vShield 快速入门指南

vShield Manager 5.0
vShield App 5.0
vShield Edge 5.0
vShield Endpoint 5.0

在本文档被更新的版本替代之前，本文档支持列出的每个产品的版本和所有后续版本。要查看本文档的更新版本，请访问 http://www.vmware.com/cn/support/pubs。

ZH_CN-000695-00

vmware®

最新的技术文档可以从 VMware 网站下载：

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

VMware 网站还提供最近的产品更新信息。

您如果对本文档有任何意见或建议，请把反馈信息提交至：

docfeedback@vmware.com

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

北京办公室
北京市海淀区科学院南路 2 号
融科资讯中心 C 座南 8 层
www.vmware.com/cn

上海办公室
上海市浦东新区浦东南路 999 号
新梅联合广场 23 楼
www.vmware.com/cn

广州办公室
广州市天河北路 233 号
中信广场 7401 室
www.vmware.com/cn

目录

关于本书

《vShield 快速入门指南》手册介绍了如何使用 vShield Manager 用户界面、vSphere Client 插件和命令行界面 (CLI) 安装和配置 VMware® vShield 系统。此信息包括分步配置说明以及建议的最佳做法。

目标读者

本手册专供要在 VMware vCenter 环境中安装或使用 vShield 的用户使用。本手册的目标读者为熟悉虚拟机技术和虚拟数据中心操作且经验丰富的系统管理员。本手册假设您熟悉 VMware Infrastructure 4.x，包括 VMware ESX、vCenter Server 和 vSphere Client。

VMware 技术刊物词汇表

VMware 技术刊物词汇表中介绍了您可能不熟悉的术语。有关 VMware 技术文档中所使用的术语的定义，请访问 http://www.vmware.com/support/pubs。

文档反馈意见

VMware 欢迎您提供文档改进意见和建议。如有任何意见或建议，请将反馈信息提交至 docfeedback@vmware.com。

技术支持和教育资源

您可以获取以下技术支持资源。有关本文档和其他文档的最新版本，请访问：http://www.vmware.com/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/support。

对于优先级最高的问题，已签署相应支持合同的客户应使用电话支持，以迅速获得支持。请访问 http://www.vmware.com/support/phone_support.html。

支持服务项目

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

VMware 专业服务

VMware 培训服务课程提供了丰富的实践练习、案例研究示例和课程材料，均可用作您工作中的参考工具。培训形式多样，包括现场授课、课堂培训以及实时网络教学。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/services。

1 vShield 简介

本章介绍您安装的 VMware® vShield 组件。

本章讨论了以下主题：

vShield 组件一览

VMware vShield 是专为 VMware vCenter Server 集成而构建的安全虚拟设备套件。vShield 是保护虚拟化数据中心免遭攻击和误用的关键安全组件，可帮助您实现合规性强制要求目标。

vShield 包含对保护虚拟机至关重要的虚拟设备和服务。可通过基于 Web 的用户界面、vSphere Client 插件、命令行界面 (CLI) 和 REST API 配置 vShield。

vCenter Server 包含 vShield Manager。以下每个 vShield 软件包都需要一个许可证：

- vShield App
- vShield App with Data Security
- vShield Edge
- vShield Endpoint

一个 vShield Manager 管理多个 vShield App、vShield Edge、vShield Endpoint 和 vShield Data Security 实例。

- vShield Manager 第 8 页，

  vShield Manager 是 vShield 的集中式网络管理组件，可作为虚拟设备安装在 vCenter Server 环境中的任意 ESX 主机上。vShield Manager 可在与安装 vShield 代理不同的 ESX 主机上运行。

- vShield App 第 8 页，

  vShield App 是基于管理程序的防火墙，可保护虚拟数据中心中的应用程序免遭基于网络的攻击。组织可查看和控制虚拟机之间的网络通信。您可以基于逻辑构造（如 VMware vCenter 容器和 vShield 安全组），而不仅是基于物理构造（如 IP 地址）来创建访问控制策略。此外，可变 IP 寻址会提供在多租户区域中使用同一 IP 地址简化置备的功能。

- vShield Edge 第 8 页，

  vShield Edge 提供网络边缘安全和网关服务，用于隔离端口组、vDS 端口组或 Cisco Nexus 1000V 中的虚拟机。vShield Edge 通过提供 DHCP、VPN、NAT 和负载平衡等常见网关服务将隔离的末端网络连接到共享（上行链路）网络。vShield Edge 通常部署在 DMZ、VPN 外联网和多租户云计算环境中，vShield Edge 在这些环境中为虚拟数据中心 (Virtual Datacenter, VDC) 提供外围安全保护。

- vShield Endpoint 第 9 页，

  vShield Endpoint 可将防病毒和防恶意软件代理处理任务转移到 VMware 合作伙伴提供的专用安全虚拟设备上。由于安全虚拟设备（与客户机虚拟机不同）不会脱机，因此可以不断地更新防病毒签名，从而为主机上的虚拟机提供持续保护。另外，还可以在新虚拟机（或处于脱机状态的现有虚拟机）联机时，立即使用最新防病毒签名保护这些虚拟机。

- vShield Data Security 第 10 页，

  可通过 vShield Data Security 查看存储在组织的虚拟化环境和云环境中的敏感数据。根据 vShield Data Security 报告的冲突，您可以确保敏感数据受到充分保护，并且能评估与周围环境中的法规是否相符。

vShield Manager

vShield Manager 是 vShield 的集中式网络管理组件，可作为虚拟设备安装在 vCenter Server 环境中的任意 ESX 主机上。vShield Manager 可在与安装 vShield 代理不同的 ESX 主机上运行。

