给 vShield Manager 的 IP 地址。

必须将 IP 地址预置为支持 **`https`**。

2 接受安全证书。

此时将显示 vShield Manager 登录屏幕。

3 使用用户名 **`admin`** 和密码 **`default`** 登录 vShield Manager 用户界面。

vShield Manager 用户界面在右侧框中打开至 **[Configuration] > [vCenter]** 选项卡内容。在初始登录时，vShield Manager 中不显示任何信息，因为您尚未同步与 vCenter Server 的通信。

4 按照如下方式完成 **[vCenter]** 选项卡表单：

字段	操作
[IP address/Name]	键入 vCenter Server 的 IP 地址。
[User Name]	键入 vSphere Client 用户名。
[Password]	键入与 vSphere Client 用户名关联的密码。

5 单击 **[Commit]**。

vShield Manager 连接到 vCenter Server，登录并访问 VMware Virtual Infrastructure SDK。位于 vShield Manager 屏幕左侧的清单树应与 vSphere Client [主机和群集] 清单树视图匹配。

请注意 vShield Manager 不显示在 vShield Zones 清单面板中。**[Settings & Reports]** 对象代表清单面板中的 vShield Manager。

添加 vShield

您可以通过从 vShield 模板创建副本将 vShield 添加到 vCenter Server 和 vShield Zones 清单中。

您应该为每个带有附加网卡的 vSwitch 安装一个 vShield 实例。任何连接到未安装 vShield 的 vSwitch 的虚拟机均不受 vShield Zones 保护。

请注意 要在 vNetwork 分布式交换机 (vNDS) 上安装 vShield，请参见《vShield Zones 管理指南》。

添加 vShield

1 登录 vShield Manager。

2 在清单树中，单击要保护的 ESX 主机。

3 单击显示在右侧框上方的 **[Install vShield]** 选项卡。

4 单击 **[Configure install parameters]**。

5 按照如下方式完成该表单：

字段	操作
[Select from available vShields]	将此字段留空。仅当在没有已建立的模板的情况下添加 vShield 时才使用此字段。
[Select template to clone]	单击此下拉菜单并选择 vShield 模板。
[Select a datastore to place clone]	单击此下拉菜单并选择要存储 vShield 副本的数据存储。
[Enter a name for the clone]	键入 vShield 副本的唯一名称。此名称将显示在 vSphere Client 清单和 vShield Manager 清单中。
[Specify IP Address of vShield VM]	键入要分配到 vShield 的管理端口的 IP 地址。
[Specify IP Mask for vShield]	键入与分配的 IP 地址关联的 IP 子网掩码。
[Specify IP Address of Default Gateway for vShield]	键入默认网络网关的 IP 地址。
[Specify Secure Key for vShield]（默认情况下留空）	（可选）键入用于确保在 vShield 和 vShield Manager 之间进行安全通信的密钥。默认情况下，此字段中的此条目处于屏蔽状态。此默认种子用于加密 vShield 和 vShield Manager 之间的通信。这些密钥不在网络上共享。
[Select a vSwitch to shield]	单击下拉菜单选择要保护的 vSwitch。符合保护条件的 vSwitch 在随附表中突出显示为绿色。

6 单击 **[Continue]**（位于表单上方）。

此时将显示 [Installation Summary] 屏幕。此屏幕显示于在 ESX 上安装 vShield 的示例图之前或之后。

请注意 示例图是静态的，不直接反映虚拟网络。屏幕右侧编号的安装脚本详细介绍了实际安装步骤。

7 单击 **[Install]**。

您可以按位于 vSphere Client 窗口底部的 [Recent Tasks] 状态窗格中的 vShield 安装步骤执行安装。有关安装过程的详细信息，请参见 “vShield 自动安装概览”（第 13 页）。

此时 vShield 安装完成。

8 在安装完成后，打开 vSphere Client。

9 在清单中找到该 vShield。

注意它处于已启动状态。

启用持续发现以标识客户虚拟机流量

在安装了 vShield Manager 和 vShield，并且 vShield 与 vShield Manager 进行通信之后，您必须为 vShield 启用持续发现操作以保护虚拟机。

启用对虚拟机流量的持续发现

1 登录 vShield Manager。

2 从清单树单击 vShield 实例。

3 单击 **[VM Discovery]** 选项卡。

4 单击 **[Automated]** 副标题。

5 在 **[Scheduled Discovery Status]** 下拉菜单中，选择 **[Continuous]**。

不要填写表单中的其他字段。

6 单击 **[OK]**。

发现操作开始。发现持续运行，并根据应用程序和协议规范标识流量。

7 转到 **[VM Discovery] > [Results]** 以查看发现输出。

发现的流量由虚拟机 IP 地址分隔。每个发现的虚拟机都保存在 **[VM Inventory]** 选项卡下，可以在 vShield Manager 中以数据中心、群集容器级别以及虚拟机级别使用。

vShields 的其他 vCenter 配置

如果启用了 VMware HA 或 VMware DRS 功能，则必须禁止 vShield Zones 虚拟设备进行移动。必须在安装每个 vShield Zones 组件之后执行此操作。

您可以使用 VMotion 迁移 vShield Manager 虚拟设备，不会产生不良影响。

禁止 VMware HA 或 VMware DRS 移动 vShield Zones 虚拟设备

1 登录 vSphere Client。

2 右键单击包含 vShield Zones 虚拟设备的群集并单击 **[Edit Properties]**。

此时将打开 “管理设置”对话框。

3 在 VMware HA 下，单击 **[Virtual Machine Options]**。

在列表中找到 vShield Manager 和 vShield。

4 对于每个 vShield Zones 虚拟设备，选择下列值：

- **[VM Restart Priority]**: **[Disabled]**
- **[Host Isolation Response]**: **[Leave VM powered on]**

