



趋势科技服务器深度 安全防护系统 8.0

SP1 入门和安装指南

趋势科技（中国）有限公司保留对本文档以及此处所述产品进行更改而不通知的权利。在安装及使用本软件之前，请阅读自述文件、发布说明和最新版本的适用用户文档，这些文档可以通过趋势科技的以下 Web 站点获得：

<http://www.trendmicro.com/download/zh-cn/>

Trend Micro、Trend Micro 地球徽标、Deep Security 和 TrendLabs 是趋势科技（中国）有限公司/Trend Micro Incorporated 的商标或注册商标。所有其他产品或公司名称可能是其各自所有者的商标或注册商标。

版权所有 © 2012 趋势科技（中国）有限公司/Trend Micro Incorporated。保留所有权利。

文档编号：APCM85395/120425

发布日期：2012 年 4 月

版本：1.3 (SP1)

趋势科技服务器深度安全防护系统的用户文档介绍了软件的主要功能以及针对生产环境的安装说明。请在安装或使用软件之前通读本文档。

趋势科技 Web 站点中的联机帮助和联机知识库提供了有关如何使用软件内特定功能的详细信息。

趋势科技一直致力于改进其文档。如对该文档或趋势科技的任何其他文档有任何问题、意见或建议，请通过 service@trendmicro.com.cn 与我们联系。我们始终欢迎您的反馈。

目录

目录.....	iii
前言.....	ix
前言.....	ix
联系趋势科技.....	ix
关于趋势科技.....	ix
趋势科技服务器深度安全防护系统文档.....	x
入门.....	11
简介.....	11
软件组件.....	12
趋势科技服务器深度安全防护系统防护模块.....	14
云安全智能防护网络.....	17
虚拟环境中的防恶意软件防护.....	18
趋势科技服务器深度安全防护系统 8.0 (SP1) 中的新增功能.....	18
趋势科技服务器深度安全防护系统 8.0 中的新增功能.....	19
虚拟环境中的无客户端防护快速入门指南.....	22
准备 VMware 环境.....	23
安装数据库以供趋势科技服务器深度安全防护系统管理中心使用... ..	23
部署趋势科技服务器深度安全防护系统环境.....	23
在虚拟机上启用防护.....	24

客户端防护快速入门指南	25
安装数据库以供趋势科技服务器深度安全防护系统管理中心使用	25
部署趋势科技服务器深度安全防护系统环境	25
在计算机上启用防护	25
混合环境中防护的快速入门指南	26
虚拟设备和使用趋势科技服务器深度安全防护系统客户端的协调 方法	26
趋势科技服务器深度安全防护系统 — 安装指南	29
系统要求	29
趋势科技服务器深度安全防护系统管理中心系统要求	29
趋势科技服务器深度安全防护系统中继系统要求	30
趋势科技服务器深度安全防护系统虚拟设备的 ESX/ESXi 要求	30
趋势科技服务器深度安全防护系统虚拟设备系统要求	30
趋势科技服务器深度安全防护系统客户端系统要求	31
趋势科技服务器深度安全防护系统通知程序系统要求	31
准备	32
所需条件	32
性能建议	35
高可用性环境	36
所需资源核对清单	37
为无客户端防护准备 VMware 环境	38
建议的环境 — 概述	38
最低要求	39
所需资源核对清单	40
服务器准备	41
客户虚拟机操作系统准备	43
为趋势科技服务器深度安全防护系统管理中心安装数据库	45
数据库磁盘空间	45
帐户详细信息	46
安装趋势科技服务器深度安全防护系统管理中心	47
复制安装包	47
安装适用于 Windows 的趋势科技服务器深度安全防护系统管理 中心	47
安装适用于 Linux 的趋势科技服务器深度安全防护系统管理中心	50
运行趋势科技服务器深度安全防护系统管理中心	50

趋势科技服务器深度安全防护系统中继配置.....	50
趋势科技服务器深度安全防护系统管理中心静默安装.....	51
部署趋势科技服务器深度安全防护系统中继.....	52
准备.....	52
复制安装包.....	53
安装适用于 Windows 的趋势科技服务器深度安全防护系统中继.....	53
安装适用于 Linux 的趋势科技服务器深度安全防护系统中继.....	54
间隙环境中的趋势科技服务器深度安全防护系统中继和组件更新... ..	55
VMware 集成的其他配置.....	57
为趋势科技服务器深度安全防护系统虚拟设备部署准备 ESX/ESXi.....	59
将趋势科技服务器深度安全防护系统软件包导入到 DSM 中.....	59
通过安装过滤器驱动程序为虚拟设备部署准备 ESX/ESXi.....	60
部署趋势科技服务器深度安全防护系统虚拟设备.....	62
增加 DSVA 内存（可选）.....	64
对 DSVA 禁用 DRS 和 HA.....	64
激活趋势科技服务器深度安全防护系统虚拟设备.....	65
激活客户虚拟机.....	66
自动为无状态 ESXi 部署设备.....	67
安装 TFTP Server.....	67
安装 VMware Auto-deploy.....	67
为 PXE 配置 DHCP Server.....	68
将趋势科技服务器深度安全防护系统过滤器驱动程序添加到 VIB 镜像.....	68
安装 vSphere PowerCLI.....	68
准备第一个镜像.....	69
将新镜像添加到库中.....	69
部署第一个主机.....	70
配置主机配置文件.....	71
部署趋势科技服务器深度安全防护系统客户端.....	73
准备.....	73
复制安装包.....	73
安装适用于 Windows 的趋势科技服务器深度安全防护系统客户端.....	74
安装适用于 Linux 的趋势科技服务器深度安全防护系统客户端.....	75
安装适用于 Solaris 的趋势科技服务器深度安全防护系统客户端.....	77
安装适用于 AIX 的趋势科技服务器深度安全防护系统客户端.....	83
安装适用于 HP-UX 的趋势科技服务器深度安全防护系统客户端.....	83

安装趋势科技服务器深度安全防护系统通知程序84

- 复制安装包84
- 无客户端通知程序的 VMCI 设置84
- 安装适用于 Windows 的趋势科技服务器深度安全防护系统通知程序85

基本趋势科技服务器深度安全防护系统配置86

- 配置电子邮件通知86
- 创建角色和用户帐户87
- 配置趋势科技服务器深度安全防护系统中继87
- 向趋势科技服务器深度安全防护系统管理中心添加计算机89
- 在计算机上启用防护89
- 基本防火墙配置90
- Java 安全性91

升级93

升级方案93

升级趋势科技服务器深度安全防护系统 8.0 软件组件95

- 升级趋势科技服务器深度安全防护系统管理中心95
- 远程升级趋势科技服务器深度安全防护系统组件95
- 手动升级趋势科技服务器深度安全防护系统中继96
- 手动升级趋势科技服务器深度安全防护系统客户端96

从具有无客户端防恶意软件的 DS 7.5 升级（维持 ESX/ESXi 4.1）98

- 阶段一：升级 VMware 组件98
- 阶段二：升级趋势科技服务器深度安全防护系统组件99

从具有无客户端防恶意软件的 DS 7.5 升级（将 ESX/ESXi 4.1 升级到 5.0） 101

- 升级过程摘要 101
- 阶段一：升级 VMware 组件 103
- 阶段二：升级趋势科技服务器深度安全防护系统组件 104

从仅具有无客户端防火墙和 DPI 的 DS 7.5 升级（维持 ESX/ESXi 4.1） 107

- 阶段一：升级 VMware 组件 107
- 阶段二：升级趋势科技服务器深度安全防护系统组件 108

从仅具有无客户端防火墙和 DPI 的 DS 7.5 升级（将 ESX/ESXi 4.1 升级到 5.0）	110
升级过程摘要	110
阶段一：升级 VMware 组件	111
阶段二：升级趋势科技服务器深度安全防护系统组件	112
从仅具有基于客户虚拟机客户端的防护的趋势科技服务器深度安全防护系统 7.5 升级	114
升级过程	114
趋势科技服务器深度安全防护系统管理中心设置属性文件	117
设置属性文件	117
安装输出	125
趋势科技服务器深度安全防护系统管理中心内存使用	127
趋势科技服务器深度安全防护系统虚拟设备内存使用	129
性能功能	131
性能配置文件	131
磁盘空间不足警报	132
创建 SSL 认证证书	133
与客户端和设备版本的互操作性	137
故障排除	139
趋势科技服务器深度安全防护系统管理中心	139
趋势科技服务器深度安全防护系统虚拟设备	143
趋势科技服务器深度安全防护系统客户端	144
诊断信息收集	148
FAQ	149

已知不兼容软件.....	153
卸载趋势科技服务器深度安全防护系统.....	155
删除趋势科技服务器深度安全防护系统虚拟设备	155
从准备好的 ESX/ESXi 移除趋势科技服务器深度安全防护系统 过滤器驱动程序	156
卸载趋势科技服务器深度安全防护系统中继	156
卸载趋势科技服务器深度安全防护系统客户端	157
卸载趋势科技服务器深度安全防护系统通知程序	159
卸载趋势科技服务器深度安全防护系统管理中心	159
部署 DSA 所需的最低 VMware 权限.....	161
准备 ESX/ESXi 主机	163
部署虚拟设备	163
激活虚拟机（受保护的计算机）	164
持续的操作	164



前言

欢迎使用《趋势科技™ 服务器深度安全防护系统入门和安装指南》。本指南介绍了趋势科技服务器深度安全防护系统，可以协助进行部署、安装、升级、初始配置和故障排除，从而帮助您开始使用该系统。

联系趋势科技

有关趋势科技的联系信息，请访问趋势科技支持 Web 站点：

<http://www.trendmicro.com.cn/corporate/techsupport/solutionbank/>

关于趋势科技

趋势科技（中国）有限公司/Trend Micro Incorporated 是网络防病毒和 Internet 内容安全软件和服务方面的全球领导者，通过其获奖的趋势科技企业防护策略，专注于帮助客户防止和最大程度降低网络病毒和混合威胁攻击的影响。趋势科技具有全球运营业务，在东京证券交易所和 NASDAQ 具有交易股票。

趋势科技服务器深度安全防护系统文档

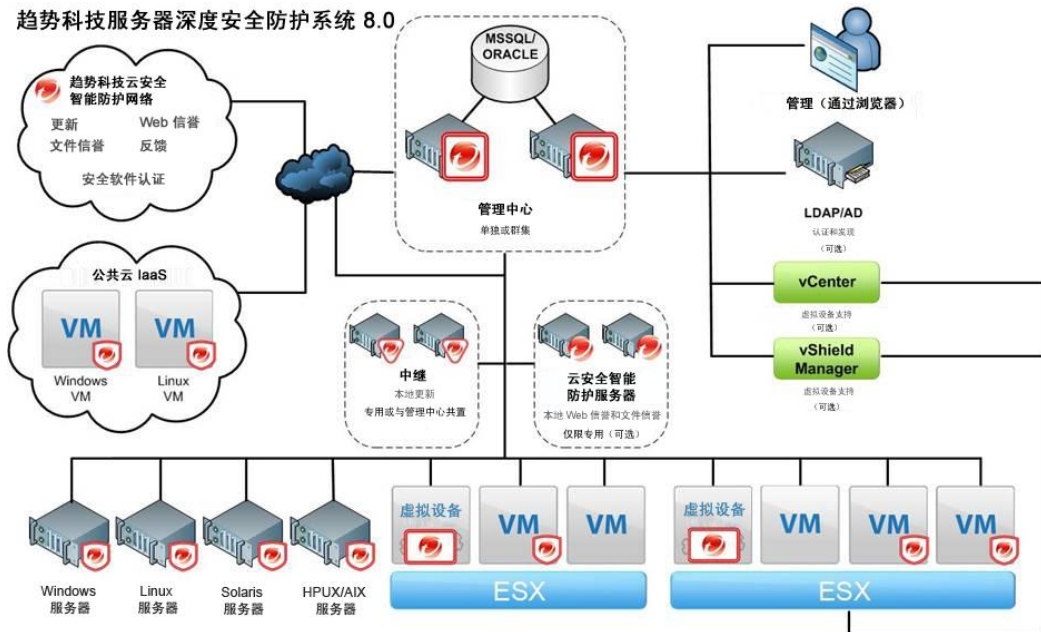
文档	描述
入门和安装指南	PDF 文档，讨论如何开始使用趋势科技服务器深度安全防护系统以及安装和升级趋势科技服务器深度安全防护系统的要求和过程。
管理员指南	PDF 文档，提供有关主要产品任务的“方法教学”信息、用法建议、参考数据以及文本框特定信息，例如有效参数范围和最佳值。
联机帮助	提供有关主要产品任务的“方法教学”信息、用法建议、参考数据以及文本框特定信息，例如有效参数范围和最佳值。
自述文件	包含已知问题列表和基本安装步骤。还可能包含帮助或印刷文档中没有的最新产品信息。
知识库	包括问题解决和疑难解答信息的联机数据库。提供已知产品问题的最新信息。要访问知识库，请转至以下 Web 站点： http://cn.trendmicro.com/cn/support/techsupport/index.htm

第 1 章

入门

简介

趋势科技服务器深度安全防护系统 8.0



高级防护

趋势科技™ 服务器深度安全防护系统 8.0 提供了对动态数据中心中的系统（范围遍及虚拟桌面到物理、虚拟或云服务器）的高级保护。趋势科技服务器深度安全防护系统提供了全面的防护，其中包括：

- 防恶意软件
- Web 信誉
- 防火墙
- DPI
 - 入侵检测和阻止 (IDS/IPS)
 - Web 应用程序防护
 - 应用程序控制
- 完整性监控
- 日志审查

趋势科技服务器深度安全防护系统与趋势科技云安全智能防护网络基础架构集成，从云提供高级防护。云安全智能防护网络为趋势科技服务器深度安全防护系统提供了 Web 信誉技术、安全软件认证服务（文件信誉），并从趋势科技服务器深度安全防护系统收集威胁信息反馈。

软件组件

趋势科技服务器深度安全防护系统包含以下一组组件，这些组件协同起来提供防护：

- **趋势科技服务器深度安全防护系统管理中心**，是管理员用来配置安全策略并向以下执行组件部署防护的集中式管理组件：趋势科技服务器深度安全防护系统虚拟设备和趋势科技服务器深度安全防护系统客户端。
- **趋势科技服务器深度安全防护系统虚拟设备**是针对 VMware™ vSphere™ 环境构建的安全虚拟机，可提供防恶意软件、IDS/IPS、防火墙、Web 应用程序防护和应用程序控制防护。

- **趋势科技服务器深度安全防护系统客户端**是一种直接部署在计算机上的安全客户端，可以提供 IDS/IPS、防火墙、Web 应用程序防护、应用程序控制、完整性监控和日志审查防护。
- **趋势科技服务器深度安全防护系统中继**，将趋势科技服务器深度安全防护系统更新从趋势科技全局更新服务器传递到趋势科技服务器深度安全防护系统组件。始终至少需要一个趋势科技服务器深度安全防护系统中继才能将更新转发到趋势科技服务器深度安全防护系统管理中心（DPI 规则）。获取防恶意软件组件更新（特征码和引擎组件）时，客户端和设备可以使用趋势科技服务器深度安全防护系统中继改善性能。趋势科技服务器深度安全防护系统中继还包含上述全部趋势科技服务器深度安全防护系统客户端功能。
- **趋势科技服务器深度安全防护系统通知程序**是一个 Windows 系统托盘应用程序，用于向受保护计算机的用户显示安全通知。它还会在趋势科技服务器深度安全防护系统阻止恶意软件或阻止对 Web 页的访问时提供弹出式用户通知。该通知程序可以在由虚拟设备保护的计算机上独立安装。在 Windows 上，它在缺省情况下自动随趋势科技服务器深度安全防护系统中继和趋势科技服务器深度安全防护系统客户端一起安装。

趋势科技服务器深度安全防护系统还与**云安全智能防护服务器**集成，从而连接到趋势科技云安全智能防护网络，向趋势科技服务器深度安全防护系统客户端和设备提供 Web 和文件信誉服务。

趋势科技服务器深度安全防护系统防护模块

下表标识了趋势科技服务器深度安全防护系统虚拟设备、趋势科技服务器深度安全防护系统客户端或两者同时提供的防护模块：

	趋势科技服务器 深度安全防护系统 虚拟设备 (8.0)	趋势科技服务器深度安全防护系统 客户端 (8.0)			
		Windows™	Linux	Solaris™	HP- UX™、 AIX™
防恶意软件	是	是	是	否	否
Web 信誉	是	是	否	否	否
防火墙	是	是	是	是	否
深度包检查： IDS/IPS 应用程序 控制 Web 应用程序 防护	是	是	是	是	否
完整性监控	是	是	是	是	是
日志审查	否	是	是	是	是

有关受支持功能、平台和版本的更多详细信息，请参阅《趋势科技服务器深度安全防护系统 8.0 SP1 管理员指南》或联机帮助的[参考](#)一节中的“平台支持的功能”表。

防恶意软件

防恶意软件针对基于文件的威胁提供实时和按需防护，其中包括通常称为恶意软件、病毒、特洛伊木马和间谍软件的那些威胁。

为了识别威胁，防恶意软件会针对整个威胁数据库检查文件，其中的某些部分在趋势科技服务器深度安全防护系统中将作为可更新特征码在本地进行保留。防恶意软件还检查文件是否有某些特征，如压缩和已知的入侵代码。

为解决威胁，防恶意软件会在对系统的损害降至最低的情况下，选择性地执行可包含和移除威胁的操作。防恶意软件可以清除、删除或隔离恶意文件。它还可以终止进程并删除与已识别威胁关联的其他系统对象。