使用 vShield Manager 用户界面或 vSphere Client 插件，管理员可以安装、配置和维护 vShield 组件。vShield Manager 用户界面利用 VMware Infrastructure SDK 显示 vSphere Client 清单面板的副本，并包含 Hosts & Clusters 和 Networks 视图。

vShield App

vShield App 是基于管理程序的防火墙，可保护虚拟数据中心中的应用程序免遭基于网络的攻击。组织可查看和控制虚拟机之间的网络通信。您可以基于逻辑构造（如 VMware vCenter 容器和 vShield 安全组），而不仅是基于物理构造（如 IP 地址）来创建访问控制策略。此外，可变 IP 寻址会提供在多租户区域中使用同一 IP 地址简化置备的功能。

应当在群集内的每台 ESX 主机上安装 vShield App，这样 VMware vMotion 操作便可正常运行，且虚拟机在 ESX 主机之间迁移时仍会受保护。默认情况下，使用 vMotion 无法移动 vShield App 虚拟设备。

流监控功能会显示在应用程序协议级别的虚拟机之间的网络活动。您可以使用此信息审核网络流量、定义和细化防火墙策略以及标识网络。

vShield Edge

vShield Edge 提供网络边缘安全和网关服务，用于隔离端口组、vDS 端口组或 Cisco Nexus 1000V 中的虚拟机。vShield Edge 通过提供 DHCP、VPN、NAT 和负载平衡等常见网关服务将隔离的末端网络连接到共享（上行链路）网络。vShield Edge 通常部署在 DMZ、VPN 外联网和多租户云计算环境中，vShield Edge 在这些环境中为虚拟数据中心 (Virtual Datacenter, VDC) 提供外围安全保护。

标准 vShield Edge 服务（包含 vCloud Director）

防火墙 支持的规则包括 IP 5 元组配置（包含用于 TCP、UDP 和 ICMP 状态监测的 IP 地址和端口范围）。

网络地址转换 分别用于控制源 IP 地址和目标 IP 地址以及 TCP 和 UDP 端口转换的独立控制项。

动态主机配置协议 (DHCP) 配置 IP 池、网关、DNS 服务器和搜索域。

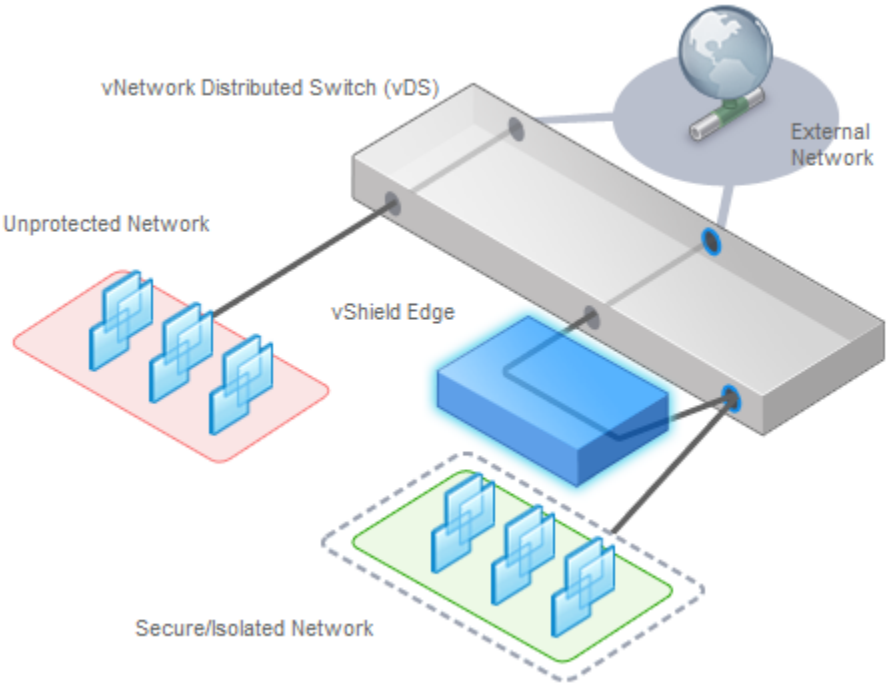
高级 vShield Edge 服务

点对点虚拟专用网络 (VPN) 使用标准化 IPsec 协议设置与所有主要防火墙供应商进行交互操作。

负载平衡 简单动态地配置虚拟 IP 地址和服务器组。

vShield Edge 支持将所有服务的 syslog 导出到远程服务器。

图 1–1 为保护 vDS 端口组而安装的 vShield Edge

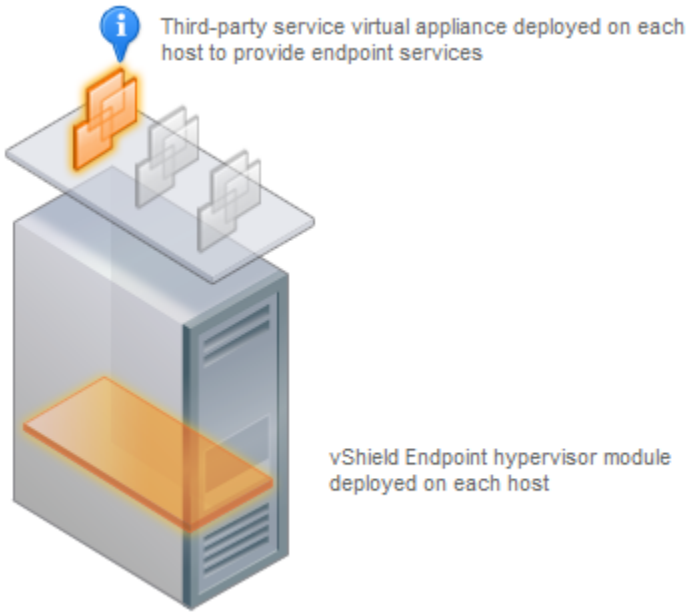


vShield Endpoint

vShield Endpoint 可将防病毒和防恶意软件代理处理任务转移到 VMware 合作伙伴提供的专用安全虚拟设备上。由于安全虚拟设备（与客户机虚拟机不同）不会脱机，因此可以不断地更新防病毒签名，从而为主机上的虚拟机提供持续保护。另外，还可以在新虚拟机（或处于脱机状态的现有虚拟机）联机时，立即使用最新防病毒签名保护这些虚拟机。

vShield Endpoint 可作为虚拟化管理程序模块和来自第三方防病毒供应商（VMware 合作伙伴）的安全虚拟设备安装在 ESX 主机上。管理程序可从外部扫描客户机虚拟机，而无需从每个虚拟机中的代理进行扫描。这使 vShield Endpoint 在优化内存使用情况的同时更为有效地避免出现资源瓶颈。