5 如果已经启用了 DRS，请单击 VMware DRS 下的 **[Virtual Machine Options]**。

在列表中找到 vShield Manager 和 vShield。

6 对于每个 vShield Zones 虚拟设备，为 **[Automation Level]** 选择 **Disabled**。

7 在配置所有的 vShield Zones 虚拟设备之后，单击 **[OK]**。

在默认操作中，在操作员或 VMotion 尝试迁移虚拟机期间 vShield 会引发错误。该错误提示服务器连接到了虚拟 Intranet。虚拟 Intranet 是虚拟机连接到的网络，位于 vShield 的保护端的 vSwitch 上。此 vSwitch 不带有物理网卡。vShield 将流量桥接到连接到物理网卡的网络的非保护端。

启用 VMotion 以禁用虚拟 Intranet 检查

1 在运行 vCenter Server 的计算机上找到 `vpxd.cfg` 文件。默认情况下，此文件安装在 `C:\Documents and Settings\All Users\Application Data\VMware\VMware vCenter Server`。

2 在文本编辑器中编辑该 `vpxd.cfg` 文件。

将以下各行添加为 `config` 节的子级别，使它们与 `vpxd` 节的级别相同。

```
<migrate>
    <test>
        <CompatibleNetworks>
            <VMOnVirtualIntranet>false</VMOnVirtualIntranet>
        </CompatibleNetworks>
    </test>
</migrate>
```

3 保存该 `vpxd.cfg` 文件。

4 重新启动 VMware vCenter Server 服务。您可以通过转到 **[Control Panel] > [Administrative Tools] > [Services]** 来访问该服务菜单。

要进一步配置 vShield Zones，请参见《vShield Zones 管理指南》。

关闭 vShield Zones 虚拟机

您可以随时关闭 vShield Zones 虚拟机。在关闭 vShield Zones 虚拟机后，当再次启动该虚拟机时将使用上次保存的配置。

关闭 vShield Zones 虚拟机

1 在 vSphere Client 中，从清单面板中选择 vShield Zones 虚拟机。

2 单击 **[Console]** 选项卡打开 vShield Zones CLI。

3 登录 CLI。

4 在登录后，键入 `enable` 以进入特权模式。

5 键入 `shutdown`。

6 当关闭 CLI 后，在清单面板上右键单击虚拟机并选择 **[Power] > [Power Off]**。

vShield 自动安装概览

当从引用的模板中进行安装时， vShield 安装过程执行下列步骤：

1 创建 vSwitch 主机的副本。

此 vSwitch 副本不包含网卡。vSwitch 副本的名称由 vSwitch 主机的名称加上 _VS 构成：vSwitch1_VS。

2 创建一个受保护的区域端口组 VSprot_*vShield-name*，并将该端口组附加到 vSwitch 主机。

3 在 vShield 实例的管理接口的 vSwitch 主机上创建一个管理端口组 VSmgmt_*vShield-name*。

4 创建一个不受保护的区域端口组 VSunprot_*vShield-name*，并将该端口组附加到 vSwitch 副本。

重要信息 不要将虚拟机添加到受保护的端口组或不受保护的端口组。这些端口组配置为启用杂乱模式，该模式允许 vShield 查看所有通过的流量。

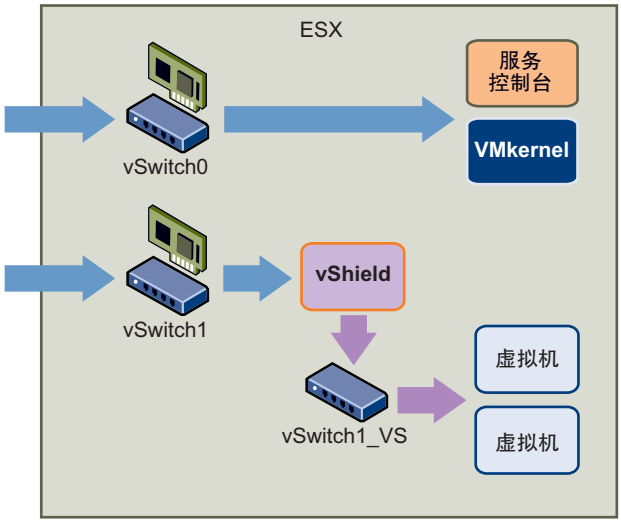
5 连接并启动 vShield 实例。

6 将 vShield 上的虚拟接口附加到受保护的端口组和不受保护的端口组。

7 将虚拟机从 vSwitch 主机移动到 vSwitch 副本。

如果 vShield Manager 虚拟机位于同一 vSwitch 上，则不进行移动。在 vShield Manager 安装期间，创建用于放置 vShield Manager 的名为 **[vsmgmt]** 的端口组。 vShield 安装识别此端口组名称并忽略此端口组中的任何虚拟机。

图 1. 在 vSwitch 上安装 vShield



了解从 vShield 安装创建的端口组

vShield 安装需要创建两个端口组。这些端口组分隔信任区域：不受保护区域和受保护区域。不受保护区域监控入站流量，而受保护区域监控出站流量。每个端口组承载一个 vShield 接口：U0 适用于不受保护区域， P0 适用于受保护区域。通过将这些接口连接到创建的端口组， vShield 可以监控所有入站和出站流量。

将不受保护端口组和受保护端口组配置为启用杂乱模式。在杂乱模式中，客户机适配器可以侦听所有通过的数据包。在非杂乱模式中，客户机适配器将仅侦听其自身 MAC 地址上的流量。默认情况下，客户机适配器设置为非杂乱模式。为保护起见， vShield 必须可以查看所有通过的流量。不要将任何其他虚拟机添加到这些端口组。