趋势科技服务器深度安全防护系统虚拟设备目前支持对 VMware vSphere™ 环境内的虚拟机的防恶意软件防护。

趋势科技服务器深度安全防护系统客户端目前支持对 Windows 计算机（物理或虚拟）的防恶意软件防护。

趋势科技服务器深度安全防护系统管理中心的防恶意软件模块目前支持：

- 使用 VMware vShield Endpoint 执行无客户端防恶意软件防护
- 对 vSphere 上运行的活动虚拟机的防护
- 适用于安全配置文件和虚拟机的高度可定制防恶意软件配置
- 实时手动预设扫描
- 使用趋势科技云安全智能防护网络
- 隔离文件管理，包括从趋势科技服务器深度安全防护系统管理中心下载和删除
- 内置到控制面板 widget 和报告中的防恶意软件支持
- 从趋势科技服务器深度安全防护系统管理中心集成防恶意软件 Web 服务

Web 信誉

Web 信誉基于 Web 页面的信誉评估来阻止 Web 页面。它查询趋势科技服务器来获取评估，这些评估是从多个来源收集的，包括 Web 页面链接、域和 IP 地址关系、垃圾邮件源和垃圾邮件中的链接。通过联机获取评估，Web 信誉使用最新的可用信息来阻止有害页面。

防火墙

防火墙定义允许或拒绝哪些流量进出受保护的计算机。可以根据协议、端口使用、流量方向、使用的接口和主机标识等触发器的组合来应用防火墙规则。由于它是状态防火墙，因此还可以实施规则来防御各种侦察扫描和拒绝服务攻击。

可以通过安装趋势科技服务器深度安全防护系统客户端在物理计算机和虚拟机上实施防火墙防护。

还可以通过在托管 VM 的 VMware ESX/ESXi™ 虚拟机监控程序上安装趋势科技服务器深度安全防护系统虚拟设备来保护 VMware 环境中的虚拟机。通过虚拟设备，无需安装客户端便可以为 VM 提供防火墙防护。可以通过同时在 VM 上安装客户端来增强防护（“协调方法”）。客户端将提供主要防护，虚拟设备作为后援防护。

深度包检查 (DPI)

深度包检查分析进出计算机的网络流量的实际内容。DPI 规则用于找到伪装成合法流量的攻击。这些规则可以阻止包含旨在利用计算机上特定应用程序和操作系统漏洞的内容的流量。

DPI 规则通过保护漏洞不受已知和未知攻击来提供入侵检测和阻止 (IDS/IPS) 防护。DPI 规则还通过一组 Web 应用程序防护规则来保护 Web 应用程序中的漏洞（如跨站点脚本 (XSS) 和 SQL 注入）。通过检测已知的应用程序流量（在企业环境中可能需要限制），DPI 规则还可以用于向计算机提供应用程序控制。

持续的趋势科技服务器深度安全防护系统规则更新会自动提供最新的全面防护，以抵御已知和未知攻击。

可以通过在计算机上安装客户端在物理计算机和虚拟机上实施 DPI 防护。

DPI 可以仅使用虚拟设备保护虚拟机，您也可以使用协调方法，同时使用虚拟设备和客户端来保护计算机。

完整性监控

完整性监控模块用于监控对系统中指定区域（某些文件、注册表值等）进行的更改。这可以使您注意到未经授权软件的安装或已安装软件的意外更改。

趋势科技服务器深度安全防护系统虚拟设备以及物理或虚拟计算机上的趋势科技服务器深度安全防护系统客户端目前支持完整性监控模块。

日志审查

日志审查模块用于监控系统日志，在发生特定类型事件时发出警报。例如，某个日志审查规则在特定时间范围内出现特定数量的认证不成功事件时发出警报。

日志审查模块要求在物理计算机或虚拟机上安装客户端。目前趋势科技服务器深度安全防护系统虚拟设备不对其提供支持。

云安全智能防护网络

趋势科技服务器深度安全防护系统使用趋势科技的云安全智能防护网络从云提供实时安全。

云安全智能防护网络为趋势科技服务器深度安全防护系统提供以下服务：

- Web 信誉技术
- 文件信誉技术
- 智能反馈
- 趋势科技更新服务器

要了解这些服务的更多信息，请转至 <http://cn.trendmicro.com/securecloud2/>

趋势科技服务器深度安全防护系统中继

趋势科技服务器深度安全防护系统中继提供从趋势科技服务器深度安全防护系统环境到全局更新服务器的链接。

云安全智能防护服务器

还可以在趋势科技服务器深度安全防护系统环境中部署趋势科技云安全智能防护服务器，从而为趋势科技服务器深度安全防护系统提供备用本地云安全智能防护服务。

虚拟环境中的防恶意软件防护

与 VMware vShield Endpoint 集成

趋势科技服务器深度安全防护系统 8.0 旨在为使用 VMware vSphere 的虚拟环境提供防护。

VMware vCenter 管理托管要受保护的客户 VM 的 ESXi 虚拟机监控程序。VMware vShield Manager 管理依次与 VMware 精简客户端通信的 VMware vShield Endpoint。最后两个组件提供趋势科技服务器深度安全防护系统用来提供防恶意软件保护的 API。

趋势科技服务器深度安全防护系统管理中心协调提供给各个客户虚拟机的防恶意软件保护。这是通过使用 VMware Endpoint API 将保护应用到虚拟机的趋势科技服务器深度安全防护系统虚拟设备执行的。趋势科技服务器深度安全防护系统过滤器驱动程序控制进出客户虚拟机的网络流量。

有关更多详细信息，请参阅[虚拟环境中的无客户端防护快速入门指南](#)。

趋势科技服务器深度安全防护系统 8.0 (SP1) 中的新增功能

Linux 上基于客户端的防恶意软件

趋势科技服务器深度安全防护系统现在为 Linux 提供基于客户端的防恶意软件支持。

支持 VMware ESX/ESXi 4.1 和 ESXi 5.0

可以在 4.1 和 5.0 版的 ESX/ESXi 上安装 8.0 版的趋势科技服务器深度安全防护系统过滤器驱动程序和虚拟设备，并为该 ESX/ESXi 提供防护。

防恶意软件扫描例外

您现在可以通过专门列出或通过使用通配符，从防恶意软件扫描中排除目录、文件和文件扩展名。

趋势科技服务器深度安全防护系统 8.0 中的新增功能

Linux 上的趋势科技服务器深度安全防护系统管理中心

趋势科技服务器深度安全防护系统管理中心可用于 Linux 平台（64 位）。

无客户端完整性监控

在趋势科技服务器深度安全防护系统 7.5 中，完整性监控功能仅随趋势科技服务器深度安全防护系统客户端一起提供。在趋势科技服务器深度安全防护系统 8.0 中，DSVA 目前还提供完整性监控来保护无客户端虚拟机。

Windows 的趋势科技服务器深度安全防护系统客户端上的防恶意软件

除了趋势科技服务器深度安全防护系统虚拟设备上的防恶意软件保护，防恶意软件保护目前还可用在趋势科技服务器深度安全防护系统客户端 (Windows) 上。

IPv6 支持

趋势科技服务器深度安全防护系统目前支持 IPv6。

注意：虽然趋势科技服务器深度安全防护系统 8 客户端和设备支持 IPv6 网络通信，但缺省情况下会阻止该网络通信。要在趋势科技服务器深度安全防护系统 8 客户端和设备上允许 IPv6 网络通信，请转至**系统 > 系统设置 > 网络引擎**选项卡的**高级**区域，将对 **8.0 及更高版本的客户端和设备阻止 IPv6** 选项设置为否。

趋势科技服务器深度安全防护系统中继

趋势科技服务器深度安全防护系统管理中心需要此新软件来从趋势科技云安全智能防护网络提取趋势科技服务器深度安全防护系统组件更新。趋势科技服务器深度安全防护系统中继还为趋势科技服务器深度安全防护系统客户端和设备提供了从中继接收组件更新（所有防护模块所需要的，防火墙除外）的能力，从而提高性能。

可以安装多个趋势科技服务器深度安全防护系统中继，可将它们组织到层次结构中以优化带宽（例如，在远程办公室中的所有计算机上配置客户端来使用特定中继）。

云安全智能防护网络

云安全智能防护网络由趋势科技管理，其功能可以提供给趋势科技服务器深度安全防护系统基础架构使用。文件信誉在启用云安全智能防护模式时由防恶意软件模块使用。Web 信誉需要云安全智能防护服务器。

文件信誉服务：

趋势科技服务器深度安全防护系统客户端和设备存储防恶意软件特征码，将其用作扫描期间的初始文件威胁检测和消除工具。如果客户端/设备无法确定文件的风险，将向云安全智能防护网络或云安全智能防护服务器发送一条查询以进行评估。

Web 信誉服务：

Web 信誉服务通过基于 Web 站点的页面、历史位置更改以及借助恶意软件行为分析发现的可疑活动指示等因素分配信誉分数，从而跟踪 Web 域的可信性。Web 信誉服务可为站点内的特定页面或链接指定信誉评分，而不是分类或阻止整个站点。

Web 信誉

趋势科技服务器深度安全防护系统的 Web 信誉防护允许基于 Web 页面的 Web 信誉评估和所需的安全级别来阻止这些页面：威胁的已知来源、威胁的可能来源或可能的垃圾邮件源。Web 信誉使用趋势科技云安全智能防护网络。

该配置使特定 URL 被阻止或允许，并且可以提供页面的定制链接，用于替换阻止的页面。

Web 信誉防护功能可在趋势科技服务器深度安全防护系统防恶意软件防护使用授权下使用。

智能反馈

趋势科技智能反馈在趋势科技产品和公司的 24/7 威胁研究中心和技术之间提供持续的信息传送。借助于智能反馈，产品变为趋势科技云安全智能防护网络的活动部分，在该网络中将实时共享和分析大量威胁数据。通过这种互连，可以前所未有的速度识别、分析和停止新威胁——解决每日发布的数千个新威胁和威胁变种的响应能力级别。

协调方法

协调方法实施方式的变化意味着，如果趋势科技服务器深度安全防护系统虚拟设备和该设备保护的某个虚拟机上的趋势科技服务器深度安全防护系统客户端中均激活并使用了防恶意软件或完整性监控功能，只有客户端中的防护功能生效。

自动标记和可信源

作为完整性监控防护的一部分，改进的自动标记功能允许管理员基于与所选已知良好事件的相似性来自动标记受保护计算机中的事件。已知良好事件的来源可以是本地可信计算机或趋势科技的**安全软件认证服务**的已知良好签名。可以使用这些标记来对事件进行组织，以简化事件监控和管理任务。

趋势科技服务器深度安全防护系统通知程序

趋势科技服务器深度安全防护系统通知程序是一个 Windows 系统托盘应用程序，显示趋势科技服务器深度安全防护系统客户端和趋势科技服务器深度安全防护系统中继的状态。当趋势科技服务器深度安全防护系统客户端阻止恶意软件或对 Web 页面的访问时，该通知程序还提供弹出用户通知。

缺省情况下，该通知程序在 Windows 上随趋势科技服务器深度安全防护系统中继和趋势科技服务器深度安全防护系统客户端自动安装，但是还可以在从趋势科技服务器深度安全防护系统虚拟设备接收无客户端防护的虚拟机上安装该通知程序。

客户端自我保护

管理员可使用趋势科技服务器深度安全防护系统管理中心来防止本地最终用户卸载、停止或以其他方式修改趋势科技服务器深度安全防护系统客户端。

虚拟环境中的无客户端防护快速入门指南

本节介绍了趋势科技服务器深度安全防护系统如何集成到 VMware 环境中来使用趋势科技服务器深度安全防护系统虚拟设备提供无客户端防护。



必须先准备 VMware 环境，然后才能部署任何趋势科技服务器深度安全防护系统组件。本指南包含过程的详细描述。

准备 VMware 环境

如果要对虚拟机实施无客户端防恶意软件或完整性监控防护，则需要 VMware vShield Manager 和 VMware vShield Endpoint 驱动程序。

您将需要：

1. 部署 VMware vShield Manager。vShield Manager 用于部署 vShield Endpoint Protection 并授予使用授权。
2. 在 ESX/ESXi 虚拟机监控程序上安装 vShield Endpoint 主机驱动程序。
3. 在要保护的虚拟机上安装 vShield Endpoint 驱动程序。

安装数据库以供趋势科技服务器深度安全防护系统管理中心使用

趋势科技服务器深度安全防护系统需要 Microsoft SQL Server 或 Oracle Database。
(趋势科技服务器深度安全防护系统管理中心还自带有一个内置数据库，该数据库仅适用于评估目的。)

部署趋势科技服务器深度安全防护系统环境

从趋势科技下载趋势科技服务器深度安全防护系统安装包后，您将需要：

1. 安装趋势科技服务器深度安全防护系统管理中心。
2. 安装至少一个趋势科技服务器深度安全防护系统中继。
3. 执行趋势科技服务器深度安全防护系统管理中心和趋势科技服务器深度安全防护系统中继的基本配置。
4. VMware 环境的其他配置。
5. 为趋势科技服务器深度安全防护系统虚拟设备部署准备 ESX/ESXi (通过部署趋势科技服务器深度安全防护系统过滤器驱动程序)。
6. 安装并激活趋势科技服务器深度安全防护系统虚拟设备。
7. 在要保护的 Windows 虚拟机上安装趋势科技服务器深度安全防护系统通知程序 (可选)。

在虚拟机上启用防护

使用趋势科技服务器深度安全防护系统管理中心激活要保护的虚拟机。

- 通过向设备分配安全配置文件（安全配置文件包含趋势科技服务器深度安全防护系统防护模块的规则），向虚拟机应用防护。

注意：请记住，对于新添加的虚拟机，必须始终先为其安装 vShield Endpoint 驱动程序，然后才能向其提供防恶意软件或完整性监控防护。

客户端防护快速入门指南

本节介绍物理计算机或虚拟机上安装有客户端时如何进行防恶意软件和/或防火墙与 DPI 防护的基础知识。

注意：某些功能并非在所有平台上都可用。有关平台支持的功能的完整详细列表，请参阅联机帮助或《管理员指南》。

安装数据库以供趋势科技服务器深度安全防护系统管理中心使用

趋势科技服务器深度安全防护系统需要 Microsoft SQL Server 或 Oracle Database。
(趋势科技服务器深度安全防护系统管理中心还自带有一个内置数据库，该数据库仅适用于评估目的。)

部署趋势科技服务器深度安全防护系统环境

从趋势科技下载趋势科技服务器深度安全防护系统安装包后，您将需要：

1. 安装趋势科技服务器深度安全防护系统管理中心。
2. 安装至少一个趋势科技服务器深度安全防护系统中继。
3. 执行趋势科技服务器深度安全防护系统管理中心和趋势科技服务器深度安全防护系统中继的基本配置。
4. 在要保护的物理计算机或虚拟机上安装趋势科技服务器深度安全防护系统客户端。

在计算机上启用防护

1. 使用趋势科技服务器深度安全防护系统管理中心激活趋势科技服务器深度安全防护系统客户端。
2. 通过向客户端分配安全配置文件（安全配置文件包含趋势科技服务器深度安全防护系统防护模块的规则），向计算机应用防护。

混合环境中防护的快速入门指南

趋势科技服务器深度安全防护系统可以仅使用虚拟设备保护虚拟机，您也可以使用协调方法，同时使用虚拟设备和客户端来保护计算机。

虚拟设备和使用趋势科技服务器深度安全防护系统客户端的协调方法

虚拟设备

趋势科技服务器深度安全防护系统虚拟设备为虚拟机提供防恶意软件、防火墙、入侵检测/阻止、应用程序控制、Web 应用程序和完整性监控防护，而无需存在客户虚拟机客户端。虚拟设备使用 VMware 的 VMsafe-NET API 来截获 vSphere 环境中通过虚拟机监控程序的网络流量。对每台虚拟机应用安全策略。

相较于客户虚拟机客户端，虚拟设备可提供以下一些特有的安全优势：

- 设备与客户虚拟机隔离。客户虚拟机可在仅安装最少所需软件的情况下运行。
- 可以简单快速的保护可能尚未为其分配安装安全软件的管理时间的新计算机和恢复的计算机。
- 可以保护不能直接访问其操作系统的虚拟机和其他设备，即使这些计算机由其他管理员管理也是如此。

趋势科技服务器深度安全防护系统虚拟设备简化了部署。无需在虚拟机上远程安装客户端软件。无需从趋势科技服务器深度安全防护系统连接到虚拟机。

协调方法

使用虚拟设备保护虚拟机不会妨碍对同一主机上的虚拟机使用趋势科技服务器深度安全防护系统客户端。使用协调方法保护虚拟机时，如果客户端变为脱机，会自动激活来自设备的防护。

这种协调的方法提供了以下好处：

- 可以在虚拟机上运行建议扫描。
- 为虚拟机提供移动性。可以在数据中心或云提供商之间移动虚拟机，所受保护也随之移动。
- 性能改进。当趋势科技服务器深度安全防护系统客户端在虚拟机上处于活动状态时，虚拟设备会自动将流量传递到客户端。
- 通过使用趋势科技服务器深度安全防护系统客户端提供防护，允许您在虚拟机上实现其他完整性监控和日志审查模块。

要对特定的防护模块实施协调方法，则客户端和设备均必须实施该防护。下表显示了可以利用协调方法的趋势科技服务器深度安全防护系统防护模块：

	受设备支持	受客户端支持**	协调方法可用
防恶意软件	是	是	否
Web 信誉	是	是	是
防火墙	是	是	是
深度包检查	是	是	是
完整性监控	是	是	否
日志审查	否	是	否

注意：某些功能并非在所有平台上都可用。有关平台支持的功能的完整详细列表，请参阅联机帮助或《管理员指南》。

趋势科技服务器深度安全防护系统 — 安装指南

系统要求

本节列出了趋势科技服务器深度安全防护系统软件组件的硬件和软件要求。

趋势科技服务器深度安全防护系统管理中心系统要求

- **内存:** 4GB
- **磁盘空间:** 1.5GB (建议使用 5GB)
- **操作系统:**
 - **Windows:** Windows Server 2008 (32 位和 64 位)、Windows Server 2008 R2 (64 位)、Windows Server 2003 SP2 (32 位和 64 位)、Windows Server 2003 R2 (32 位和 64 位)
 - **Linux:** Red Hat 5 (64 位)、Red Hat 6 (64 位)
- **数据库 (建议但可选):** Oracle 11g、Oracle 10g、Microsoft SQL Server 2008、Microsoft SQL Server 2005。(建议使用 20GB RAM 进行预分配)
- **Web 浏览器:** Mozilla Firefox 3.5+ (启用 cookie)、Internet Explorer 7+ (启用 cookie)