图 1–2 安装在 ESX 主机上的 vShield Endpoint



vShield Data Security

可通过 vShield Data Security 查看存储在组织的虚拟化环境和云环境中的敏感数据。根据 vShield Data Security 报告的冲突，您可以确保敏感数据受到充分保护，并且能评估与周围环境中的法规是否相符。

部署方案

使用 vShield，您可以为各种虚拟机部署构建安全区域。您可以根据特定应用程序、网络分段或自定义合规性因素隔离虚拟机。确定区域分配策略后，可以通过部署 vShield 在这些区域中强制实施访问规则。

- 保护 DMZ 第 11 页，

  DMZ 是指混合信任区域。客户端从 Internet 进入以获取 Web 和电子邮件服务，DMZ 中的服务可能要求访问内部网络中的服务。

- 隔离和保护内部网络第 11 页，

  可以使用 vShield Edge 将内部网络与外部网络隔离。vShield Edge 提供外围防火墙保护和边界服务，以保护端口组中的虚拟机，并支持通过 DHCP、NAT 和 VPN 与外部网络通信。

- 保护群集中的虚拟机第 11 页，

  可以使用 vShield App 保护群集中的虚拟机。

- vShield Edge 的常见部署第 12 页，

  可以使用 vShield Edge 隔离末端网络，从而使用 NAT 允许流量传入和传出网络。如果部署内部末端网络，可以通过 VPN 通道实现 LAN 到 LAN 的加密，从而利用 vShield Edge 保护网络之间的通信。

- vShield App 的常见部署第 12 页，

  可以使用 vShield App 在 vDC 中创建安全区域。可以强制在 vCenter 容器或安全组上实施防火墙策略。安全组是可以通过 vShield Manager 用户界面创建的自定义容器。利用基于容器的策略，您可以创建混合的信任区域，而不需要外部物理防火墙。

保护 DMZ

DMZ 是指混合信任区域。客户端从 Internet 进入以获取 Web 和电子邮件服务，DMZ 中的服务可能要求访问内部网络中的服务。

可以将 DMZ 虚拟机置于一个端口组中，并使用 vShield Edge 对该端口组进行保护。vShield Edge 提供防火墙、NAT 和 VPN 以及负载平衡等访问服务来保护 DMZ 服务。

要求访问内部服务的 DMZ 服务的一个常见示例是 Microsoft Exchange。Microsoft Outlook Web Access (OWA) 通常驻留在 DMZ 群集中，而 Microsoft Exchange 后端位于内部群集中。在内部群集中，您可以创建相关防火墙规则，以仅允许来自 DMZ 的 Exchange 相关请求，标识特定的源到目标参数。在 DMZ 群集中，您可以创建相关规则，将对 DMZ 的外部访问仅限于使用 HTTP、FTP 或 SMTP 协议的特定目标。

隔离和保护内部网络

可以使用 vShield Edge 将内部网络与外部网络隔离。vShield Edge 提供外围防火墙保护和边界服务，以保护端口组中的虚拟机，并支持通过 DHCP、NAT 和 VPN 与外部网络通信。

在安全的端口组内，可以在 vDS 所跨的每个 ESX 主机上安装一个 vShield App 实例，从而保护内部网络中虚拟机之间的通信。

如果您利用 VLAN 标记对流量进行分段，可以使用 App Firewall 创建智能访问策略。借助 App Firewall（而不是物理防火墙），可以合并或混合共享 ESX 群集中的信任区域。这样，您会获得 DRS 和 HA 等功能的最佳利用率和整合效果，而不是拥有单独的分段群集。将整个 ESX 部署作为单个池来管理远没有单独管理多个池复杂。

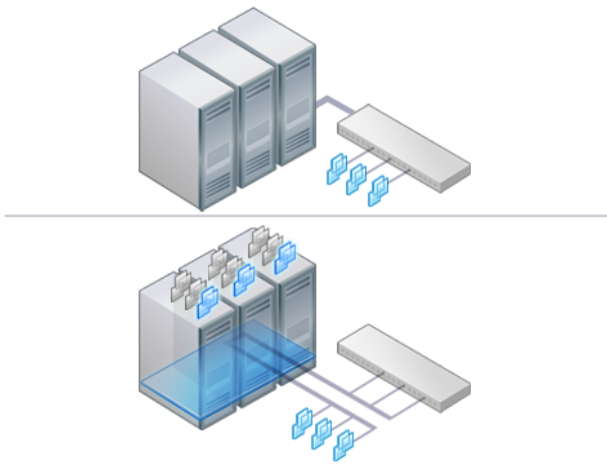
例如，可根据逻辑、组织或网络边界使用 VLAN 对虚拟机区域分段。vShield Manager 利用 Virtual Infrastructure SDK，其清单面板会在 Networks 视图下显示 VLAN 网络视图。您可以为每个 VLAN 网络构建访问规则来隔离虚拟机并丢弃传输到这些计算机的未标记流量。

保护群集中的虚拟机

可以使用 vShield App 保护群集中的虚拟机。

在 图 1–3 中，群集中的每台 ESX 主机上都安装了 vShield App。当通过 vMotion 或 DRS 在群集中的 ESX 主机之间移动虚拟机时，虚拟机仍受保护。每个 vApp 共享和维护所有传输状态。

图 1–3 安装在群集中每个 ESX 主机上的 vShield App 实例



vShield Edge 的常见部署

可以使用 vShield Edge 隔离末端网络，从而使用 NAT 允许流量传入和传出网络。如果部署内部末端网络，可以通过 VPN 通道实现 LAN 到 LAN 的加密，从而利用 vShield Edge 保护网络之间的通信。

vShield Edge 可以部署为 VMware vCloud Director 中的自助应用程序。

vShield App 的常见部署

可以使用 vShield App 在 vDC 中创建安全区域。可以强制在 vCenter 容器或安全组上实施防火墙策略。安全组是可以通过 vShield Manager 用户界面创建的自定义容器。利用基于容器的策略，您可以创建混合的信任区域，而不需要外部物理防火墙。

在不使用 vDC 的部署中，使用带有安全组功能的 vShield App 可创建信任区域并强制实施访问策略。

服务提供程序管理员可以使用 vShield App 在内部网络中的所有客户虚拟机上强制实施广泛的防火墙策略。例如，可以在所有客户虚拟机的第二个 vNIC 上强制实施一个防火墙策略，以允许虚拟机连接到某个存储服务器，但阻止虚拟机访问任意其他虚拟机。

安装准备工作 2

本章概括介绍成功安装 vShield 的先决条件。

本章讨论了以下主题：

系统要求

在 vCenter Server 环境中安装 vShield 之前，请先考虑您的网络配置和资源。您可以在每个 vCenter Server 上安装一个 vShield Manager，在每个 ESX 主机上安装一个 vShield App 或一个 vShield Endpoint，在每个端口组上安装一个 vShield Edge。

硬件

表 2–1 硬件要求

组件	最低
内存	所有 vShield 组件均需要 8 GB
磁盘空间	■ vShield Manager 需要 8 GB ■ 每个 ESX 主机上的每个 vShield App 需要 5 GB ■ 每个 vShield Edge 需要 100 MB ■ 每个 ESX 主机上的 vShield Data Security 需要 6 GB
网卡	所有 vShield 组件需要 ESX 主机上有 2 个千兆位网卡

软件

有关互操作性的最新信息，请参见 http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php 上的产品互操作性列表。

下面列出了 VMware 产品所需的最低版本。

- VMware vCenter Server 4.0 Update 2 或更高版本

- 要求每个服务器安装 VMware ESX 4.0 Update 2 或更高版本

  注意

  - vShield Endpoint 需要安装 ESXi 4.1 Patch 3 或更高版本。
  - vShield Data Security 需要安装 ESXi 4.1 Patch 3 或更高版本。
  - 如果将 vShield App 与 ESXi 5.0 结合使用，则必须安装 ESXi 5.0 Patch 1。

- VMware Tools

  对于 vShield Endpoint 和 vShield Data Security，必须将虚拟机升级到硬件版本 7 或 8，并安装与 ESXi 5.0 Patch 1 一起发行的 VMware Tools 8.6.0。

- VMware vCloud Director 1.0 或更高版本
- VMware View 4.5 或更高版本

客户端和用户访问权限

- 安装了 VMware vSphere Client 的 PC
- 添加和打开虚拟机电源的权限
- 访问存储虚拟机文件的数据存储的权限，以及将文件复制到该数据存储的帐户权限
- 在 Web 浏览器中启用 Cookies 以访问 vShield Manager 用户接口
- 可以使用下列支持的 Web 浏览器之一连接到 vShield Manager：
  - Internet Explorer 6.x 和更高版本
  - Mozilla Firefox 1.x 和更高版本
  - Safari 1.x 或 2.x

部署注意事项

部署 vShield 组件之前，请先考虑以下建议和限制条件。

- 针对 vShield 保护准备虚拟机第 15 页，

  必须确定如何使用 vShield 保护您的虚拟机。最佳做法是应根据您使用的 vShield 组件，为 vShield App、vShield Endpoint 和 vShield Data Security 在资源池中准备好所有 ESX 主机。还必须将虚拟机升级到硬件版本 7 或 8。

- vShield Manager 正常运行时间第 15 页，

  vShield Manager 必须在不受停机（如频繁重新启动或以维护模式运行）影响的 ESX 主机上运行。可以使用 HA 或 DRS 来提高 vShield Manager 的故障恢复能力。如果 vShield Manager 所在的 ESX 主机预计将要停机，请使用 vMotion 将此 vShield Manager 虚拟设备迁移至其他 ESX 主机。因此，建议使用多个 ESX 主机。

- vShield 组件之间的通信第 15 页，

  应将 vShield 组件的管理接口放置在公共网络（如 vSphere 管理网络）中。vShield Manager 必须可以连接到 vCenter Server、vShield App 和 vShield Edge 实例、vShield Endpoint 模块和 vShield Data Security 虚拟机。vShield 组件可以通过路由连接及不同的 LAN 进行通信。

- 强化对 vShield 虚拟机的保护第 15 页，

  可以通过使用基于 Web 的用户界面、命令行界面和 REST API 来访问 vShield Manager 和其他 vShield 组件。vShield 包含上述每个访问选项的默认登录凭据。安装完各 vShield 虚拟机后，应更改默认登录凭据，以强化访问保护。请注意，vShield Data Security 不包含默认的登录凭据。

针对 vShield 保护准备虚拟机

必须确定如何使用 vShield 保护您的虚拟机。最佳做法是应根据您使用的 vShield 组件，为 vShield App、vShield Endpoint 和 vShield Data Security 在资源池中准备好所有 ESX 主机。还必须将虚拟机升级到硬件版本 7 或 8。

请考虑以下问题：

我的虚拟机的分组方式?

您可能会考虑将虚拟机移动到 vDSC 上的端口组中，或移动到其他 ESX 主机上，以将虚拟机按职能、部门或其他组织要求分组，从而提高安全性，并简化访问规则配置。您可以在任意端口组的外围安装 vShield Edge，以将虚拟机与外部网络隔离。您可以在 ESX 主机上安装 vShield App，并为每个容器资源配置防火墙策略，以便根据资源的层次结构执行规则。

使用 vMotion 将我的虚拟机迁移到其他 ESX 主机后，我的虚拟机是否仍受保护?