有关内存和磁盘空间要求的其他信息，请参阅 2: 准备中的[性能建议](#)和 4: 为趋势科技服务器深度安全防护系统管理中心安装数据库中的[数据库磁盘空间](#)。

趋势科技服务器深度安全防护系统中继系统要求

- **内存:** 512MB
- **磁盘空间:** 100MB（建议使用 200MB，主要用于日志记录）（启用防恶意软件防护时建议使用 1GB）
- **Windows:** Windows 7（32 位和 64 位）、Windows Server 2008（32 位和 64 位）、Windows Server 2008 R2（64 位）、Windows Vista（32 位和 64 位）、Windows Server 2003 SP2（32 位和 64 位）、Windows Server 2003 R2（32 位和 64 位）、Windows XP（32 位和 64 位）
- **Linux:** Red Hat 5（64 位）、Red Hat 6（64 位）、CentOS 5（64 位）、CentOS 6（64 位）

趋势科技服务器深度安全防护系统虚拟设备的 ESX/ESXi 要求

除了 ESX/ESXi 标准系统要求外，还必须符合以下规范：

- **CPU:** 64 位，存在 Intel-VT 并在 BIOS 中启用
- **支持的 vSwitch:** 标准 vSwitch 或第三方 vSwitch — Cisco Nexus 1000v

注意: 不支持虚拟化 ESX/ESXi 环境（虚拟机监控程序作为虚拟机运行）。

趋势科技服务器深度安全防护系统虚拟设备系统要求

- **内存:** 1GB（内存要求随受保护的 VM 的数量而变化。请参阅[附录 C: 趋势科技服务器深度安全防护系统虚拟设备内存使用](#)，了解详细信息。）
- **磁盘空间:** 20GB
 - **操作系统:** VMware vCenter 5.0.0 和 ESXi 5.0.0 或 ESX/ESXi 4.1
 - **其他 VMware 工具:** VMware Tools、VMware vShield Manager 5.0 和 VMware vShield Endpoint Security 5.0（适用于 vShield Endpoint 驱动程序的 ESXi5 patch ESXi500-201109001 或更高版本）
 - **VMware 端点防护支持的客户虚拟机平台:** Windows Vista（32 位和 64 位）、Windows 7（32 位和 64 位）、Windows XP SP2（32 位和 64 位）、Windows Server 2003 SP2（32 位和 64 位）、Windows Server 2003 R2（32 位和 64 位）、Windows Server 2008（32 位和 64 位）、Windows Server 2008 R2（64 位）。（有关支持的客户虚拟机平台的最新列表，请参阅 VMware 文档。）

趋势科技服务器深度安全防护系统客户端系统要求

- **内存:**
 - **具有防恶意软件:** 512MB
 - **无防恶意软件:** 128MB
- **磁盘空间:** 100MB (建议使用 200MB, 主要用于日志记录) (启用防恶意软件防护时建议使用 1GB)
- **Windows:** Windows 7 (32 位和 64 位)、Windows Server 2008 R2 (64 位)、Windows Server 2008 (32 位和 64 位)、Windows Vista (32 位和 64 位)、Windows Server 2003 Sp1 (32 位和 64 位) 带有 patch "Windows Server 2003 Scalable Networking Pack"、Windows Server 2003 SP2 (32 位和 64 位)、Windows Server 2003 R2 SP2 (32 位和 64 位)、Windows XP (32 位和 64 位)
- **Solaris:** Solaris 9 和 10 (64 位 Sparc)、Solaris 10 和 11 (64 位 x86)
- **Linux:** Red Hat 4 (32 位和 64 位)、Red Hat 5 (32 位和 64 位)、Red Hat 6 (32 位和 64 位)、SuSE 10 (32 位和 64 位)、SuSE 11 (32 位和 64 位)、Ubuntu 10.04.3 LTS (64 位)、CentOS 5 (32 位和 64 位)、CentOS 6 (32 位和 64 位)、Amazon Linux (请参阅最新客户端发行说明了解支持的版本)。(Red Hat 5 (32 位)、Red Hat 6 (32 位)、CentOS 5 (32 位)、CentOS 6 (32 位)、SuSE 10 (32 位)、SuSE 11 (32 位) 和 Amazon Linux (32 位) 上不支持基于客户端的防恶意软件。)
- **AIX:** AIX 5.3 和 6.1 (AIX 客户端仅支持完整性监控和日志审查。)
- **HP-UX:** 11i v3 (11.31) (HP-UX 客户端仅支持完整性监控和日志审查。)

注意: 在 Windows XP 或 Windows 2003 上运行的 Windows 客户端在 IPv6 环境中不起作用。

趋势科技服务器深度安全防护系统通知程序系统要求

- **Windows:** Windows 7 (32 位和 64 位)、Windows Server 2008 R2 (64 位)、Windows Server 2008 (32 位和 64 位)、Windows Vista (32 位和 64 位)、Windows Server 2003 Sp1 (32 位和 64 位) 带有 patch "Windows Server 2003 Scalable Networking Pack"、Windows Server 2003 SP2 (32 位和 64 位)、Windows Server 2003 R2 SP2 (32 位和 64 位)、Windows XP (32 位和 64 位)

准备

本节介绍了成功部署趋势科技服务器深度安全防护系统的所需条件。

所需条件

趋势科技服务器深度安全防护系统安装包

可以从趋势科技下载专区获取所有趋势科技服务器深度安全防护系统安装包：

<http://www.trendmicro.com/download/zh-cn/>。

注意：要验证每个安装包的完整性，请使用哈希计算器计算已下载软件的哈希值并将其与趋势科技下载专区 Web 站点上发布的值相比较。

提供了适用于多种类型操作系统的趋势科技服务器深度安全防护系统客户端软件包。请为每种需要保护的计算机分别下载相应的趋势科技服务器深度安全防护系统客户端安装包。

将趋势科技服务器深度安全防护系统管理中心、趋势科技服务器深度安全防护系统中继、趋势科技服务器深度安全防护系统虚拟设备和趋势科技服务器深度安全防护系统过滤器驱动程序的安装包放在同一文件夹中。这样，趋势科技服务器深度安全防护系统管理中心便会在安装时自动导入中继、虚拟设备和过滤器驱动程序。

注意：对安全组件、趋势科技服务器深度安全防护系统客户端和趋势科技服务器深度安全防护系统虚拟设备的更新均可以使用趋势科技服务器深度安全防护系统管理中心进行部署。但是，新版本的趋势科技服务器深度安全防护系统管理中心必须独立于当前的趋势科技服务器深度安全防护系统管理中心进行安装。也就是说，必须从趋势科技下载专区下载新版本，然后运行安装程序，并按照说明执行软件升级。

使用授权（激活码）

对于要使用的每个趋势科技服务器深度安全防护系统防护模块，使用授权（激活码）均是必需的。

VMware 组件还需要使用授权。

管理员/Root 权限

需要拥有管理员/Root 权限才可以安装趋势科技服务器深度安全防护系统软件组件。

可用端口

在趋势科技服务器深度安全防护系统管理中心主机上：

您必须确保托管趋势科技服务器深度安全防护系统管理中心的计算机上的以下端口处于打开状态且未保留用于其他目的：

- **端口 4120：**“波动信号”端口，趋势科技服务器深度安全防护系统客户端和设备使用该端口与趋势科技服务器深度安全防护系统管理中心进行通信（可配置）。
- **端口 4119：**浏览器使用其连接到趋势科技服务器深度安全防护系统管理中心。还用于来自 ESXi 的通信以及 DSVa 的安全更新请求（可配置）。
- **端口 1521：**双向 Oracle Database 服务器端口。
- **端口 1433 和 1434：**双向 Microsoft SQL Server 数据库端口。
- **端口 389、636 和 3268：**连接到 LDAP 服务器以集成 Active Directory（可配置）。
- **端口 80、433：**连接到趋势科技 7.5 旧式 ActiveUpdate 服务器（可配置）。
- **端口 25：**与 SMTP 服务器通信来发送电子邮件警报（可配置）。
- **端口 53：**用于 DNS 查询。

注意：有关趋势科技服务器深度安全防护系统使用的端口的详细列表，请参阅联机帮助或《管理员指南》的**参考**一节中的“**趋势科技服务器深度安全防护系统所使用的端口**”。

在趋势科技服务器深度安全防护系统中继、客户端和设备上：

您必须确保托管趋势科技服务器深度安全防护系统中继的计算机上的以下端口处于打开状态且未保留用于其他目的：

- **端口 4122：** 中继与客户端/设备之间的通信。
- **端口 4118：** 管理中心与客户端之间的通信。
- **端口 4123：** 供虚拟设备使用，用于在将其受保护的 VM vMotion 至另一个 ESX/ESXi 时向中继发送完整性监控基线信息。
- **端口 80、433：** 连接到趋势科技更新服务器和云安全智能防护服务器。
- **端口 514（可选）：** 与 Syslog 服务器双向通信。

根据通信方向配置，趋势科技服务器深度安全防护系统管理中心自动实现防火墙规则，来打开托管趋势科技服务器深度安全防护系统中继、客户端和设备的计算机上的所需通信端口。

注意： 请参阅联机帮助或《管理员指南》的**计算机**一节中的“**通信方向**”。

网络通信

趋势科技服务器深度安全防护系统管理中心与趋势科技服务器深度安全防护系统中继/客户端/设备和虚拟机监控程序通信时使用 DNS 主机名。

为了成功部署趋势科技服务器深度安全防护系统客户端/设备/中继，必须确保每台计算机均可以解析趋势科技服务器深度安全防护系统管理中心的主机名。这要求趋势科技服务器深度安全防护系统管理中心计算机拥有 DNS 项或在中继/客户端/设备计算机的 hosts 文件中存在对应项。

注意： 您会在趋势科技服务器深度安全防护系统管理中心安装过程中指定此主机名。如果没有 DNS，必须在安装期间指定 IP 地址。

可靠时间戳

运行趋势科技服务器深度安全防护系统软件的所有计算机均应与可靠的时间源保持同步。例如，定期与网络时间协议 (NTP) 服务器通信。

趋势科技服务器深度安全防护系统中继 (DSR) 计算机上的时钟必须 24 小时与趋势科技服务器深度安全防护系统管理中心 (DSM) 同步。

性能建议

以下准则提供了不同规模的趋势科技服务器深度安全防护系统部署的一般基础架构要求。

趋势科技服务器深度安全防护系统管理中心和数据库硬件

很多趋势科技服务器深度安全防护系统管理中心操作需要使用较高的 CPU 和较多的内存资源（例如更新和建议扫描）。趋势科技建议高规格环境中的每个管理中心节点均拥有 4 个核心和足够的内存。应尽可能使用 64 位版本的管理中心，因为它可以寻址 4GB 的内存（相比之下，32 位版本只能寻址 1GB）。

数据库应该安装在与性能最好的管理中心节点的规格相同或更高的硬件之上。为了实现最高的性能，数据库应拥有 8-16GB 内存并且可以快速访问本地或网络连接存储器。在可能的情况下，应咨询数据库管理员有关数据库服务器的最佳配置，并且应实施维护计划。

趋势科技服务器深度安全防护系统多管理中心节点

您可能需要为趋势科技服务器深度安全防护系统管理中心安装准备多个计算机。在实际环境中，可以配置连接到单个数据库的多个趋势科技服务器深度安全防护系统管理中心节点，用于负载平衡和恢复目的。对于评估目的，仅需要一个趋势科技服务器深度安全防护系统管理中心。

有关运行多个管理中心节点的更多信息，请参阅联机帮助或《管理员指南》的[参考一节](#)中的[多节点管理中心](#)。

专用服务器

如果最终部署预期不超过 1000 台计算机（实体或虚拟），则可以在同一计算机上安装趋势科技服务器深度安全防护系统管理中心和数据库。如果您认为可能会超过 1000 台计算机，则应在专用服务器上安装趋势科技服务器深度安全防护系统管理中心和数据库。数据库和趋势科技服务器深度安全防护系统管理中心位于拥有 1GB LAN 连接的同一网络中也很重要，这样可确保在两者之间进行顺畅的通信。同样的情况适用于其他趋势科技服务器深度安全防护系统管理中心节点：同一地点的专用服务器。建议管理中心和数据库之间的延迟为 2ms 或更低。

注意： 不论是否具有 1000 台被管理计算机，出于冗余原因，最好运行多个管理中心节点。

高可用性环境

如果您打算利用 VMware 高可用性 (HA) 功能，请确保在开始安装趋势科技服务器深度安全防护系统之前建立了 HA 环境。用于恢复操作的所有 ESX/ESXi 虚拟机监控程序必须同其 vCenter 一起导入到趋势科技服务器深度安全防护系统管理中心中，必须对其进行准备，并且必须在每个虚拟机监控程序上安装趋势科技服务器深度安全防护系统虚拟设备。以这种方式设置环境将确保在执行 HA 恢复操作之后趋势科技服务器深度安全防护系统防护仍然有效。

注意： 在使用 VMware 分布式资源计划程序 (DRS) 的 VMware 环境中部署虚拟设备时，重要的是该设备没有作为 DRS 进程的一部分与虚拟机一起被 vMotion。必须将虚拟设备“固定”到其特定的 ESX/ESXi 主机。您必须主动将所有虚拟设备的 DRS 设置更改为“手动”或“禁用”（推荐），以便 DRS 不会对其 vMotion。如果虚拟设备（或任何虚拟机）已设置为“禁用”，则 vCenter Server 不会迁移该虚拟机或为其提供迁移建议。这称为将虚拟机“绑定”到其注册的主机。这是对 DRS 环境中的虚拟设备的推荐操作过程。（另一种方法是将虚拟设备部署到本地存储，而不是共享存储。将虚拟设备部署到本地存储后，DRS 将无法对其进行 vMotion。）有关 DRS 以及将虚拟机绑定到特定 ESX/ESXi 主机的更多信息，请查看 VMware 文档。

注意：如果虚拟机被 HA 从受 DSVa 保护的 ESX/ESXi vMotion 到不受 DSVa 保护的 ESX/ESXi，该虚拟机将变为不受保护。如果随后将虚拟机 vMotion 回原始 ESXi，则其不会再次自动受到保护，除非您创建了基于事件的任务来激活和保护已通过可用 DSVa vMotion 到 ESXi 的计算机。有关更多信息，请参阅联机帮助或《管理员指南》的**任务**一节。

所需资源核对清单

检查	服务器	要求
	数据库：SQL Server 或 Oracle	内存：4GB 磁盘空间：>20GB 操作系统：Windows Server 2008（64 位）
	趋势科技服务器深度安全防护系统管理中心	内存：4GB 磁盘空间：5GB 操作系统：Windows Server 2008（64 位）或 Linux（64 位）
	趋势科技服务器深度安全防护系统中继	可以在趋势科技服务器深度安全防护系统管理中心主机上共置一个中继。 磁盘空间：200MB 操作系统：Windows Server 2008（64 位）或 Linux（64 位）

检查	使用授权要求	
	趋势科技服务器深度安全防护系统管理中心	防护模块需要使用授权。

为无客户端防护准备 VMware 环境

建议的环境 — 概述

下面介绍了典型 VMware 环境中的趋势科技服务器深度安全防护系统部署。

包括两种类型的 ESX/ESXi 主机：

主机 A，是 ESX/ESXi 虚拟机监控程序，在其上运行趋势科技服务器深度安全防护系统管理中心 8.0、vShield Manager 5.0 和 vCenter Server 5.0 的单个虚拟机 (VM)（可以在物理计算机上安装）。（可选）可以在主机 A 上的虚拟机上安装趋势科技云安全智能防护服务器和趋势科技服务器深度安全防护系统中继。还可以为另一个趋势科技服务器深度安全防护系统管理中心节点提供其他虚拟机。还应该为安装趋势科技服务器深度安全防护系统数据库提供一个 VM。

主机 B，是 ESX 虚拟机监控程序，在其上运行趋势科技服务器深度安全防护系统虚拟设备 (DSVA) 和需要防护的 VM。

注意：虽然可以在物理计算机上安装 vCenter Server、vShield Manager 和趋势科技服务器深度安全防护系统管理中心，但大多数企业在 VM 上安装它们，因为可以使用虚拟环境。它们安装在单独的 ESX/ESXi 上，因为在趋势科技服务器深度安全防护系统部署期间必须重新启动受保护的 ESX/ESXi。另请注意，趋势科技服务器深度安全防护系统数据库未显示在下图中。它还可以安装在物理计算机上或安装在 VM 上（但是，再次说明，不是在受保护的 ESX/ESXi 上）。



最低要求

主机 A: ESX/ESXi

(一个客户 VM 上的每个以下组件) :

检查	硬件要求
	vCenter Server 5.0 , 在 Windows Server 2008 或 2003 (64 位) 上
	vShield Manager 5.0
	数据库 (Oracle 或 SQL), 用于趋势科技服务器深度安全防护系统
	趋势科技服务器深度安全防护系统管理中心 8.0 , 在 Windows Server 2008 R2 或 Windows 2003 (64 位) 上
	Intel (64 位处理器) • 6GB RAM: • 1GB 用于 vCenter • 2GB 用于 vShield Manager 2GB 用于 DSM 160GB HDD CD/DVD 驱动器

检查	硬件要求
	趋势科技服务器深度安全防护系统中继 8.0 (在趋势科技服务器深度安全防护系统管理中心 VM 上为可选)

主机 B: ESX/ESXi

检查	硬件要求
	趋势科技服务器深度安全防护系统虚拟设备 8.0
	要保护的 客户 VM
	Intel (64 位处理器) 4GB RAM: <ul style="list-style-type: none"> 1GB 用于趋势科技服务器深度安全防护系统虚拟设备 其他取决于要在此主机上安装的客户虚拟机操作系统数 80GB HDD CD/DVD 驱动器