是的，如果资源池中的主机已准备好，则可以在这些主机之间迁移虚拟机，且不会影响安全状态。有关准备 ESX 主机的信息，请参见第 22 页，“准备所有 ESX 主机”。

vShield Manager 正常运行时间

vShield Manager 必须在不受停机（如频繁重新启动或以维护模式运行）影响的 ESX 主机上运行。可以使用 HA 或 DRS 来提高 vShield Manager 的故障恢复能力。如果 vShield Manager 所在的 ESX 主机预计将要停机，请使用 vMotion 将此 vShield Manager 虚拟设备迁移至其他 ESX 主机。因此，建议使用多个 ESX 主机。

vShield 组件之间的通信

应将 vShield 组件的管理接口放置在公共网络（如 vSphere 管理网络）中。vShield Manager 必须可以连接到 vCenter Server、vShield App 和 vShield Edge 实例、vShield Endpoint 模块和 vShield Data Security 虚拟机。vShield 组件可以通过路由连接及不同的 LAN 进行通信。

注意 vShield Manager 必须与要管理的 vShield 组件位于同一 vCenter Server 环境中。不能跨不同 vCenter Server 环境使用 vShield Manager。

强化对 vShield 虚拟机的保护

可以通过使用基于 Web 的用户界面、命令行界面和 REST API 来访问 vShield Manager 和其他 vShield 组件。vShield 包含上述每个访问选项的默认登录凭据。安装完各 vShield 虚拟机后，应更改默认登录凭据，以强化访问保护。请注意，vShield Data Security 不包含默认的登录凭据。

- vShield Manager 用户界面第 16 页，

  可以通过打开 Web 浏览器窗口并导航到 vShield Manager 管理端口的 IP 地址来访问 vShield Manager 用户界面。

- 命令行界面第 16 页，

  可以通过 vSphere Client 控制台会话使用命令行界面来访问 vShield Manager、vShield App 和 vShield Edge 虚拟设备。要访问 vShield Endpoint 虚拟设备，请参见防病毒解决方案提供商的说明。不能通过使用命令行界面访问 vShield Data Security 虚拟机。

- REST 请求第 16 页，

  所有 REST API 请求都要在 vShield Manager 中进行身份验证。

vShield Manager 用户界面

可以通过打开 Web 浏览器窗口并导航到 vShield Manager 管理端口的 IP 地址来访问 vShield Manager 用户界面。

默认用户帐户 admin 拥有 vShield Manager 的所有访问权限。首次登录后，应该更改 admin 用户帐户的默认密码。请参见第 20 页，“更改 vShield Manager 用户界面默认帐户的密码”。

命令行界面

可以通过 vSphere Client 控制台会话使用命令行界面来访问 vShield Manager、vShield App 和 vShield Edge 虚拟设备。要访问 vShield Endpoint 虚拟设备，请参见防病毒解决方案提供商的说明。不能通过使用命令行界面访问 vShield Data Security 虚拟机。

登录各虚拟设备所用的用户名 (**`admin`**) 和密码 (**`default`**) 与登录 vShield Manager 用户界面所用的用户名和密码相同。进入 Enabled 模式也使用密码 **`default`**。

有关强化 CLI 的详细信息，请参见《vShield 命令行界面参考》。

REST 请求

所有 REST API 请求都要在 vShield Manager 中进行身份验证。

使用 Base 64 编码确定以下格式的“用户名-密码”组合：username:password。必须使用具有访问特权的 vShield Manager 用户界面帐户（用户名和密码）来提交请求。有关 REST API 身份验证请求的详细信息，请参见《vShield API 编程指南》。

安装 vShield Manager 3

VMware vShield 提供防火墙保护、流量分析功能以及网络外围服务来保护 vCenter Server 虚拟基础架构。在大多数虚拟数据中心中，vShield 虚拟设备均已实现自动化安装。

vShield Manager 是 vShield 的集中式管理组件。使用 vShield Manager 可监视并集中配置 vShield App、vShield Endpoint 和 vShield Edge 实例。vShield Manager 在 ESX 主机上作为虚拟设备运行。

VMware vShield 随 VMware ESX 4.0 和 4.1 一起提供。基本的 VMware vShield 软件包中包含 vShield Manager 和 vShield Zones。可以配置 vShield Zones 防火墙规则集来监视 IP 地址与 IP 地址间的通信流量。

vShield Manager 的安装过程是一个多步骤流程。您必须按顺序执行所有任务才能成功安装 vShield Manager。

要强化网络安全状态，可以获取 vShield App、vShield Endpoint 和 vShield Edge 的许可证。

本章讨论了以下主题：

获取 vShield Manager OVA 文件

vShield Manager 虚拟机打包为开放虚拟化设备 (OVA) 文件，这样您便可以使用 vSphere Client 将 vShield Manager 导入到数据存储和虚拟机清单中。

安装 vShield Manager 虚拟设备

可以在配置了 DRS 的群集中的 ESX 主机上安装 vShield Manager 虚拟机。

必须将 vShield Manager 安装到将与之交互操作的 vCenter 中。一个 vShield Manager 服务于一个 vCenter Server 环境。

vShield Manager 虚拟机安装文件中包含 VMware Tools。请勿尝试在 vShield Manager 上升级或安装 VMware Tools。

步骤

1 登录 vSphere Client。

2 创建一个端口组来托管 vShield Manager 的管理接口。

vShield Manager 管理接口必须可供将来所有的 vShield Edge、vShield App 和 vShield Endpoint 实例访问。

注意 请勿将 vShield Manager 的管理接口与服务控制台和 VMkernel 置于同一端口组中。

3 转到 **File > Deploy OVF Template**。

4 单击 **Deploy from file**，然后单击 **Browse**，找到 PC 中 vShield Manager OVA 文件所在的文件夹。

5 完成向导中的操作。

vShield Manager 作为虚拟机安装到清单中。

6 打开 vShield Manager 虚拟机电源。

配置 vShield Manager 的网络设置

必须使用 vShield Manager 的命令行界面 (CLI) 来配置 IP 地址、识别默认网关以及设置 DNS 设置。

最多可以指定两个 DNS 服务器，以供 vShield Manager 解析 IP 地址和主机名称。如果通过使用主机名称（而不是 IP 地址）添加了 vCenter Server 环境中的任意 ESX 主机，则需要 DNS。

步骤

1 右键单击 vShield Manager 虚拟机，然后单击 **Open Console** 打开 vShield Manager 的命令行界面 (CLI)。

引导过程可能会持续几分钟。

2 显示 `manager login` 提示后，使用用户名 **`admin`** 和密码 **`default`** 登录 CLI。

3 使用密码 **`default`** 进入 Enabled 模式。

```
manager> enable
Password:
manager#
```

4 运行 `setup` 命令打开 CLI setup 向导。

CLI setup 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 地址必须可供所有已安装的 vShield App、vShield Edge 和 vShield Endpoint 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 '[]'.