所需资源核对清单

检查	软件要求	注意
	VMware vCenter 5.0	包括 vCenter Server 和 vCenter Client GUI 应用程序。产品安装期间需要使用授权。
	VMware vShield Manager 5.0	产品安装期间需要使用授权。
	趋势科技服务器深度安全防护系统管理中心 8.0 (DSM)	产品安装期间需要使用授权。
	VMware vShield Endpoint 5.0 (ESXi5 patch ESXi500-201109001 或更高版本)	将使用授权添加到 vCenter。
	趋势科技服务器深度安全防护系统过滤器驱动程序 8.0 (FD)	
	趋势科技服务器深度安全防护系统虚拟设备 8.0 (DSVA)	

检查	软件要求	注意
	支持的客户虚拟机操作系统	在每个客户虚拟机 VM 上需要的 vShield Endpoint 驱动程序。 (从 ESXi5 patch ESXi500-201109001 开始, vShield Endpoint 驱动程序包括在 VMware Tools 中)。
	趋势科技服务器深度安全防护系统客户端 8.0 (可选)	用于协调保护。

服务器准备

服务器准备 (在主机 A 上)

按建议的顺序执行任务。

任务 1: ESXi 5.0 安装 (可选)

注意: 如果使用的是现有 ESX/ESXi 4.1, 且打算升级到 ESXi 5.0, 则可以继续执行任务 2。

- 步骤 1. 在主机 A 上安装 ESXi 5.0
- 步骤 2. 配置 ESXi (例如, 网络静态 IP)

任务 2: vCenter Server 5.0 安装

- 步骤 1. 准备客户虚拟机操作系统 Windows Server 2008 或 2003 (64 位)
- 步骤 2. 下载 vCenter Server 5.0 和 vSphere Client 5.0
- 步骤 3. 安装 vCenter Server 5.0
- 步骤 4. 在同一客户 VM 或任何其他计算机 (除了在 ESX/ESXi 主机 B 上) 安装 vSphere Client
- 步骤 5. 在 vCenter 控制台上, 通过“添加主机”来添加主机 A

注意: vCenter 控制台是指 vSphere Client GUI。

任务 3: vShield Manager (vSM) 5.0 安装

- 步骤 1. 在 vCenter 控制台上，选择文件 > 部署 OVF 模板
- 步骤 2. 浏览并选择 vShield Manager OVA 文件
确保仅在 ESXi 主机 A 上部署 vSM
- 步骤 3. 部署 vSM 后，打开 vSM 并从控制台以 admin:default 身份登录
键入 "enable" 来打开授权模式命令，使用 "default" 作为密码
键入 "setup" 并执行相应步骤来完成 vSM 网络配置
- 步骤 4. 通过使用 Internet 浏览器转至 <https://<vSM-ip>> 来登录到 vSM
确保显示 vSM Web 控制台

任务 4: 为数据库安装准备客户虚拟机操作系统

此客户虚拟机将托管 Oracle 或 SQL 数据库以供趋势科技服务器深度安全防护系统管理中心使用。

- 步骤 1. 准备客户虚拟机操作系统 Windows 2008 R2 或 2003（64 位）
（确保应用最新的 Patch）。

任务 5: 为趋势科技服务器深度安全防护系统管理中心安装准备客户虚拟机操作系统

- 步骤 1. 准备客户虚拟机操作系统 Windows 2008 R2 或 2003（64 位）
- 步骤 2. （可选）为其他趋势科技服务器深度安全防护系统管理中心节点准备其他客户虚拟机操作系统

重要事项: 仅在托管要保护的 VM 的 ESX/ESXi 虚拟机监控程序上安装趋势科技服务器深度安全防护系统管理中心，前提是该 ESX/ESXi 是 ESX/ESXi 群集的一部分。这是因为趋势科技服务器深度安全防护系统管理中心会强制 ESX/ESXi 进入维护模式。如果 ESX/ESXi 是群集的一部分，在此过程中，VM（包括趋势科技服务器深度安全防护系统管理中心）将 vMotion 到其他 ESX/ESXi 主机。

客户虚拟机操作系统准备

客户虚拟机操作系统准备（在主机 B 上）— 趋势科技服务器深度安全防护系统要保护的虚拟机

任务 6：ESXi 5.0 安装（可选）

注意：如果使用的是现有 ESX/ESXi 4.1，且不打算升级到 ESXi 5.0，则可以继续执行任务 7。

- 步骤 1. 在主机 B 上安装 ESXi 5.0
- 步骤 2. 配置 ESXi 网络设置（例如，网络静态 IP）
- 步骤 3. 在 vCenter 控制台上，通过“添加主机”来添加主机 B

任务 7：客户虚拟机操作系统准备

趋势科技服务器深度安全防护系统防恶意软件要保护的**客户 VM #1**

- 步骤 1. 安装客户虚拟机操作系统。
(如果使用 Windows 2003 Server，请确保安装 Service Pack 2)
- 步骤 2. 确保客户 VM 具有基本磁盘卷。不支持动态磁盘。（注意：Windows 2003 的缺省安装包含基本磁盘）
- 步骤 3. 将 VMware vShield Endpoint 驱动程序安装到此计算机。

自 ESXi 5 patch ESXi500-201109001 起，vShield Endpoint 驱动程序包含在 VMware Tools 中的 vShield 驱动程序内。（请注意，安装 VMware Tools 期间缺省情况下不安装 vShield 驱动程序。）

注意：可以将 vShield Endpoint 5.0 与 ESX/ESXi 4.1 Patch 3 配合使用。但是，在 ESX/ESXi 4.1 Patch 3 主机上运行的客户虚拟机必须运行随 ESXi 5.0 Patch 1 提供的 VMware Tools 版本。

随 ESX/ESXi 4.1 Patch 3 提供的 VMware Tools 版本不包含 Endpoint 驱动程序。因此，它无法与 vShield Endpoint 5.0 配合使用。

要下载随 ESXi 5.0 Patch 1 提供的 VMware Tools 版本，请转至 <http://packages.vmware.com/tools/esx/5.0p01/windows/index.html>。

安装 Endpoint vShield 驱动程序:

1. 启动 VMware Tools 安装程序并选择执行交互式安装。
2. 在 VMware Tools 安装期间, 选择 "Custom Install"。
3. 展开 "VMware Device Drivers"。
4. 展开 "VMCI Driver"。
5. 选择 "vShield Drivers" 并选择 "This feature will be installed on local drive"。
6. 单击 "Yes" 重新启动计算机。

趋势科技服务器深度安全防护系统要保护的**客户 VM #2**

步骤 1. 可以在主机 B 上安装多个受支持的客户 VM。请按照上述相同步骤操作并安装 vShield Endpoint 驱动程序。

注意: 如果打算使用手动或预设扫描, 请务必在客户虚拟机上关闭睡眠模式和待机模式。如果客户虚拟机在扫描期间进入睡眠或待机模式, 则会遇到指出扫描异常终止的错误。虚拟机必须处于运行状态, 才能成功完成扫描。

注意: 在高可用性环境中, 为了向已进行 vMotion 的客户虚拟机提供无客户端防护, 趋势科技强烈建议在群集中的所有 ESX/ESXi 虚拟机监控程序上安装趋势科技服务器深度安全防护系统虚拟设备。

完成上述任务后, 继续按照以下各节中的说明来:

- 安装数据库
- 安装趋势科技服务器深度安全防护系统管理中心和趋势科技服务器深度安全防护系统中继
- 配置 DSM 以与 VMware 集成
- 为 DSVA 做准备并部署 DSVA

为趋势科技服务器深度安全防护系统管理中心安装数据库

趋势科技服务器深度安全防护系统管理中心自带有一个内置数据库 (Apache Derby)，该数据库仅适用于评估目的。对于企业部署，趋势科技服务器深度安全防护系统需要 Microsoft SQL Server 2008 或 2005，或者 Oracle Database 11g 或 10g。

在安装趋势科技服务器深度安全防护系统管理中心过程中，安装程序会询问使用内置数据库引擎还是两个支持的企业数据库引擎之一。如果选择后者，安装程序会提示您提供配置信息。

注意：如果您打算使用 Microsoft SQL Server 或 Oracle Database，则必须在安装趋势科技服务器深度安全防护系统管理中心**之前**安装该软件并创建数据库。

数据库磁盘空间

应预先分配数据库磁盘空间。在缺省级别保留日志记录时，保护计算机的每个趋势科技服务器深度安全防护系统客户端平均需要大约 50MB 的数据库磁盘空间来保存数据，另外还需要 5MB 的空间来保存事务日志。因此，一千台计算机将需要 50GB 保存数据以及 5GB 保存事务日志，两千台计算机将需要 100GB 保存数据以及 10GB 来保存事务日志，依此类推。

每台计算机需要的空间量是所记录的日志（事件）数和它们的保留时间的函数。通过**系统 > 系统设置**窗口的**防火墙和 DPI**选项卡，您可以控制多种设置，如事件日志文件的最大大小、在任意给定时间内要保留的日志文件数（“清除控制”）。同样，通过状态配置**属性**窗口上的**TCP、UDP 和 ICMP**选项卡，您可以配置执行状态配置事件日志记录的方式。类似设置可用于**系统 > 系统设置**窗口中的其他趋势科技服务器深度安全防护系统模块。（有关日志记录的更多信息，请参阅联机帮助或《趋势科技服务器深度安全防护系统管理员指南》的**参考**和**方法教学**两节中的“高级日志记录策略模式”和“配置日志记录”。）

可以在全局、安全配置文件和单个计算机级别微调这些事件收集设置。（请参阅联机帮助或《管理员指南》的**参考**一节中的**继承与覆盖**。）

注意：在缺省设置中，以下三个模块通常使用的磁盘空间最多，按降序顺序为：防火墙、完整性监控、日志审查。

帐户详细信息

记下在创建数据库实例时使用的帐户详细信息，因为在趋势科技服务器深度安全防护系统管理中心安装过程中将需要这些信息。

注意：创建 SQL 数据库时，必须向 SQL 帐户授予 DSM 数据库的 **DB_Creator** 服务器角色和 **DB_Owner**。

注意：创建 Oracle 数据库时，必须为帐户分配 "CONNECT" 和 "RESOURCE" 角色，并且必须为帐户授予权限以进行 "CREATE TABLES"、"CREATE SEQUENCES" 和 "CREATE TRIGGERS" 等操作。

DSM 与 SQL Server 的通信

使用命名管道连接到 SQL Server 时，趋势科技服务器深度安全防护系统管理中心的主机和 SQL Server 主机之间必须存在经正确认证的 Microsoft Windows 通信通道。此通道在以下情况下已存在：

- SQL Server 与趋势科技服务器深度安全防护系统管理中心位于同一主机上，
- 两台主机为同一域的成员，或者
- 两台主机之间存在信任关系。

如果不存在此通信通道，则趋势科技服务器深度安全防护系统管理中心将无法通过命名管道与 SQL Server 进行通信。

安装趋势科技服务器深度安全防护系统管理中心

复制安装包

向目标计算机复制相应的趋势科技服务器深度安全防护系统管理中心安装程序和趋势科技服务器深度安全防护系统中继安装程序。

注意：趋势科技服务器深度安全防护系统功能需要一个或多个趋势科技服务器深度安全防护系统中继。如果要在趋势科技服务器深度安全防护系统管理中心的计算机上安装共置趋势科技服务器深度安全防护系统中继，应该将趋势科技服务器深度安全防护系统中继安装包复制到与趋势科技服务器深度安全防护系统管理中心安装包相同的位置。在趋势科技服务器深度安全防护系统管理中心安装期间，安装程序会检查趋势科技服务器深度安全防护系统中继软件包，如果存在并选择了该软件包，成功安装了趋势科技服务器深度安全防护系统管理中心后，安装程序将自动继续趋势科技服务器深度安全防护系统中继安装。

安装适用于 Windows 的趋势科技服务器深度安全防护系统管理中心

必须以管理员身份登录才能安装趋势科技服务器深度安全防护系统管理中心。

步骤 1. 通过双击安装文件启动趋势科技服务器深度安全防护系统管理中心。
选择要安装的趋势科技服务器深度安全防护系统管理中心的语言版本，然后单击**确定**。

注意：用户可以通过以下方法选择要使用的语言：转至**系统 > 设置 > 用户**，然后更改**属性**窗口中的语言设置。

步骤 2. 出现“安装向导”时，单击**下一步继续**。

步骤 3. 接受许可协议，然后单击**下一步**。

步骤 4. 指定要安装趋势科技服务器深度安全防护系统管理中心的文件夹，然后单击**下一步**。

注意：选择文件夹时，安装程序可能会在选定的路径后附加上建议的文件夹名称。如果使用的是“浏览”按钮，请在继续前检查文件夹条目。

步骤 5. 指定要使用的数据库类型。

如果使用 Oracle 或 SQL Server 数据库，则必须在安装趋势科技服务器深度安全防护系统管理中心之前创建数据库。输入帐户详细信息。

步骤 6. 输入激活码。

请输入所有防护模块的激活码或分别输入已购买使用授权的各个模块的激活码。

如果未输入任何激活码，您仍可以继续，但将无法使用任何防护模块。（您可以在安装趋势科技服务器深度安全防护系统管理中心后转至**系统 > 使用授权**输入首个激活码或添加激活码。）

步骤 7. 键入此计算机的主机名、URL 或 IP 地址。

注意：管理中心地址必须为可解析的主机名（完全限定的域名）或 IP 地址。如果环境中 DNS 不可用，或如果某些计算机无法使用 DNS，则应使用固定 IP 地址而不使用主机名。

可以选择更改缺省通信端口：

“管理中心端口”指可通过 HTTPS 访问管理中心的基于浏览器的 UI 的端口。

“波动信号端口”指管理中心侦听来自客户端/设备的通信的端口。

单击**下一步**。

步骤 8. 输入主管理员帐户的用户名和密码。

选中**强制使用强密码**（建议）会要求此管理员及以后创建的管理员的密码包括大写和小写字母、非字母数字字符以及数字，并且要求使用最小字符数。

单击**下一步**。

步骤 9. 选中“自动更新”（建议）。

如果选中，趋势科技服务器深度安全防护系统管理中心将自动检索最新的组件或检查新软件。（以后可以使用趋势科技服务器深度安全防护系统管理中心配置更新。）

单击**下一步**。

步骤 10. 选择是否安装共置趋势科技服务器深度安全防护系统中继。

（如果在趋势科技服务器深度安全防护系统管理中心安装程序的位置没有趋势科技服务器深度安全防护系统中继安装包，将跳过此步骤。）

注意： 如果此时选择不安装共置中继，以后可以通过按[部署趋势科技服务器深度安全防护系统中继](#)中所述安装[趋势科技服务器深度安全防护系统中继](#)来安装共置中继。

单击**下一步**。

步骤 11. 选择是否要启用趋势科技智能反馈（建议）。

（以后可以使用趋势科技服务器深度安全防护系统管理中心启用或配置智能反馈）。

（可选）通过从下拉列表中进行选择来输入行业。

单击**下一步**。

步骤 12. 确认设置。验证输入的信息，然后单击**完成**继续。

步骤 13. 单击**完成**关闭**安装**向导。

Deep Security Manager 服务会在安装完成时启动。

如果在步骤 11 中选择了安装共置趋势科技服务器深度安全防护系统中继，现在将以静默方式运行中继安装。

要启动趋势科技服务器深度安全防护系统管理中心基于 Web 的管理控制台，请在单击**完成**之前选择**运行趋势科技服务器深度安全防护系统管理中心**选项。

注意： 安装程序会在程序菜单中添加趋势科技服务器深度安全防护系统管理中心的快捷方式。如果要远程访问管理中心，需要留意此 URL。

确保可以登录到趋势科技服务器深度安全防护系统管理中心基于 Web 的管理控制台。

安装适用于 Linux 的趋势科技服务器深度安全防护系统管理中心

要从 Linux GUI 安装，说明与安装适用于 Windows 的趋势科技服务器深度安全防护系统管理中心（上述）相同。

要从 Linux 命令行安装，请参阅[趋势科技服务器深度安全防护系统管理中心静默安装](#)（下文）。

运行趋势科技服务器深度安全防护系统管理中心

Deep Security Manager 服务在启动时自动启动。可以从 Microsoft 服务管理控制台启动、重新启动和停止该服务。服务名称是 "Trend Micro Deep Security Manager"。

要运行基于 Web 的管理控制台，请转至**开始**菜单中的**趋势科技**程序组，并单击**趋势科技服务器深度安全防护系统管理中心**。

要从远程计算机运行基于 Web 的管理控制台，您必须记住以下 URL：

```
https://[hostname]:[port]/
```

其中，**[hostname]** 是安装趋势科技服务器深度安全防护系统管理中心的服务器的主机名，**[port]** 是在安装的步骤 8 中指定的“管理中心端口”（缺省为 4119）。

要求访问基于 Web 的管理控制台的用户使用他们的用户帐户凭证进行登录。

趋势科技服务器深度安全防护系统中继配置

趋势科技服务器深度安全防护系统要求至少安装和配置一个趋势科技服务器深度安全防护系统中继。

如果选择了安装共置趋势科技服务器深度安全防护系统中继，请按照[基本趋势科技服务器深度安全防护系统配置](#)中所述使用趋势科技服务器深度安全防护系统管理中心配置趋势科技服务器深度安全防护系统中继。

如果尚未安装共置趋势科技服务器深度安全防护系统中继，则应该先按照[部署趋势科技服务器深度安全防护系统中继](#)中所述安装一个中继，然后再对其进行配置。

趋势科技服务器深度安全防护系统管理中心静默安装

要在 Windows 上启动静默安装，请输入以下命令：

```
Manager-Windows-<Version>.x64.exe -q -console -varfile <PropertiesFile>
```

或在 Linux 上：

```
Manager-Linux-<Version>.x64.sh -q -console -varfile <PropertiesFile>
```