IP Address (A.B.C.D):
Subnet Mask (A.B.C.D):
Default gateway (A.B.C.D):
Primary DNS IP (A.B.C.D):
Secondary DNS IP (A.B.C.D):
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.

manager> exit
manager login:
```

5 登录 CLI。

6 对默认网关执行 Ping 操作，验证网络连通性。

```
manager> ping A.B.C.D
```

7 在 PC 中，对 vShield Manager 的 IP 地址执行 ping 命令，验证是否可以访问 IP 地址。

登录 vShield Manager 用户界面

安装并配置 vShield Manager 虚拟机后，登录 vShield Manager 用户界面。

步骤

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

vShield Manager 用户界面在 SSL 会话中打开。

2 接受安全证书。

注意 可以使用 SSL 证书进行身份验证。请参见《vShield 管理指南》。

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。

应首先更改默认密码，以防止未授权的使用。请参见第 20 页，“更改 vShield Manager 用户界面默认帐户的密码”。

4 单击 **Log In**。

使 vShield Manager 与 vCenter Server 同步

与 vCenter Server 同步后，可在 vShield Manager 用户界面中显示 VMware Infrastructure 清单。

必须拥有具备管理权限的 vCenter Server 用户帐户才能完成此任务。

注意 vShield Manager 虚拟机不会作为资源显示在 vShield Manager 用户界面的清单面板中。**Settings & Reports** 对象代表清单面板中的 vShield Manager 虚拟机。

步骤

1 登录 vShield Manager。

2 单击 vShield Manager 清单面板中的 **Settings & Reports**。

3 单击 **Configuration** 选项卡。

4 单击 **vCenter** 选项卡。

5 在 **IP address/Name** 字段中键入 vCenter Server 的 IP 地址或主机名。

6 在 **User Name** 字段中键入 vSphere Client 登录用户名。

7 在 **Password** 字段中键入与用户名关联的密码。

8 单击 **Save**。

在 vSphere Client 中注册 vShield Manager 插件

使用 **vSphere Plug-in** 选项，可以作为 vSphere Client 插件注册 vShield Manager。在注册插件之后，可以从 vSphere Client 配置大部分 vShield 选项。

步骤

1 单击 vShield Manager 清单面板中的 **Settings & Reports**。

2 单击 **Configuration** 选项卡。

3 单击 **vSphere Plug-in**。

4 单击 **Register**。

5 如果已登录 vSphere Client，请注销。

6 登录 vSphere Client。

7 选择 ESX 主机。

8 确认 **vShield** 选项卡作为一个选项显示。

更改 vShield Manager 用户界面默认帐户的密码

可以更改 admin 帐户的密码，来强化对 vShield Manager 的访问保护。

步骤

1 登录 vShield Manager 用户界面。

2 单击 vShield Manager 清单面板中的 **Settings & Reports**。

3 单击 **Users** 选项卡。

4 选择 admin 帐户。

5 单击 **Update User**。

6 输入新密码。

7 在 **Retype Password** 字段中再次键入该密码进行确认。

8 单击 **OK** 保存更改。

安装 vShield Edge、vShield App、vShield Endpoint 和 vShield Data Security

4

安装 vShield Manager 后，可以获取许可证来激活 vShield App、vShield Endpoint、vShield Edge 和 vShield Data Security 组件。vShield Manager OVA 软件包中包含安装这些加载项组件所需的驱动程序和文件。通过 vShield App 许可证，您也可以使用 vShield Endpoint 组件。

本章讨论了以下主题：

在评估模式下运行 vShield 许可组件

在为 vShield Edge、vShield App 和 vShield Endpoint 购买并激活许可证之前，可以在评估模式中安装和运行软件。评估模式用于演示和评估目的。在此模式下，vShield Edge、vShield App 和 vShield Endpoint 在安装后便可正常运行，不需要进行任何许可配置，在首次激活后可以正常运行 60 天。

以评估模式运行时，vShield 组件能够支持允许的最大数量的实例。

在 60 天试用期过后，除非获得软件许可证，否则您将无法再继续使用 vShield。例如，您将不能打开 vShield App 或 vShield Edge 虚拟设备的电源或保护您的虚拟机。

要继续正常使用 vShield App 和 vShield Edge 功能或者恢复在 60 天试用期过后无法使用的功能，您需要获取并安装许可证文件，激活所购买 vShield 组件的相应功能。

为 vShield App、vShield Edge、vShield Endpoint 和 vShield Data Security 准备 Virtual Infrastructure

在安装这些加载项组件之前，需要准备好 ESX 主机和 vNetwork 环境。vShield App、vShield Endpoint 和 vShield Data Security 组件需要安装在 ESX 主机上。vShield Edge 组件需要安装在端口组、vNetwork Distributed Switch (vDS) 端口组或 Cisco® Nexus 1000V 上。

安装 vShield 组件许可证

安装 vShield Edge、vShield App 和 vShield Endpoint 组件之前，必须为其安装许可证。可以在使用 vSphere Client 完成 vShield Manager 安装后，安装这些许可证。通过 vShield App 许可证，您也可以使用 vShield Endpoint 组件。

步骤

1 在与 vCenter Server 系统连接的某个 vSphere Client 主机中，选择 **Home > Licensing**。

2 在报告视图中，选择 **Asset**。

3 右键单击一项 vShield 资产，然后选择 **Change license key**。

4 选择 **Assign a new license key**，然后单击 **Enter Key**。

5 输入许可证密钥，输入密钥的可选标签，然后单击 **OK**。

6 单击 **OK**。

7 针对拥有许可证的每一项 vShield 组件重复以上步骤。

准备所有 ESX 主机

您应当针对 vShield 加载项功能组件准备 vCenter 环境中的所有 ESX 主机。

准备 ESX 主机时需用到以下信息：

- 一个针对每个 vShield App 虚拟设备的管理 (MGMT) 端口的 IP 地址。每个 IP 地址都应可以从 vShield Manager 访问，并且应位于 vCenter 和 ESX 主机管理接口所用的管理网络中。
- 用于放置 vShield App 的本地或网络存储。

vShield 虚拟设备中包含 VMware Tools。请勿尝试更改或升级 vShield 虚拟设备上的 VMware Tools 软件。

步骤

1 登录 vSphere Client。

2 在清单树中选择一个 ESX 主机。

3 单击 **vShield** 选项卡。

4 接受安全证书。

5 对 **vShield App** 服务单击 **Install**。

下一个屏幕将开始安装所有三种服务。

6 在 vShield App 下，输入以下信息。

选项	描述
Datastore	选择用来存储 vShield App 虚拟机文件的数据存储区。
Management Port Group	选择用于托管 vShield App 的管理接口的端口组。该端口组必须能够访问 vShield Manager 的端口组。
IP Address	键入要分配给 vShield App 的管理接口的 IP 地址。
Netmask	键入与分配的 IP 地址关联的 IP 子网掩码。
Default Gateway	键入默认网络网关的 IP 地址。

7 选中 **vShield Endpoint** 复选框。

8 单击表单顶部的 **Install**。

可以按照 vSphere Client 屏幕的 Recent Tasks 窗格中的 vShield App 安装步骤操作。

9 安装完所有组件后，执行以下操作：

- vShield App：此时 vShield App 安装已经完成。转至数据中心、群集或端口组容器级的 **vShield App > App Firewall** 选项卡以配置防火墙规则。每个 vShield App 都将继承 vShield Manager 中的全局防火墙规则集。默认防火墙规则集允许所有流量通过。您必须配置阻止规则才能明确阻止流量。要配置 App Firewall 规则，请参阅《vShield 管理指南》。
- vShield Endpoint：要完成安装，请参见第 24 页，“安装 vShield Endpoint”。
- vShield Data Security：要完成安装，请参见第 25 页，“安装 vShield Data Security”。

安装 vShield Edge

每个 vShield Edge 虚拟设备都具有外部和内部网络接口。内部接口连接至安全的端口组，并充当端口组中所有受保护虚拟机的网关。分配给内部接口的子网掩码可以是 RFC 1918 私有地址。vShield Edge 的外部接口连接至上行链路端口组，后者可以访问共享企业网络或提供访问层联网功能的服务。

每个 vShield Edge 要求至少具有一个 IP 地址来对外部接口进行编号。可以为负载平衡器、点对点 VPN 和 NAT 服务配置多个外部 IP 地址。内部接口可以使用与其他受 vShield Edge 保护的端口组重叠的私有 IP 地址块。

您可以在每个端口组、每个 vDS 端口组或每个 Cisco® Nexus 1000V 上安装一个 vShield Edge。

如果启用了 DRS 和 HA，将可以动态迁移 vShield Edge。

步骤

1 登录 vSphere Client。

2 转到 **View > Inventory > Networking**。

3 在 vDS 上，创建一个端口组。

此端口组为内部端口组。

4 将一个租户的客户虚拟机移动到内部端口组上。

5 选择新的内部端口组。

6 单击 **Edge** 选项卡。

7 在 **Network Interfaces** 下，输入以下信息。

选项	描述
外部	
Port Group	选择 vDS 中的外部端口组。该端口组托管物理网卡，并连接至外部网络。
IP Address	输入外部端口组的 IP 地址。
Subnet Mask	键入与分配的外部 IP 地址关联的 IP 子网掩码。
Default Gateway	键入默认网络网关的 IP 地址。
内部	
Port Group	这是所选的内部端口组。
IP Address	键入内部端口组的 IP 地址。
Subnet Mask	键入与分配的内部 IP 地址关联的 IP 子网掩码。

8 在 **Edge deployment resource selection** 中，输入以下信息。

选项	描述
Resource Pool	选择要部署 vShield Edge 的资源池。
Host	选择数据存储驻留的 ESX 主机。
Datastore	选择用来存储 vShield Edge 虚拟机文件的数据存储。

9 单击 **Install**。

安装完成后，配置服务和防火墙规则来保护安全端口组中的虚拟机。要配置 vShield Edge，请参阅《vShield 管理指南》。

安装 vShield Endpoint

以下安装说明假定您拥有以下系统：

- 群集中每个 ESX 主机上均安装了受支持版本的 vCenter Server 和 ESXi 的数据中心。有关所需版本的信息，请参见第 13 页，第 2 章“安装准备工作”。
- 安装了并正在运行 vShield Manager 5.0。
- 安装了并正在运行防病毒解决方案管理服务器。

vShield Endpoint 安装工作流程

为安装 vShield Endpoint 准备好 ESX 主机后，按以下步骤安装 vShield Endpoint：

1 根据防病毒解决方案提供商的说明，为每个 ESX 主机部署并配置一个安全虚拟机 (SVM)。

2 在所有要受保护的虚拟机上安装与 ESXi 5.0 Patch 1 一起发布的 VMware Tools 8.6.0。

在客户机虚拟机上安装 VMware Tools

VMware Tools 必须安装在要受到保护的每台客户机虚拟机上。在安装了安全解决方案的 ESX 主机上启动已安装 VMware Tools 的虚拟机后，所启动的虚拟机会自动得到保护。这意味着受保护的虚拟机在关机和重启后仍可以得到安全保护，当通过 vMotion 迁移到另一个安装了安全解决方案的 ESX 主机时也不例外。

前提条件

- 确保客户机虚拟机安装了支持的 Windows 版本。vShield Endpoint 5.0 支持的 Windows 操作系统版本包括：
  - Windows Vista（32 位）
  - Windows 7（32/64 位）
  - Windows XP（32 位）
  - Windows 2003（32/64 位）
  - Windows 2003 R2（32/64 位）
  - Windows 2008（32/64 位）