"-q" 设置强制 install4j 在无人（静默）模式下执行。

"-console" 设置强制消息显示在控制台中 (stdout)。

<PropertiesFile> 自变量是指向标准 Java 属性文件的完整/绝对路径。每个属性通过其在 Windows 趋势科技服务器深度安全防护系统管理中心安装（上述）中的等效 GUI 窗口和设置来识别。例如，“地址和端口”窗口上的趋势科技服务器深度安全防护系统管理中心地址指定如下：

```
AddressAndPortsScreen.ManagerAddress=
```

此文件中的大多数属性都具有可接受的缺省值，可以省略。使用内置数据库的简单安装唯一需要的值包括：

```
LicenseScreen.License  
CredentialsScreen.Administrator.Username  
CredentialsScreen.Administrator.Password
```

所有可能设置的完整描述位于[附录 A：趋势科技服务器深度安全防护系统管理中心设置属性文件](#)。

部署趋势科技服务器深度安全防护系统中继

趋势科技服务器深度安全防护系统管理中心需要至少一个趋势科技服务器深度安全防护系统中继，以便从趋势科技更新服务器提取更新。除了防火墙，所有防护功能都需要更新。

趋势科技服务器深度安全防护系统管理中心仅从趋势科技服务器深度安全防护系统中继获取更新信息。趋势科技服务器深度安全防护系统管理中心的典型配置是在相同计算机上使用共置趋势科技服务器深度安全防护系统中继。如果选择不安装共置趋势科技服务器深度安全防护系统中继，应该在其他计算机上安装趋势科技服务器深度安全防护系统中继。

本节介绍独立型趋势科技服务器深度安全防护系统中继安装。

如果已经在趋势科技服务器深度安全防护系统管理中心安装过程中安装了共置趋势科技服务器深度安全防护系统中继，则不需要执行这些步骤。

完成中继安装后，按照[基本趋势科技服务器深度安全防护系统配置](#)中所述使用趋势科技服务器深度安全防护系统管理中心配置趋势科技服务器深度安全防护系统中继。

准备

注意：使用中继组时，如果 Linux 上的趋势科技服务器深度安全防护系统中继使用 Windows 上的趋势科技服务器深度安全防护系统中继作为其更新源，这些中继将无法正确更新。建议 Windows 和 Linux 上的趋势科技服务器深度安全防护系统中继应该仅配置为从趋势科技全局更新源或从相同平台的中继进行更新。

趋势科技服务器深度安全防护系统中继 (DSR) 计算机上的时钟必须 24 小时与趋势科技服务器深度安全防护系统管理中心 (DSM) 同步。如果 DSR 时钟在 DSM 时钟之后，则“客户端激活”操作将不能成功，因为趋势科技服务器深度安全防护系统管理中心为 DSR 生成的证书尚无效。

注意：如果发生此情况，则会在“系统事件”中记录“客户端激活不成功”事件：“在趋势科技服务器深度安全防护系统管理中心到趋势科技服务器深度安全防护系统客户端协议中发生客户端错误: 收到 HTTP 客户端错误: 证书尚无效”。

复制安装包

将安装文件复制到目标计算机。

安装适用于 Windows 的趋势科技服务器深度安全防护系统中继

注意：趋势科技服务器深度安全防护系统中继安装程序在 Windows 计算机上安装中继服务器和趋势科技服务器深度安全防护系统客户端功能。

请记住，必须在 Windows 计算机上拥有管理员权限才能安装并运行趋势科技服务器深度安全防护系统中继。

步骤 1. 双击安装文件来运行安装包。

单击**下一步**开始安装。

步骤 2. 接受许可协议，然后单击**下一步**继续。

步骤 3. 选择要安装的功能（防恶意软件等一些功能是可选的）。

单击“浏览”指定要安装趋势科技服务器深度安全防护系统中继的位置。

（如果进行升级，则将无法更改安装目录。要安装到其他目录，必须首先卸载先前版本。）

单击**重置**将功能选择重置为缺省设置。

注意：无法取消选择防火墙和 DPI 功能。这些功能构成核心趋势科技服务器深度安全防护系统客户端体系结构的一部分，始终安装这些功能，即使不使用防火墙和 DPI 功能。

单击**磁盘使用量**查看选定功能所需的总空间并与选定目标位置上的可用空间进行比较。

单击**下一步**继续。

步骤 4. 单击**安装**继续安装。

步骤 5. 单击**完成**完成安装。

此时，趋势科技服务器深度安全防护系统中继已在此计算机上安装且正在运行，并且会在每次计算机启动时启动。您会在 Windows 系统托盘中看到**趋势科技服务器深度安全防护系统通知程序**图标。

完成安装后，按照[基本趋势科技服务器深度安全防护系统配置](#)中所述使用趋势科技服务器深度安全防护系统管理中心配置趋势科技服务器深度安全防护系统中继。

注意：在安装期间，网络接口会中断几秒钟，然后恢复正常。如果使用 DHCP，则会生成一个新的请求，这可能导致为恢复的连接生成新的 IP 地址。

注意：建议不要使用 Windows 远程桌面安装趋势科技服务器深度安全防护系统中继，因为安装过程中会暂时断开连接。但是，在启动远程桌面时使用以下命令行参数将允许安装程序在断开连接后在服务器上继续运行：在 Windows Server 2008 或 Windows Vista SP1 和更高版本或 Windows XP SP3 和更高版本上，请使用：

```
mstsc.exe /admin
```

在较早版本的 Windows 上，请使用：

```
mstsc.exe /console
```

完成安装后，按照[基本趋势科技服务器深度安全防护系统配置](#)中所述使用趋势科技服务器深度安全防护系统管理中心配置趋势科技服务器深度安全防护系统中继。

安装适用于 Linux 的趋势科技服务器深度安全防护系统中继

安装适用于 Linux 的趋势科技服务器深度安全防护系统中继：

步骤 1. 要在 Linux 计算机上安装趋势科技服务器深度安全防护系统中继，您需要以 "root" 身份登录。或者，可以使用 "sudo" 工具安装中继。

```
$ su  
Password:
```

步骤 2. 使用 "rpm -i" 安装 ds_agent 软件包：

```
# rpm -i Relay-RedHat_2.6.18_8.EL5_i686-8.0.0-xxxx.i386.rpm

Preparing... #####
[100%]
   1:ds_agent #####
[100%]
Loading ds_filter_im module version 2.4.21-20.EL-i686 [ OK ]
Starting ds_agent: [ OK ]
```

（使用 "rpm -U" 从先前安装版本升级。此方法将保留您的配置文件设置）

步骤 3. 趋势科技服务器深度安全防护系统中继会在安装后自动启动。

在 Linux 上启动、停止和重置趋势科技服务器深度安全防护系统中继：

命令行选项：

```
/etc/init.d/ds_agent start - starts the Agent
/etc/init.d/ds_agent status - displays the status of the Agent
/etc/init.d/ds_agent stop - stops the Agent
/etc/init.d/ds_agent reset - resets the Agent
/etc/init.d/ds_agent restart - restarts the Agent
```

完成安装后，按照[基本趋势科技服务器深度安全防护系统配置](#)中所述使用趋势科技服务器深度安全防护系统管理中心配置趋势科技服务器深度安全防护系统中继。

间隙环境中的趋势科技服务器深度安全防护系统中继和组件更新

在缺省体系结构中，至少配置一个趋势科技服务器深度安全防护系统中继，以便从趋势科技全局更新源下载更新。

但是，如果您的环境要求不允许趋势科技服务器深度安全防护系统中继通过 Internet 连接到更新服务器，则可以使用备用方法将更新的软件包导入到中继，以便分发到其他趋势科技服务器深度安全防护系统软件组件。

使用趋势科技服务器深度安全防护系统中继生成更新软件包

将需要在可以访问 Internet 和趋势科技更新服务器的位置中安装另一个趋势科技服务器深度安全防护系统管理中心和趋势科技服务器深度安全防护系统中继。使用该趋势科技服务器深度安全防护系统管理中心激活中继并将其配置为定期从趋势科技更新服务器下载组件更新。（请参阅[基本趋势科技服务器深度安全防护系统配置](#)。）

中继下载了组件更新后，使用以下过程创建压缩的更新包，您可以将该包传输到需要更新的间隙中继：

步骤 1. 要从命令行创建中继更新包，请输入以下内容：

```
dsa_control /b
```

命令行输出将显示生成的 .zip 文件的名称和位置。

步骤 2. 将中继更新包 .zip 文件复制到要导入更新的趋势科技服务器深度安全防护系统中继的安装位置。

注意：应始终从将导入包的平台上运行的趋势科技服务器深度安全防护系统中继生成趋势科技服务器深度安全防护系统更新软件包。

Linux 上运行的趋势科技服务器深度安全防护系统中继无法成功导入从 Windows 上的趋势科技服务器深度安全防护系统中继生成的更新软件包。如果具有混合（Windows 和 Linux）环境，应始终在 Linux 趋势科技服务器深度安全防护系统中继上生成更新包，以确保所有其他中继都可以导入该包。

将更新导入到间隙趋势科技服务器深度安全防护系统中继

如果组件更新是从趋势科技服务器深度安全防护系统管理中心（预设或手动）启动的，并且趋势科技服务器深度安全防护系统中继无法从配置的更新服务器位置获取更新，则它将自动检查中继更新包 .zip 文件是否存在于它的安装目录位置中。

如果找到中继更新包文件，则趋势科技服务器深度安全防护系统中继会从该文件提取和导入更新。

注意：请记住，在更新成功导入到中继后移除中继更新包 .zip 文件。

配置间隙中继的更新源

间隙中继将尝试联系更新服务器以检查是否存在更新。要避免更新失败警报，请将中继设置为将自己用作更新源。

1. 在中继的**详细信息**窗口中，转至“系统”>“系统设置”>“更新”
2. 在**中继**区域中，选择“其他更新源:”并输入 <https://localhost:4122>
3. 单击**保存**

VMware 集成的其他配置

准备趋势科技服务器深度安全防护系统/VMware 环境的其他配置

本节列出完成趋势科技服务器深度安全防护系统与 VMware 环境集成以进行无客户端防护所需的其他任务。

此时.....

- 已经按照[为无客户端防护准备 VMware 环境](#)中所述设置了 VMware 环境
- 已经安装了趋势科技服务器深度安全防护系统管理中心（和数据库）
- 已经在 DSM 上安装和配置了趋势科技服务器深度安全防护系统中继

ESX/ESXi 主机 B 上的 VMware vShield Endpoint 部署

请参考[为无客户端防护准备 VMware 环境](#)中的图。

- 步骤 1. 通过浏览到 `https://<vSM-ip>` 来登录到 vShield Manager
输入 `admin:default` 作为登录帐户
- 步骤 2. 在右侧**配置**选项卡中，输入 vCenter Server 信息
- 步骤 3. 在左侧导航窗格中选择**主机与群集**
- 步骤 4. 选择趋势科技服务器深度安全防护系统要保护的 ESX/ESXi 虚拟机监控程序（主机 B）
在右侧窗格中，单击具有服务项目 **vShield Endpoint** 的**安装**链接
- 步骤 5. 在**选择要安装/升级的服务**中，选中 **vShield Endpoint** 并单击窗口右上方的**安装**按钮
- 步骤 6. 安装后，确保服务 **vShield Endpoint** 正确显示安装的版本（**安装**链接已更改为**卸载**）
- 步骤 7. 在 vCenter 控制台上，转至“vShield Manager 控制台”选项卡
以 `admin:default` 身份登录
- 步骤 8. 键入 `enable` 命令打开授权模式，使用 `default` 作为密码

- 步骤 9. 键入 **reboot** 重新启动 vShield Manager
- 步骤 10. 通过浏览到 <https://<vSM-ip>> 来登录到 vShield Manager
 - 确保显示 vShield Manager Web 控制台
 - 验证 ESX/ESXi 的状态，确保为 vShield Endpoint 显示正确的版本信息

将 vCenter 添加到 DSM 的被管理计算机列表

必须使用具有完全访问权限的 DSM 用户帐户执行趋势科技服务器深度安全防护系统管理中心配置。

- 步骤 1. 从 DSM 的左侧导航面板选择**计算机 > 新建 > 添加 VMware vCenter...**
- 步骤 2. 输入 vCenter Server IP 地址（或主机名）、vCenter 的用户名和密码。单击**下一步**。

注意： 确保 DNS 已配置且能够将 FQDN 解析为此环境中的所有计算机使用的 IP 地址，否则输入 IP 地址。

- 步骤 3. 输入 vShield Manager Server 地址、用户名和密码。
（也可在以后从 DSM 配置此信息）。
单击**下一步**。
- 步骤 4. 接受 vShield Manager SSL 证书。
- 步骤 5. 接受 VMware 缺省证书。
- 步骤 6. 查看 vCenter 信息。单击**完成**。
将显示“已成功添加 VMware vCenter”消息，单击**关闭**。
- 步骤 7. 检查**计算机 > vCenter - [名称]**，确保列出 vCenter。

注意： 在具有 3000 台以上的计算机向 vCenter Server 报告的非常大的环境中，此重要过程可能要花费 20 到 30 分钟来完成。可以检查 vCenter **新任务** 部分来验证是否有活动正在运行。

为趋势科技服务器深度安全防护系统虚拟设备部署准备 ESX/ESXi

本节介绍如何准备 VMware 环境以使用 DSVa 进行无客户端防护。

此时.....

- 已经按照[为无客户端防护准备 VMware 环境](#)中所述设置了 VMware 环境
- 已经安装了趋势科技服务器深度安全防护系统管理中心（和数据库）
- 已经在 DSM 上安装和配置了趋势科技服务器深度安全防护系统中继
- 已经在受保护的主机 ESX/ESXi 上部署了 VMware vShield Endpoint，并且 vCenter 已经添加到 DSM 的被管理计算机列表，请参阅[VMware 集成的其他配置](#)

将趋势科技服务器深度安全防护系统软件包导入到 DSM 中

将趋势科技服务器深度安全防护系统过滤器驱动程序 (DSFD) 和趋势科技服务器深度安全防护系统虚拟设备 (DSVA) 导入到 DSM 中

必须使用具有完全访问权限的 DSM 用户帐户执行趋势科技服务器深度安全防护系统管理中心配置。

步骤 1. 在 DSM 中，选择**系统 > 更新**。

步骤 2. 向下滚动并从**软件更新**区域选择**导入软件...**。

根据所使用的虚拟机监控程序的版本，浏览并选择 FilterDriver-ESX_5.0-8.0.0-xxxx.x86_64.zip 或 FilterDriver-ESX_4.1-8.0.0-xxxx.x86_64.zip。

单击**下一步**，并在下一窗口中单击**完成**。

步骤 3. 从**软件更新**区域选择**导入软件**。

浏览并选择 Appliance-ESX-8.0.0-xxxx.x86_64.zip。

单击**下一步**，然后等待显示“软件属性”窗口并选择**完成**。

注意： 根据网络带宽，软件包上传可能会花费 5-10 分钟。

步骤 4. 单击**查看导入的软件**并确保过滤器驱动程序和 DSVa 均已导入。

通过安装过滤器驱动程序为虚拟设备部署准备 ESX/ESXi

重要事项： 对于此任务，ESX/ESXi 将被置于维护模式。在此 ESX/ESXi 上运行的所有虚拟机必须停止/暂停或 vMotion 到其他 ESX/ESXi 主机（确保设置具有 vMotion 支持的群集服务器，以便可以自动执行此操作）。

注意： 要安装过滤器驱动程序，必须将 ESX/ESXi 上的主机配置文件接受级别设置为“接受 VMware”、“支持合作伙伴”或“支持团体”。可以在 vCenter Client 中更改此设置，方法是选择 ESX/ESXi、转至配置选项卡并编辑主机镜像配置文件接受级别。

- 步骤 1. 在 DSM 中，选择**计算机 > vCenter > 主机和群集**。
- 步骤 2. 在“计算机”列表中找到 ESX/ESXi 主机（其“状态”列应显示为“未准备”），右键单击它，然后选择**操作 > 准备 ESX** 以显示**准备 ESX Server 向导**。单击**下一步**。
- 步骤 3. 选择**是**允许趋势科技服务器深度安全防护系统管理中心自动使 ESX/ESXi 进入和退出维护模式。
单击**完成**。
- 步骤 4. ESX/ESXi 准备过程将完成所有活动，而无需进一步的输入。
(ESX/ESXi 将置于维护模式，将安装趋势科技服务器深度安全防护系统过滤器驱动程序，且将重新启动 ESX/ESXi)。

步骤 5. 该过程完成后，可以选择继续进行下一步，即部署趋势科技服务器深度安全防护系统虚拟设备。

选择“不，稍后部署”。单击“关闭”。（趋势科技服务器深度安全防护系统虚拟设备安装在后面讲述）。

步骤 6. 这将完成 ESX/ESXi 准备。

注意：您可以在 VMware vSphere Client 管理控制台中监控此准备过程。

步骤 7. 返回**计算机 > vCenter**，并确保 ESX/ESXi 的状态设置为“已准备”。

步骤 8. 转至 vSphere Client。选择 **ESX/ESXi Server > “配置”选项卡 > 网络**。检查是否已创建 vSwitch。

步骤 9. SSH 到 ESX/ESXi Server 中并运行以下命令来确认正确安装了 VMware 和趋势科技驱动程序。

```
vmkload_mod -l | grep dvfilter
```

注意：dvfilter 随 ESX/ESXi 安装一起提供。dvfilter-dsa 是准备过程完成时安装到 ESX/ESXi 的趋势科技驱动程序。

对于 ESX/ESXi 4.1:

```
esxupdate query | grep Trend
```

对于 ESXi 5.0:

```
esxcli software vib list | grep Trend
```

检查是否显示了 dvfilter-dsa 的正确版本和状态。

部署趋势科技服务器深度安全防护系统虚拟设备

本节介绍如何安装和激活 DSVA 来提供无客户端防护。

此时.....