  - Windows 2008 R2（64 位）

步骤

1 安装包位于您下载 ESXi 5.0 Patch 1 的 VMware 客户网站上。

2 将安装包下载到您的 PC 上，然后进行解压。

3 打开客户机虚拟机上的控制台窗口。

4 单击 **CD/DVD drive 1 > Connect to ISO image on local disk**。

5 单击 **Browse** 以找到 PC 中 VMware Tools ISO 文件所在的文件夹。

6 完成向导中的操作。如果选择执行自定义安装，则必须选择要安装的 vShield 驱动程序。

VMware Tools 必须安装在要受到保护的每台客户机虚拟机上。

vShield Endpoint 主机组件将两个防火墙规则添加到 ESX 主机：

- vShield-Endpoint-Mux 规则打开端口 48651 到端口 48666，以供主机组件和合作伙伴安全虚拟机之间进行通信。
- 合作伙伴可以使用 vShield-Endpoint-Mux-Partners 规则来安装主机组件。默认情况下，该规则已禁用。

安装 vShield Data Security

只有安装 vShield Endpoint 后才能安装 vShield Data Security。

前提条件

验证主机和客户机虚拟机上是否已安装 vShield Endpoint。

步骤

1 登录 vSphere Client。

2 在清单树中选择一个 ESX 主机。

3 单击 **vShield** 选项卡。

4 单击 vShield Data Security 旁边的 **Install**。

5 选中 **vShield Data Security** 复选框。

6 在 vShield Data Security 下，输入以下信息。

选项	描述
Datastore	选择要添加 vShield Data Security 服务虚拟机的数据存储。
Management Port Group	选择用于托管 vShield Data Security 的管理接口的端口组。该端口组必须能够访问 vShield Manager 的端口组。
Control IP	vShield 会自动填充。

7 要配置静态 IP，请选中 **Configure static IP for management interface** 复选框。

输入 **IP address**、**Netmask** 和 **Default Gateway** 详细信息。

注意 如果未选择 **Configure static IP for management interface**，则会使用动态主机配置协议 (DHCP) 分配 IP 地址。

8 单击 **Install**。

vShield Data Security 虚拟机将安装在所选主机上。

升级 vShield

5

要升级 vShield，必须先升级 vShield Manager，然后升级其他具有许可证的组件。

本章讨论了以下主题：

升级 vShield Manager

可以仅从 vShield Manager 用户界面将 vShield Manager 升级到新版本。可以从 vShield Manager 用户界面或通过使用 REST API 将 vShield App、vShield Edge 和 vShield Endpoint 升级到新版本。

步骤

1 将 vShield 升级捆绑包下载到 vShield Manager 可浏览到的位置。

升级捆绑包文件的名称类似于 `VMware-vShield-Manager-upgrade_bundle-`*`buildNumber`*`.tar.gz.`。

2 从 vShield Manager 清单面板中，单击 **Settings & Reports**。

3 单击 **Updates** 选项卡。

4 单击 **Upload Settings**。

5 单击 **Browse**，然后选择 `VMware-vShield-Manager-upgrade_bundle-`*`buildNumber`*`.tar.gz.` 文件。

6 单击 **Open**。

7 单击 **Upload File**。

8 单击 **Install** 以开始升级过程。

9 单击 **Confirm Install**。

升级过程将重新引导 vShield Manager，因此您可能会失去与 vShield Manager 用户界面的连接。不会重新引导其他任何 vShield 组件。

10 右键单击 vShield Manager 虚拟机，然后单击 **Open Console** 打开 vShield Manager 命令行界面 (CLI)。

11 看到 **e1000_watchdog_task:NIC Link is up** 消息后，登录到 vShield Manager 用户界面。

12 单击 **Updates** 选项卡。

Installed Release 面板将显示刚安装的 vShield 版本的内部版本号。

下一步

重新启动 vSphere Client。

升级 vShield App

升级数据中心中每个主机上的 vShield App。

步骤

1 登录 vSphere Client。

2 转至 **Inventory > Hosts and Clusters**。

3 选择要在其上升级 vShield App 的主机。

Summary 选项卡显示选定主机上安装的每个 vShield 组件以及可用版本。

4 选择 vShield App 旁边的 **Update**。

5 选中 **vShield App** 复选框。

6 单击 **Install**。

升级 vShield Edge

升级数据中心中每个端口组上的 vShield Edge。

步骤

1 登录 vSphere Client。

2 转至 **Views > Inventory > Networking**。

3 单击 **vShield Edge** 选项卡。

4 单击 **Upgrade**。

5 选择 **vShield Edge**。

6 单击 **Install**。

升级 vShield Endpoint

要将 vShield Endpoint 升级到较新版本，必须首先卸载数据中心的每个主机上的 vShield Endpoint，然后安装新版本。

要卸载 vShield Endpoint，请参见《vShield 管理指南》中的“卸载 vShield Endpoint 模块”。

要安装 vShield Endpoint，请参见第 24 页，“安装 vShield Endpoint”。

升级 vShield Data Security

升级数据中心中每个主机上的 vShield Data Security。

步骤

1 登录 vSphere Client。

2 转至 **Inventory > Hosts and Clusters**。

3 选择要在其上升级 vShield App 的主机。

Summary 选项卡显示选定主机上安装的每个 vShield 组件以及可用版本。

4 选择 vShield Data Security 旁边的 **Update**。

5 选中 **vShield Data Security** 复选框。

6 单击 **Install**。

索引

X

Y

Z