- 已经按照[为无客户端防护准备 VMware 环境](#)中所述设置了 VMware 环境
- 已经安装了趋势科技服务器深度安全防护系统管理中心（和数据库）
- 已经在 DSM 上安装和配置了趋势科技服务器深度安全防护系统中继
- 已经在受保护的主机 ESX/ESXi 上部署了 VMware vShield Endpoint，并且 vCenter 已经添加到 DSM 的被管理计算机列表，请参阅[VMware 集成的其他配置](#)
- 已经为趋势科技服务器深度安全防护系统虚拟设备部署准备了受保护的 ESX/ESXi 主机

注意：有关所需 VMware 权限的详细列表，请参阅[附录 K：DSVA 部署的最低 VMware 权限](#)。

将趋势科技服务器深度安全防护系统设备 (DSVA) 部署到 ESX/ESXi

必须使用具有完全访问权限的 DSM 用户帐户执行趋势科技服务器深度安全防护系统管理中心配置。

- 步骤 1. 在 DSM 中，选择**计算机 > vCenter**。
- 步骤 2. 右键单击受保护的 ESX/ESXi 主机并选择**操作 > 部署设备**。单击**下一步**。
- 步骤 3. 输入设备的**设备名称**并为设备选择**数据存储**。
选择数据中心的**文件夹**，然后选择设备的**管理网络**。
单击**下一步**。
- 步骤 4. 定义**设备主机名**。为设备输入 **IPv4 地址**和/或 **IPv6 地址**。（缺省情况下启用 DHCP）。
单击**下一步**。

- 步骤 5. 选择完整配置格式（建议）。
- （**完整配置格式**使用分配的全部磁盘空间，而**精简配置格式**使用最少的磁盘空间）。
- 单击**完成**，并等待几分钟以完成 DSVa 上传。
- 步骤 6. 在下一窗口中接受 SSL 证书并等待几分钟，直到部署了设备。
- 您应该看到“已成功部署设备”消息。
- 步骤 7. 在“激活趋势科技服务器深度安全防护系统设备”部分下，选择“**不，稍后激活**”。
- （激活在后面讲述）。
- 单击**关闭**。
- 步骤 8. 检查 vCenter 以确保 DSVa 已启动并且正在运行。
- 步骤 9. 此时，虚拟设备会与其他计算机一同显示在 DSM **计算机 > vCenter** 列表中的 vCenter 组中。

验证步骤:

- 检查 1. 在 vCenter 控制台上，转至 DSVa **控制台** 选项卡。
- 记下 DSVa 的管理地址以及它是使用 eth0 还是 eth1。
- 确保正确配置网络适配器并且它们位于正确的网络池中。
- 检查 2. 转至虚拟机**属性 > 摘要**选项卡，然后单击**编辑设置**。
- 检查 3. 转至**硬件**选项卡，其中提供了 3 个接口。

注意: 网络适配器 1 始终是管理网络。DSVa 使用此接口与趋势科技服务器深度安全防护系统管理中心通信。

网络适配器 2 由 DSVa 用来与 VM 内核 VNIC IP 通信。检查 ESXi 网络配置，确保 **vm-service-trend-pg** 位于与 **vm-service-vmknics-pg** 相同的虚拟交换机上。

检查 4. 确保可以 ping 趋势科技服务器深度安全防护系统管理中心。

键入命令：

```
sudo ping <趋势科技服务器深度安全防护系统管理中心的 FQDN>
```

注意： 确保 DNS 配置正确并且能够将 FQDN 解析为此环境中的所有计算机使用的 IP 地址。否则，使用 IP 地址。

增加 DSVA 内存（可选）

缺省情况下，向 DSVA 分配 1GB 内存。

将内存增加到 4GB，以便 DSVA 保护 33 - 64 台虚拟机。

将内存增加到 8GB，以便 DSVA 保护 65 台以上的虚拟机。

增加 DSVA 内存

步骤 1. 在 vCenter 控制台中，转至 DSVA **控制台** 选项卡。

步骤 2. 关闭 DSVA 电源。

```
sudo shutdown -h now
```

步骤 3. 转至**摘要 > 编辑设置 > 硬件**选项卡。

步骤 4 向虚拟设备分配所需的内存量。

步骤 5 打开 DSVA 电源。

对 DSVA 禁用 DRS 和 HA

步骤 1. 在 vSphere Client 中，打开群集设置。

步骤 2. 关闭 HA 和 DRS。

激活趋势科技服务器深度安全防护系统虚拟设备

必须使用具有完全访问权限的 DSM 用户帐户执行趋势科技服务器深度安全防护系统管理中心配置。

步骤 1. 在 DSM 中，选择**计算机 > vCenter**。

步骤 2. 右键单击 DSVA 计算机并选择**操作 > 激活设备**。

单击**下一步**。

步骤 3. 对于安全配置文件，选择趋势科技服务器深度安全防护系统虚拟设备。

单击**下一步**。

将启动激活过程。

步骤 4. DSVA 将在 vShield Manager 中注册自己。您将看到多个任务在 vCenter 控制台中执行。

注意： DSVA 需要 vShield Manager 配置位于 ESX/ESXi 上的每台计算机的 VMX 文件。根据虚拟机数目，可能要花费几个小时来完成激活。

（如果 vShield Manager 遇到问题，DSVA 可能无法激活。检查是否可以打开 vShield Manager Web 控制台。如果它未响应，您可以重新启动 vShield Manager 并在 vShield 启动后等待几分钟，然后再次尝试 DSVA 激活。）

步骤 5. 在**激活主机虚拟机**下，选择“不，稍后激活”。

（此步骤将在后面讲述）

单击**关闭**。

步骤 6. DSVA 将成功激活。

返回**计算机 > vCenter**并确保 DSVA 的状态设置为**被管理 (联机)**。

注意： 确保“防恶意软件就绪”状态设置为“是”。如果状态为“否”，请检查“ESX/ESXi 防恶意软件状态”。确保 dvfilter 和 dvfilter-dsa 驱动程序都在运行。

激活客户虚拟机

向 ESX/ESXi 分配客户虚拟机

- 步骤 1. 向 ESX/ESXi 主机移动计算机。
- 步骤 2. 如果计算机处于脱机状态，打开计算机电源。

激活虚拟机

- 步骤 1. 在 DSM 中，选择**计算机 > vCenter**。
- 步骤 2. 右键单击虚拟机并选择**操作 > 激活**。
- 步骤 3. 右键单击虚拟机并选择**操作 > 分配安全配置文件**。
- 步骤 4. 要激活防恶意软件防护，请应用 **Windows 防恶意软件保护** 安全配置文件。（此操作仅启用防恶意软件功能）。
- 步骤 5. 检查虚拟机的状态并确保**防恶意软件**状态为**实时**。
- 步骤 6. 分配安全配置文件之后，将立即自动开始重新生成完整性监控基线。
生成基线后（这会花费一些时间），可以执行完整性的自动或手动扫描。

验证步骤：

如果正在激活防恶意软件防护，但是防恶意软件状态显示防恶意软件引擎脱机，则可以检查一些事项：

- 检查 1. 确保 VMware 工具在虚拟机上是最新的
- 检查 2. 确保 vShield Endpoint 客户端已安装并且 vsepflt 驱动程序在 VM 上运行：

```
sc query vsepflt
```
- 检查 3. 确保趋势科技服务器深度安全防护系统管理中心可以将信息与 vCenter 同步
- 检查 4. 在 DSM 的**计算机**列表中，确保 ESX/ESXi 状态为“vShield Endpoint: 已安装”
- 检查 5. 在 DSM 的**计算机**列表中，确保 DSVa 状态为“vShield Endpoint: 已注册”
- 检查 6. 确保受保护计算机的防恶意软件状态为**打开或实时**

自动为无状态 ESXi 部署设备

除了 ESXi 5.0 标准系统要求之外，还必须安装以下各项，且必须将其配置为自动为无状态 ESX 部署设备：

- VMware Virtual Center，已经按照[为无客户端防护准备 VMware 环境](#)中所述对其进行了设置
- TFTP Server
- VMware Auto-deploy
- 如果使用 DHCP，则必须为 PXE 配置 DHCP Server
- 主机配置文件，用于在 vCenter 自动启动时立即通过 vCenter 处理 ESXi 的配置部分
- 在 Windows 计算机上安装的 vSphere powerCLI，它可以通过网络访问 vCenter Server
- 趋势科技下载站点中的趋势科技过滤器驱动程序和设备：
<http://www.trendmicro.com/download/zh-cn/>

安装 TFTP Server

安装 TFTP Server，如 WinAgents TFTP Server。在 Windows 服务器上创建一个目录，例如：E:\tftproot，并使此目录成为您的 TFTP 根目录。

安装 VMware Auto-deploy

1. 安装 vCenter Auto Deploy 软件。可以在您的 vCenter Server 上安装此软件，或者可以在单独的 Windows 服务器上运行此软件并将其配置为指向您的 vCenter Server。
您将需要提供 vCenter Server 的 IP 以及凭证。
2. 在您的 vSphere Infrastructure Client 中安装插件。您可以在“主页”选项卡中看到 Auto Deploy 图标。
3. 将引导镜像添加到 TFTP Server 根目录，如下所示：
 - a. 在 vSphere Client 中，单击 Auto Deploy 插件。
 - b. 选择下载 TFTP 引导 Zip 并将此 ZIP 文件解压缩到您的 TFTP 根目录中。

- c. 要测试您的配置的情况，请启动 ESXi 主机，或者仅为测试而启动 VM。确保主机或 VM 使用 PXE 引导。您应该会看到为它分配了一个 IP 地址，并且开始加载 TFTP 镜像。
- d. 接下来，您将看到尽管已加载 TFTP 镜像，但不存在任何与此主机关联的 ESXi 镜像。此窗口还会显示许多计算机属性，以后尝试用规则约束主机时可以使用这些属性。

为 PXE 配置 DHCP Server

如果使用 DHCP，请为 PXE 引导配置 DHCP Server。这些特定步骤取决于您为 DHCP 使用的产品。您需要在您的 DHCP Server 上打开该作用域，并添加以下选项：

```
066 - Boot server host name: <ip of your TFTP / PXE boot server>
067 - Boot file name: undionly.kpxe.vmw-hardwired
```

将趋势科技服务器深度安全防护系统过滤器驱动程序添加到 VIB 镜像

为使趋势科技过滤器驱动程序 vib 自动作为 PXE 引导镜像的一部分进行部署，请采用某个缺省 ESXi 镜像，并将趋势科技过滤器驱动程序 vib 作为新镜像的一部分重新生成该镜像，然后更名该文件。例如，如果使用 VMware-ESXi-5.0.0-441354-depot.zip，请将该文件命名为 VMware-ESXi-5.0.0-441354-Trend-dvfilter-depot.zip。

将过滤器驱动程序与一个主机配置文件一起添加到镜像，这样可以允许 ESXi 对趋势科技服务器深度安全防护系统管理中心显示为“已准备”。

可从 VMware 获得 VMware vCenter Server Appliance，它是已经提供 PXE 引导功能的预配置基于 Linux 的虚拟机。与使用 Windows vCenter Virtual Center 相比，使用 VMware vCenter Server Appliance 需要的自动部署设置更少。有关 VMware vCenter Server Appliance 安装的信息，请参阅发布的 *vSphere 安装和设置* 相关内容。

安装 vSphere PowerCLI

1. 下载 vSphere 5 PowerCLI 并将其安装在将处理镜像的服务器上。
2. 要测试 VMware PowerCLI 是否正常工作，请启动 VMware vSphere PowerCLI 命令提示符并运行：Get-DeployCommand。

此操作将提供处理 Auto Deploy 所需的所有命令的列表。此时，已安装 vSphere Auto Deploy 的所有必需项。

准备第一个镜像

要准备第一个镜像，需要提供：

- 主机的 IP 地址和 DNS 主机名
- 主机的 MAC 地址
- 镜像名称（从 VMware 站点下载的文件名称），例如，"VMware-ESXi-5.0.0-441354-Trend-dvfilter-depot.zip"
- 镜像名称（在添加到库中之后），例如，"ESXi-5.0.0-441354-standard"
- 您的 SoftwareDepot 的目录，该目录将由 Auto Deploy 软件使用

准备镜像

1. 创建名为 "Staging" 的目录。
2. 创建一个称为 "VIB-downloads" 的目录，您将在其中存储要部署的 VIB 和镜像。
3. 将基本 VMware ESXi 5.0 镜像部署到新主机，而不进行任何进一步的配置。
4. 基于 MAC 地址将该镜像附加到主机，这样，在您的 vCenter 中，该主机将显示在 "Staging" 文件夹中命名的一个文件夹中。由于它没有任何配置，因此它还不会显示在群集中。
5. 为 MAC 地址创建 DHCP 保留。
6. 在您的 DHCP 作用域中，创建保留并使用正确的主机名。在 DNS 中，为此主机名和 IP 地址创建一个 A-record，并为其提供一个 PTR/反向查找记录。

将新镜像添加到库中

1. 运行以下命令以将该镜像插入到 "SoftwareDepot" 目录中：

```
Add-EsxSoftwareDepot "E:\VIB-downloads\VMware-ESXi-5.0.0-441354-depot.zip"
```

2. 运行以下命令以查看您的库中存在哪些镜像：

```
Get-EsxImageProfile
```

现在可以部署该镜像了。

部署第一个主机

主机重新启动之后，将拾取 TFTP 镜像并向 vSphere Auto Deploy 服务器请求镜像。

注意：创建规则时，存在两个规则集：一个 "working-set" 和一个 "active-set"。
"working-set" 充当规则库，而 "active-set" 是对主机可用的规则。

部署主机

1. 创建一个规则以使用 "New-DeployRule" 命令将镜像连接到主机：

```
New-DeployRule -Name "<rule_name>" -Item "<image_name>", "<folder_name>"  
-Pattern "mac=<mac_address>"
```

刚创建的新规则名为 "PreStaging"。该规则可确保将称为 "ESXi-5.0.0-441354-standard" (Get-EsxImageProfile) 的镜像部署到具有指定 MAC 地址的主机，并将该镜像置于 vCenter 中的 "Staging" 文件夹中。

例如，以下命令会创建一个称为 "PreStaging" 的规则，并确保将称为 "ESXi-5.0.0-441354-standard" (Get-EsxImageProfile) 的镜像部署到 MAC 地址为 00:1a:92:b8:da:77 的主机，并将该镜像置于 vCenter 中的 "Staging" 文件夹中：

```
New-DeployRule -Name "PreStaging" -Item "ESXi-5.0.0-441354-standard",  
"Staging" -Pattern "mac=00:1a:92:b8:da:77"
```

2. 要查看已创建的规则，请使用以下命令：

```
Get-DeployRule
```

这是 "working set" 中的一个规则。

3. 要创建 "active set" 的规则部分，请使用以下命令：

```
Add-DeployRule -DeployRule "PreStaging"
```

4. 要检查 "active set" 中的规则，请运行 Get-DeployRuleSet 命令。
5. 启动要安装的主机。该主机应该显示在您的 vCenter 中。

配置主机配置文件

在您的主机显示在 vCenter 中之后，请配置主机配置文件（包括 vSwitch），附加数据存储，并确认 NTP 设置。由于该主机是无盘主机，因此请设置 syslog 和核心转储位置。（可以在 vCenter 工具目录中找到 syslog 工具和 Coredump 实用工具。）

注意：如果要配置主机并在此时重新启动，那么所有更改都将丢失。要保留配置，必须定义一个主机配置文件。

注意：使用高级主机配置时，您可能希望使用 vSphere Enable/Disable Profile Configurations 选项进行故障排除。

在 ESXi 主机收到错误时，您的服务器现在还可以接收核心转储。

1. 将您的 ESXi 主机配置为使用 Coredump 服务器。要执行此操作，请进入您的主机的配置窗口，转到安全配置文件并启用 SSH，然后使用您的 SSH 客户端登录到 ESXi 控制台并运行以下命令：

```
esxcli system coredump network set --interface-name vmk0 --server-ipv4
192.168.0.40 --server-port 6500
esxcli system coredump network set --enable true
esxcli system coredump network get
```

最后一行指示是否已启用新设置。

2. 从 ESXi 主机注销并切换回您的 vSphere Client。

重要事项：确保再次禁用 SSH，因为我们将生成一个配置文件，且不希望在此配置文件运行的所有新主机上启用 SSH。

3. 在 vSphere Client 中，转到 "Host and Clusters" 视图，然后选择您刚准备好的主机。
4. 右键单击该主机，然后选择 **Create Profile from host**。
5. 为配置文件提供一个名称，例如 "Profile-Cluster01"。
6. 在 vSphere Client 中，使用 Host Profiles 部分将配置文件附加到此主机，然后检查配置文件是否合规。

使用主机配置文件自动部署主机

上面创建的第一个规则确保会将具有特定 MAC 地址的主机连接到标准镜像并置于 "Staging" 文件夹中：

```
New-DeployRule -Name "PreStaging" -Item "ESXi-5.0.0-441354-standard",  
"Staging" -Pattern "mac=00:1a:92:b8:da:77"
```

自动部署主机

1. 创建一个规则以将主机移动到生产群集中。将您在 DHCP 作用域中使用的 IP 范围用于 ESXi 主机，并在 DHCP 作用域中为每个主机创建一个保留，并且使用以下格式创建一个 DNS 记录：

```
New-DeployRule -Name "<rule_name>" -Item "<image_name>",  
"<cluster_name>", "<host_profile>" -Pattern "ipv4=<DHCP-range>"
```

例如，在以下命令中：

```
New-DeployRule -Name "Prod-CL01" -Item "ESXi-5.0.0-441354-standard",  
"CL01", "Profile-Cluster01" -Pattern "ipv4=192.168.0.100-192.168.0.110"
```

"Prod-CL01" 是规则的名称，"CL01" 是群集的名称，"Profile-Cluster01" 是主机配置文件的名称，而 ipv4 是 DHCP 范围。

2. 在 "working-set" 中，现在存在两个规则 ("PreStaging" 和 "Prod-CL01")，而在 "active-set" 中，"PreStaging" 规则处于活动状态。使用 remove 命令，从 "active-set" 中移除 "PreStaging" 规则，接下来我们将 "Prod-CL01" 添加到 "active-set" 中并仔细检查我们已执行的事项：

```
Remove-DeployRule -DeployRule "PreStaging"  
Add-DeployRule -DeployRule "Prod-CL01"  
Get-DeployRuleSet
```

配置现在已完成。重新启动您的主机之后，这些主机将返回，并被添加到 CL01 群集中，从而作为一个正常主机完全参与。

部署趋势科技服务器深度安全防护系统客户端

本节介绍如何在每种类型的受支持平台上安装和激活趋势科技服务器深度安全防护系统客户端。

[系统要求](#)中提供了受支持平台的完整列表

此时.....

- 已经安装了趋势科技服务器深度安全防护系统管理中心（和数据库）。
- 已经在 DSM 上安装和配置了趋势科技服务器深度安全防护系统中继。

有关在您所选平台上的趋势科技服务器深度安全防护系统客户端安装，请遵循本节中的说明。

完成安装后，通过遵循[基本趋势科技服务器深度安全防护系统配置](#)中的步骤执行以下操作来使用趋势科技服务器深度安全防护系统管理中心配置计算机上防护：

- 向趋势科技服务器深度安全防护系统管理中心添加计算机
- 在计算机上启用防护

准备

注意：趋势科技服务器深度安全防护系统客户端 (DSA) 计算机上的时钟必须 24 小时与趋势科技服务器深度安全防护系统管理中心 (DSM) 同步。如果 DSA 时钟在 DSM 时钟之后，则“客户端激活”操作将不能成功，因为趋势科技服务器深度安全防护系统管理中心为 DSA 生成的证书尚无效。如果发生此情况，则会在“系统事件”中记录“客户端激活不成功”事件：“在趋势科技服务器深度安全防护系统管理中心到趋势科技服务器深度安全防护系统客户端协议中发生客户端错误: 收到 HTTP 客户端错误: 证书尚无效”。

复制安装包

将安装文件复制到目标计算机。

注意：CentOS 使用 Red Hat 5 RPM，将在趋势科技服务器深度安全防护系统管理中心中显示为 "Red Hat"。要在 CentOS 上使用趋势科技服务器深度安全防护系统客户端，请遵循安装 Linux 客户端的说明。

安装适用于 Windows 的趋势科技服务器深度安全防护系统客户端

注意：请记住，必须在 Windows 计算机上拥有管理员权限才能安装并运行趋势科技服务器深度安全防护系统客户端。

步骤 1. 双击安装文件来运行安装包。

单击**下一步**开始安装。

步骤 2. 阅读许可协议并单击**下一步**。

步骤 3. 选择要安装的功能并单击**浏览**指定要安装趋势科技服务器深度安全防护系统客户端的位置。

（如果进行升级，则将无法更改安装目录。要安装到其他目录，必须首先卸载先前版本。）

单击**重置**将功能选择重置为缺省设置。

注意：无法取消选择防火墙和 DPI 功能。这些功能构成核心趋势科技服务器深度安全防护系统客户端体系结构的一部分，始终安装这些功能，即使不使用防火墙和 DPI 功能。

单击**磁盘使用量**查看选定功能所需的总空间并与选定目标位置上的可用空间进行比较。

单击**下一步**。

步骤 4. 单击**安装**继续安装。

步骤 5. 单击**完成**完成安装。

此时，趋势科技服务器深度安全防护系统客户端已在此计算机上安装且正在运行，并且会在每次计算机启动时启动。

注意：在安装期间，网络接口会中断几秒钟，然后恢复正常。如果使用 DHCP，则会生成一个新的请求，这可能导致为恢复的连接生成新的 IP 地址。

注意： 建议不要使用 Windows 远程桌面安装趋势科技服务器深度安全防护系统客户端，因为安装过程中会暂时断开连接。但是，在启动远程桌面时使用以下命令行参数将允许安装程序在断开连接后在服务器上继续运行：在 Windows Server 2008 或 Windows Vista SP1 和更高版本或 Windows XP SP3 和更高版本上，请使用：

```
mstsc.exe /admin
```

在较早版本的 Windows 上，请使用：

```
mstsc.exe /console
```

安装适用于 Linux 的趋势科技服务器深度安全防护系统客户端

注意： 安装趋势科技服务器深度安全防护系统客户端将禁用 iptables。

要求：

对于 SuSE：

对于 SuSE 11，开始安装过程之前，在目标计算机上的 /etc/init.d/jexec 中，将以下行添加到 # Required-Start: \$local_fs 之后：

```
# Required-Stop:
```

在 Red Hat 或 SuSE 上安装趋势科技服务器深度安全防护系统客户端：

注意： 以下说明同时适用于 Red Hat 和 SuSE。要在 SuSE 上安装，请使用 SuSE RPM 名称代替 Red Hat。

步骤 1. 以 "root" 身份登录。或者，可以使用 "sudo" 工具安装客户端。

```
$ su
Password:
```

步骤 2. 使用 "rpm -i" 安装 ds_agent 软件包:

```
# rpm -i Agent-RedHat_2.6.18_8.EL5_i686-8.0.0-xxxx.i386.rpm
Preparing... #####
[100%]
   1:ds_agent #####
[100%]
Loading ds_filter_im module version 2.4.21-20.EL-i686 [ OK ]
Starting ds_agent: [ OK ]
```

(使用 "rpm -U" 从先前安装版本升级。此方法将保留您的配置文件设置)

步骤 3. 趋势科技服务器深度安全防护系统客户端会在安装后自动启动。

在 Ubuntu 上安装趋势科技服务器深度安全防护系统客户端:

要在 Ubuntu 上安装, 请使用以下命令:

```
sudo dpkg -i <driver_deb_pkg>
```

其中 <driver_deb_pkg> 是 Debian 软件包, 具有在 <DS>/src/dsa/agent/deb/ 目录中生成和放置的驱动程序。

在 Linux 上启动、停止和重置客户端:

命令行选项:

```
/etc/init.d/ds_agent start - starts the Agent
/etc/init.d/ds_agent status - displays the status of the Agent
/etc/init.d/ds_agent stop - stops the Agent
/etc/init.d/ds_agent reset - resets the Agent
/etc/init.d/ds_agent restart - restarts the Agent
```

安装适用于 Solaris 的趋势科技服务器深度安全防护系统客户端

要求:

对于 Solaris Sparc/8 和 Sparc/9:

```
libgcc 3.4.6 or better (www.sunfreeware.com)
libiconv 1.11 or better (www.sunfreeware.com)
pfil_Solaris_x.pkg
Agent-Solaris_5.x_sparc-8.x.x-yyy.sparc.pkg.gz
```

注意: "x" 将为 8 或 9, 具体取决于安装所在的 Solaris 操作系统的版本。

对于 Solaris Sparc/10:

```
SUNWgccruntime, GCC Runtime libraries
pfil_Solaris_10sparc.pkg (see note below)
Agent-Solaris_5.10_sparc-7.x.x-yyy.sparc.pkg.gz
```

对于 Solaris X86/10:

```
SUNWgccruntime, GCC Runtime libraries
pfil_Solaris_10x86.pkg (see note below)
Agent-Solaris_5.10_i386-8.x.x-xxx.x86_64.pkg.gz
```

注意: Solaris 10 Update 3 之前 (包括其在内) 的所有 Solaris 版本均要求安装 pfil。

安装 Solaris 10 客户端:

注意: 对于 Solaris 10 Update 4 及更高版本, 仅需执行步骤 5 和 6。

步骤 1. 获取所需的所有软件包 (请参阅前述内容)

步骤 2. 准备删除 Sun 版本的 ipfilter 和 pfil

a. 注意版本号和其他信息

```
modinfo | grep pfil
modinfo | grep ipf
pkginfo -l SUNWipfr
pkginfo -l SUNWipfu
```

b. 检查状态

```
svcs -x ipfilter
svcs -x pfil
```

- c. 如果这些命令中的任何一个出错，则应该在继续下一步操作之前更正问题。还检查 Sun 版本的 pfil 是否正确地加载。

```
ifconfig ce0 modlist      (使用您的网络接口)
```

并且查看 pfil 是否位于 "ip" 和网络接口之间的列表中。如果不是，则检查网络接口类型是否在 /etc/ipf/pfil.ap 中取消注释，然后重新启动并重试。在确信 Sun 版本的 ipfilter/pfil 正确工作之前，不要进行进一步操作。

- d. 导出当前 ipfilter 和 pfil 服务配置

```
svccfg export network/pfil > /var/tmp/pfil.svc  
svccfg export network/ipfilter > /var/tmp/ipfilter.svc
```

- e. 禁用这两个服务

```
svcadm -v disable pfil  
svcadm -v disable ipfilter
```

- f. 重新启动系统

步骤 3. 删除 Sun 版本的 ipfilter 和 pfil

- a. 检查重新启动后是否未加载内核模块

```
modinfo | grep ipf  
modinfo | grep pfil
```

- b. 在删除 Sun 软件包之前保存某些 Sun pfil 文件的副本

删除 Sun 软件包时将删除这些文件，但您需要它们来启动公共域版本的 pfil。

```
cp /lib/svc/method/pfil /lib/svc/method/pfil.dist  
cp /usr/sbin/pfiled /usr/sbin/pfiled.dist  
cp /etc/ipf/pfil.ap /etc/ipf/pfil.ap.dist
```

- c. 移除 Sun IPFilter 软件包

```
pkgrm SUNWipfu  
pkgrm SUNWipfr
```

- d. 重新启动系统

步骤 4. 安装 pfil

- a. 恢复 pfil 服务配置文件

```
cp /lib/svc/method/pfil.dist /lib/svc/method/pfil
```

- b. 安装 pfil

```
pkgadd -d pfil_Solaris_10xxxx.pkg all
```

- c. 安装后，移除不需要的 Solaris 9 启动脚本，pfil 将使用 "svcadm"

```
rm /etc/rc2.d/S10pfil
rm /etc/rcS.d/S10pfil
rm /etc/init.d/pfil
```

- d. 恢复 pfil 配置文件（注意，公共域 pfil 的配置文件位于 /etc/opt/ipf 中，而 Sun 的配置文件位于 /etc/ipf 中，由于步骤 4.d 中保存的服务配置文件仍指向 Sun 的配置文件路径，因此您应使用 /etc/ipf 以与 Solaris 10 保持一致。）

```
cp /etc/ipf/pfil.ap.dist /etc/ipf/pfil.ap
```

- e. 配置 pfil 网络设备

```
vi /etc/ipf/pfil.ap （取消注释相应的设备）
```

- f. 启用 pfil 服务

```
svcadm -v enable pfil
```

如果收到有关此命令的错误，说明 pfil 的服务配置文件已被删除，需要通过步骤 4.d 中的导出副本恢复

```
svccfg -v import /var/tmp/pfil.svc
svcadm -v enable pfil
```

- g. 重新启动系统

- h. 确认 pfil 服务已启动

```
modinfo | grep pfil
```

这会显示公共域版本的 pfil

(pfil 流模块 2.1.11)

(pfil 流驱动程序 2.1.11)

还检查是否已将 pfil 正确加载到 tcp/ip 堆栈中

```
ifconfig ce0 modlist    (使用您的网络接口)
```

如果不是，则检查网络接口类型是否在 pfil 配置文件 /etc/ipf/pfil.ap 中取消注释，然后重新启动并重试。

- 步骤 5. 确保已安装 SUNWgccruntime。如果未安装，则找到该软件包并进行安装：

```
pkgadd -d .SUNWgccruntime
```

- 步骤 6. 安装客户端：

```
gunzip Agent-Solaris_5.x_sparc-8.x.x-xxxx.sparc.pkg.gz
pkgadd -d Agent-Solaris_5.x_sparc-8.x.x-xxxx.sparc.pkg all
```

安装 Solaris Sparc 8 和 Sparc 9 客户端：

注意：对于 Solaris 8， pfil 驱动程序需要 SUN patch 113685。如果未安装 SUN patch 113685，可以通过联系趋势科技获取替换版本的 pfil 软件包。

注意：对于 Solaris 8，趋势科技服务器深度安全防护系统客户端需要 SUN patch 112438 (/dev/random)。

- 步骤 1. 获取所需的所有软件包（请参阅前述内容）

- 步骤 2. 安装 libiconv-1.8-solx-sparc.gz：

```
gunzip libiconv-1.8-solx-sparc.gz
pkgadd -d libiconv-1.8-solx-sparc all
```

- 步骤 3. 安装 libgcc-3.4.6-solx-sparc.gz：

```
gunzip libgcc-3.4.6-solx-sparc.gz
pkgadd -d libgcc-3.4.6-solx-sparc all
```

- 步骤 4. 安装 pfil：

```
pkgadd -d pfil_Solaris_x.pkg all
```

步骤 5. 将 pfil 流模块推送到网络接口：

```
ifconfig <interface> modinsert pfil@2
```

注意：在网络接口流中，pfil 应紧随 ip 之后。要确定 ip 的位置，请执行以下命令：

```
ifconfig <interface> modlist
```

并确保 modinsert 上使用的数字比 modlist 中 ip 的数字大一。

注意：必须将 pfil 添加到客户端将保护的每个接口的网络堆栈中。

```
touch /etc/ipf.conf
/etc/init.d/pfil start
```

（有关更多信息，请参阅下面的“在 Solaris（8 和 9 Sparc）主机上安装 PFIL 的注意事项”。）

步骤 6. 安装客户端：

```
gunzip Agent-Solaris_5.x_sparc-5.x.x-xxxx.sparc.pkg.gz
pkgadd -d Agent-Solaris_5.x_sparc-5.x.x-xxxx.sparc.pkg all
```

在 Solaris 10 上启动、停止和重置客户端

```
svcadm enable ds_agent - starts the Agent
svcadm disable ds_agent - stops the Agent
/opt/ds_agent/dsa_control -r - resets the Agent
svcadm restart ds_agent - restarts the Agent
svcs -a | grep ds - displays Agent status
```

在 Solaris 8 和 9 上启动、停止和重置客户端：

```
/etc/init.d/ds_agent start - starts the Agent
/etc/init.d/ds_agent stop - stops the Agent
/etc/init.d/ds_agent reset - resets the Agent
/etc/init.d/ds_agent restart - restarts the Agent
```

请注意，过滤活动日志文件位于 /var/log/ds_agent 中

完成安装后，通过遵循[基本趋势科技服务器深度安全防护系统配置](#)中的步骤执行以下操作来使用趋势科技服务器深度安全防护系统管理中心配置计算机上防护：

- 向趋势科技服务器深度安全防护系统管理中心添加计算机
- 在计算机上启用防护

在 Solaris（8 和 9 Sparc）主机上安装 PFIL 的注意事项

Solaris 客户端使用由 Darren Reed 开发的 PFIL IP 过滤器组件。趋势科技服务器深度安全防护系统当前支持 2.1.11 版本。我们已编写了此源代码并在趋势科技下载专区上提供了软件包：<http://www.trendmicro.com/download/zh-cn/>。

可以在以下站点上找到更多信息：<http://coombs.anu.edu.au/~avalon>。（若要获取 PFIL 源代码的副本，请联系您的支持提供商。）

pfil 的注意事项

（以下说明假设您的接口是 hme）

如果执行 "ifconfig modlist"，您将看到如下推送到接口的流模块列表（对于 hme0）：

```
0 arp
1 ip
2 hme
```

需要在 ip 和 hme 之间插入 pfil：

```
ifconfig hme0 modinsert pfil@2
```

检查该列表，您会看到：

```
0 arp
1 ip
2 pfil
3 hme
```

将 pfil 流模块配置为在打开设备时自动推送：

```
autopush -f /etc/opt/pfil/iu.ap
```

此时，

```
strconf < /dev/hme
```

应返回

```
pfil
hme
```

而且，modinfo 应该显示

```
# modinfo | grep pfil
110 102d392c 6383 24 1 pfil (pfil Streams module 2.1.11)
110 102d392c 6383 216 1 pfil (pfil Streams driver 2.1.11)
```

安装适用于 AIX 的趋势科技服务器深度安全防护系统客户端

- 步骤 1. 以 Root 身份登录
- 步骤 2. 将软件包复制到临时文件夹 ("/tmp")
- 步骤 3. 使用 gunzip 解压软件包:

```
/tmp> gunzip Agent-AIX_5.3-7.x.x-x.powerpc.bff.gz
```

- 步骤 4. 安装客户端:

```
/tmp> installp -a -d /tmp ds_agent
```

在 AIX 上启动和停止客户端:

输入以下命令之一:

```
/etc/rc.d/init.d/ds_agent start  
/etc/rc.d/init.d/ds_agent stop
```

安装适用于 HP-UX 的趋势科技服务器深度安全防护系统客户端

- 步骤 1. 以 Root 身份登录
- 步骤 2. 将软件包复制到临时文件夹 ("/tmp")
- 步骤 3. 使用 gunzip 解压软件包:

```
/tmp> gunzip Agent-HPUX_11.23_ia64-7.x.x-x.ia64.depot.gz
```

- 步骤 4. 安装客户端: (请注意, 使用完整路径引用软件包。不能使用相对路径。)

```
/tmp> swinstall -s /tmp/Agent-HPUX_11.23_ia64-7.x.x-x.ia64.depot  
ds_agent
```

在 HP-UX 上启动和停止客户端:

输入以下命令之一:

```
/sbin/init.d/ds_agent start  
/sbin/init.d/ds_agent stop
```

安装趋势科技服务器深度安全防护系统通知程序

趋势科技服务器深度安全防护系统通知程序是仅用于 Windows 上的物理计算机或虚拟机的工具，并提供恶意软件检测的本地通知。

本节介绍的独立型安装用于趋势科技服务器深度安全防护系统虚拟设备保护的无客户端计算机。

趋势科技服务器深度安全防护系统通知程序在 Windows 上作为趋势科技服务器深度安全防护系统中继和趋势科技服务器深度安全防护系统客户端安装的一部分自动安装，所以不需要使用下面的步骤进行安装。

复制安装包

将安装文件复制到目标计算机。

无客户端通知程序的 VMCI 设置

要在无客户端 VM 上使用通知程序，必须启用 VMCI：

- 步骤 1. 停止 VMware 镜像。
- 步骤 2. 在 vCenter 中，选择镜像和**编辑设置**。
- 步骤 3. 在**硬件**选项卡上，选择 **VMCI 设备**。
- 步骤 4. 选择在 **VM 之间启用 VMCI** 选项。
- 步骤 5. 单击**确定**。
- 步骤 6. 重新启动 VMware 镜像并安装趋势科技服务器深度安全防护系统通知程序。

安装适用于 Windows 的趋势科技服务器深度安全防护系统通知程序

注意：请记住，必须在 Windows 计算机上拥有管理员权限才能安装并运行趋势科技服务器深度安全防护系统通知程序。

步骤 1. 双击安装文件来运行安装包。

单击**下一步**开始安装。

步骤 2. 阅读许可协议并单击**下一步**。

步骤 3. 单击**安装**继续安装。

步骤 4. 单击**完成**完成安装。

此时，趋势科技服务器深度安全防护系统通知程序已在此计算机上安装且正在运行，并且会在 Windows 系统托盘中显示通知程序图标。

检测到恶意软件时通知程序将自动提供弹出通知（可以通过双击托盘图标打开通知程序状态和配置窗口来手动禁用通知）。

基本趋势科技服务器深度安全防护系统配置

本节介绍一些建议的趋势科技服务器深度安全防护系统管理中心配置过程。

配置电子邮件通知

在趋势科技服务器深度安全防护系统管理中心中，多种警告和错误情况会引发警报。

您应该使趋势科技服务器深度安全防护系统管理中心可在引发警报时通过现有的 SMTP 服务器发送电子邮件通知。

设置电子邮件通知：

1. 在趋势科技服务器深度安全防护系统管理中心中，转至**系统 > 系统设置 > 系统**。
2. 在 **SMTP** 区域中，输入 SMTP 服务器的地址、凭证和其他详细信息。
3. 单击**测试 SMTP 设置**按钮以测试 SMTP 配置。如果配置成功，则会显示成功通知。如果不成功，则会显示警告通知。（如果收到警告，请确保 SMTP 服务器正在运行且可以访问，并且所需端口处于打开状态，如[准备](#)中所述。）完成之后，单击**保存**。
4. 现在转至**系统 > 系统设置 > 通知**。
5. 在**警报通知 (来自管理中心)** 区域中，输入要向其发送通知的电子邮件地址。单击**保存**。

注意：此电子邮件地址不与任何单个用户的趋势科技服务器深度安全防护系统帐户相关联。可以对各个用户的帐户进行配置，以便按其接收电子邮件通知。要为某个用户启用电子邮件通知，请在**系统 > 用户**窗口上编辑该用户的**属性**。

缺省情况下，管理中心会对每个报警发送通知。

您可以通过转至**系统 > 系统设置 > 系统**，然后单击**警报配置**区域中的**查看警报配置...**来进一步限定发送通知的条件。可在每个警报的**属性**窗口上为其配置通知条件。

有关警报和通知的更多信息，请参阅联机帮助或《管理员指南》中相应的章节。

创建角色和用户帐户

趋势科技服务器深度安全防护系统使用基于角色的访问控制来限制用户对趋势科技服务器深度安全防护系统各个部分的访问。安装趋势科技服务器深度安全防护系统管理中心后，应为每个用户创建单独的帐户并为每个用户分配一个角色，该角色将限制除那些完成其职责所必需的活动外的所有活动。

趋势科技服务器深度安全防护系统随附了两个预先配置的角色：

完全访问权限：“完全访问权限”角色可以授予用户有关管理趋势科技服务器深度安全防护系统的所有可能的权限，包括创建、编辑和删除计算机、计算机组、安全配置文件、规则、防恶意软件配置、组件以及其他项。

审计员：“审计员”角色可以为用户提供在趋势科技服务器深度安全防护系统中查看所有信息的功能，但不能修改除其个人设置（例如密码、联系信息、控制台布局首选项以及其他设置）之外的所有设置。

您可以创建新角色来限制用户编辑甚至查看趋势科技服务器深度安全防护系统的元素（例如，特定计算机、安全规则的属性或系统设置）。

创建用户帐户之前，请确定用户将拥有的角色，并详细列举这些角色需要访问的趋势科技服务器深度安全防护系统元素以及访问权限的性质（查看、编辑、创建等）。创建角色后，则可以开始创建用户帐户并为其分配特定角色。

有关如何创建角色和用户帐户的详细信息，请参阅联机帮助或《管理员指南》的相应章节。

配置趋势科技服务器深度安全防护系统中继

注意：趋势科技服务器深度安全防护系统中继包含趋势科技服务器深度安全防护系统客户端，趋势科技服务器深度安全防护系统管理中心必须先激活该客户端，然后才能对其进行配置。

激活趋势科技服务器深度安全防护系统中继

在趋势科技服务器深度安全防护系统管理中心中：

1. 在**计算机**窗口中，使用**新建**选项添加安装趋势科技服务器深度安全防护系统中继的计算机，然后**激活**该计算机。
2. 检查中继客户端状态是否为**被管理 (联机)**。
3. 在趋势科技服务器深度安全防护系统中继计算机上，打开**趋势科技服务器深度安全防护系统通知程序**并检查状态是否为**正常**。

通过中继配置更新

在趋势科技服务器深度安全防护系统管理中心中：

1. 转至“系统” > “系统设置” > “更新”。
2. 单击**查看中继组**按钮。
3. 在**中继组**窗口中，单击**新建**并创建新中继组，在“成员”部分中检查新添加的中继客户端计算机。单击**确定**。
4. 转至**系统 > 更新**。您应该看到新添加的中继作为“中继”部分中中继组的成员。
5. 在**安全更新**部分中，“组件”列表将全部显示“尚未更新”。单击**立即更新组件**，然后在“组件更新向导”中单击**完成**。
6. 更新趋势科技服务器深度安全防护系统中继上的组件可能要花费几分钟时间。
7. “组件更新向导”显示更新已完成时，单击**完成**。
8. 返回**系统 > 更新**。在“安全更新”部分中，“组件”列表将全部显示“已 100% 更新”。
9. 在趋势科技服务器深度安全防护系统中继计算机上，打开趋势科技服务器深度安全防护系统通知程序，您将看到“组件”列表已经更新。

趋势科技服务器深度安全防护系统客户端和设备可以配置为从趋势科技服务器深度安全防护系统中继提取更新或者直接从趋势科技更新服务器提取更新。

中继可以组织到层次结构中以优化带宽。

使用“系统” > “系统设置” > “更新”窗口配置趋势科技服务器深度安全防护系统中继。

要为客户端/设备选择中继，请在**计算机**窗口上，右键单击客户端/设备并从**操作菜单**中选择**分配中继组**。

向趋势科技服务器深度安全防护系统管理中心添加计算机

将安装有趋势科技服务器深度安全防护系统客户端的计算机添加到趋势科技服务器深度安全防护系统管理中心的“计算机”列表中。

有四种方式可将计算机添加到趋势科技服务器深度安全防护系统管理中心**计算机**窗口：

- 通过指定计算机的 IP 地址或主机名来逐个添加计算机
- 通过扫描网络来发现计算机
- 连接到 Microsoft Active Directory 并导入计算机列表
- 连接到 VMware vCenter 并导入计算机列表

本快速入门指南介绍如何通过指定计算机 IP 地址或主机名来添加单个计算机。要使用其他方法之一，请查阅联机帮助或《管理员指南》。

单击导航窗格中的**计算机**，转至**计算机**窗口，然后单击工具栏中的**新建**。

在**主机名**文本框中键入新计算机的主机名或 IP 地址。**新建计算机**向导找到新计算机并确定存在未激活的客户端后，它还允许您指定要应用于该计算机的安全配置文件。选择与计算机的类型和功能相匹配的缺省安全配置文件。单击**下一步**时，向导将找到计算机并激活客户端。完成客户端激活后，此向导会提供是否打开计算机的**详细信息**窗口的选项，通过此窗口可以配置很多客户端的设置。目前请跳过**详细信息**窗口。

在计算机上启用防护

激活趋势科技服务器深度安全防护系统客户端

必须通过管理中心激活客户端，才能将规则分配给这些客户端。激活过程包括在客户端和管理中心之间交换唯一的指纹。这确保了仅有该趋势科技服务器深度安全防护系统管理中心（或其中一个节点）能够向客户端发送指令。

注意： 分别添加到**计算机**列表中的计算机会自动激活其客户端。激活客户端后，客户端状态将显示为“被管理(联机)”。

手动激活计算机上的客户端：

- 右键单击**计算机**列表中的计算机，然后选择**操作 > 激活**。计算机的状态列将更改为“被管理 (联机)”。

注意：如果将客户端安装在之前仅受趋势科技服务器深度安全防护系统虚拟设备保护的虚拟机上，必须从管理中心重新激活该虚拟机以注册计算机上存在的客户端。

通过将安全配置文件分配给计算机来应用防护

安全配置文件包含所有趋势科技服务器深度安全防护系统防护模块的规则。

将安全配置文件分配给计算机：

1. 右键单击**计算机**列表中要保护的计算机，然后选择**操作 > 分配安全配置文件...**。分配与计算机的类型和功能相匹配的缺省安全配置文件。缺省的安全配置文件配置有防恶意软件规则、防火墙规则、DPI 规则、完整性监控规则和日志审查防护规则。
2. 单击**确定**后，管理中心将向客户端发送安全配置文件。**计算机状态**列和管理中心的状态栏将显示客户端正在进行更新的消息。计算机上的客户端完成更新后，状态列将显示“被管理 (联机)”。

注意：当您使用趋势科技服务器深度安全防护系统管理中心更改计算机上客户端/设备的配置时（例如分配新的安全配置文件），趋势科技服务器深度安全防护系统管理中心必须将新的信息发送给该客户端/设备。这就是配置更新。配置更新通常会立刻执行，但也可以通过单击“更新配置”按钮来强制执行更新。

基本防火墙配置

趋势科技服务器深度安全防护系统的许多防火墙规则和其他元素均使用诸如 IP 列表、Mac 列表和时间表等可重用组件。如果您启用了防火墙防护并且受保护的计算机处于 Windows 域环境中，请修改名为“域控制器”的 IP 列表以启用从域控制器到域客户端的通信：

1. 在趋势科技服务器深度安全防护系统管理中心中，转至**组件 > IP 列表**，然后双击**域控制器** IP 列表以显示其**属性**窗口。
2. 编辑 **IP** 文本区域，使用代表受保护计算机可与之通信的域控制器的 IP 列表替换 IP 127.0.0.1。

3. 单击**确定**保存您所做的更改。

然后，确保以下两个防火墙规则有效：

- 域控制器的 TCP
- 域控制器的 UDP

使用以太网时，ARP 是 TCP/IP 堆栈的基础。ARP 设备提供从 IP 地址到以太网地址的转换，这对于向本地 LAN 网段中的其他系统发送数据包来说是至关重要的。如果没有此转换，则无法进行其他形式的点对点 IP 通信。

因此，趋势科技服务器深度安全防护系统管理中心不将趋势科技服务器深度安全防护系统客户端配置为丢弃 ARP 数据包是非常重要的，除非实际情况需要（配置使用静态 ARP 表）。如果网络依赖于动态 ARP，请确保以下防火墙规则有效：

- ARP

Java 安全性

趋势科技服务器深度安全防护系统管理中心在 Java 虚拟机 (JVM) 中运行，JVM 在一定程度上控制网络行为。Java 使用缓存来存储成功和失败的 DNS 查找。默认情况下将永久缓存成功查找，以防御 DNS 欺骗攻击。但是，这种缓存可能会阻止趋势科技服务器深度安全防护系统管理中心与使用 DHCP 的计算机或 IP 地址已更改的计算机进行通信。趋势科技服务器深度安全防护系统管理中心对此设置使用的值为 60 秒。

或者，当存在 DNS 欺骗风险时，可以将 DNS 缓存配置为无限期。要配置趋势科技服务器深度安全防护系统管理中心的 DNS 缓存期限，您需要执行下列操作：

1. 打开 [Manager install directory]\jre\lib\security 中的 java.security 文件
2. 找到 networkaddress.cache.ttl 所在行，并将值设置为 -1：

```
networkaddress.cache.ttl=-1
```

3. 保存文件并重新启动 Deep Security Manager 服务

有关 Java 网络缓存设置的更多信息，请参阅：

<http://java.sun.com/javase/6/docs/technotes/guides/net/properties.html>

升级

升级方案

本章介绍可能会运行趋势科技服务器深度安全防护系统的不同环境的升级过程。

升级趋势科技服务器深度安全防护系统 8.0 组件。

介绍从趋势科技服务器深度安全防护系统 8.0 初始版本升级到趋势科技服务器深度安全防护系统 8.0 SP1 的过程。

从具有无客户端防恶意软件的 DS 7.5 升级（维持 ESX/ESXi 4.1）。

介绍在实施无客户端防恶意软件防护的 VMware 4.1 环境中，从趋势科技服务器深度安全防护系统 7.5 升级到趋势科技服务器深度安全防护系统 8.0 SP1 的过程。

从具有无客户端防恶意软件的 DS 7.5 升级（将 ESX/ESXi 4.1 升级到 5.0）。

介绍在实施无客户端防恶意软件防护的 VMware 4.1 环境中，从趋势科技服务器深度安全防护系统 7.5 升级到趋势科技服务器深度安全防护系统 8.0 SP1 的过程。

从仅具有无客户端防火墙和 DPI 的 DS 7.5 升级（维持 ESX/ESXi 4.1）。

介绍在仅实施无客户端防火墙和 DPI 防护的 VMware 4.1 环境中，从趋势科技服务器深度安全防护系统 7.5 升级到趋势科技服务器深度安全防护系统 8.0 SP1 的过程。

从仅具有无客户端防火墙和 DPI 的 DS 7.5 升级（将 ESX/ESXi 4.1 升级到 5.0）。

介绍在仅实施无客户端防火墙和 DPI 防护的 VMware 4.1 环境中，从趋势科技服务器深度安全防护系统 7.5 升级到趋势科技服务器深度安全防护系统 8.0 SP1 的过程。

从仅具有基于客户虚拟机客户端的防护的趋势科技服务器深度安全防护系统 7.5 升级。

介绍在仅实施基于客户端的防护的任意环境中，从趋势科技服务器深度安全防护系统 7.5 升级到趋势科技服务器深度安全防护系统 8.0 SP1 的过程。

升级趋势科技服务器深度安全防护系统 8.0 软件组件

升级趋势科技服务器深度安全防护系统管理中心

从趋势科技下载专区下载新版本的趋势科技服务器深度安全防护系统管理中心安装包并将其复制到目标计算机。

按照新安装操作的步骤运行安装包，如[安装趋势科技服务器深度安全防护系统管理中心](#)中所述。

升级与覆盖现有的安装

如果系统上安装了先前版本的趋势科技服务器深度安全防护系统管理中心，您可以选择“**升级现有的安装版本**”或“**覆盖现有的安装版本**”。升级安装版本会将趋势科技服务器深度安全防护系统管理中心升级到最新版本，但不会覆盖您的安全配置文件、DPI 规则、防火墙规则、应用程序类型等，也不会更改应用于网络中计算机的任何安全设置。覆盖现有的安装版本会清除与先前安装版本相关的所有数据，然后安装最新的过滤器、规则、配置文件等。

注意：即使创建新的安装版本，当前由趋势科技服务器深度安全防护系统客户端应用于计算机上的现有安全元素也不会受影响，直至使用趋势科技服务器深度安全防护系统管理中心更新它们。从新的管理中心安装版本更新客户端将需要停用并重新激活这些客户端。

远程升级趋势科技服务器深度安全防护系统组件

使用趋势科技服务器深度安全防护系统管理中心，可以对趋势科技服务器深度安全防护系统中继、趋势科技服务器深度安全防护系统客户端、趋势科技服务器深度安全防护系统虚拟设备以及趋势科技服务器深度安全防护系统过滤器驱动程序进行远程升级。必须首先下载软件并将其导入到趋势科技服务器深度安全防护系统管理中心。

下载趋势科技服务器深度安全防护系统软件包：

1. 在趋势科技服务器深度安全防护系统管理中心，转至**系统 > 更新**窗口上的**软件更新**区域。
2. 按**打开下载专区...**，您将进入趋势科技下载专区 Web 站点。
3. 将中继、客户端、过滤器驱动程序和虚拟设备的最新软件包下载到本地计算机。

导入趋势科技服务器深度安全防护系统软件包：

1. 在趋势科技服务器深度安全防护系统管理中心，转至**系统 > 更新**窗口上的**软件更新**区域。
2. 按**导入软件...**，将显示**导入软件 (从文件)**向导。
3. 使用该向导将下载到的每个软件包导入到趋势科技服务器深度安全防护系统。

将软件包导入到趋势科技服务器深度安全防护系统后，您便可以从趋势科技服务器深度安全防护系统管理中心远程升级软件组件。

远程升级软件组件：

1. 在趋势科技服务器深度安全防护系统管理中心的**计算机**窗口上，右键单击您要升级的计算机（ESX、趋势科技服务器深度安全防护系统虚拟设备、趋势科技服务器深度安全防护系统客户端或趋势科技服务器深度安全防护系统中继），然后从**操作**菜单中选择适当的**升级**选项。

手动升级趋势科技服务器深度安全防护系统中继

手动升级适用于 Windows 的趋势科技服务器深度安全防护系统中继

将安装文件复制到目标计算机并按照新安装操作的步骤运行安装包。

如果进行升级，则将无法更改安装目录。要安装到其他目录，必须首先卸载先前版本。

手动升级适用于 Linux 的趋势科技服务器深度安全防护系统中继：

使用 "rpm -U" 从先前安装版本升级。此方法将保留您的配置文件设置：

```
# rpm -U Relay-RedHat_2.6.18_8.EL5_i686-8.0.0-xxxx.i386.rpm
```

手动升级趋势科技服务器深度安全防护系统客户端

注意：请记住，在升级趋势科技服务器深度安全防护系统客户端之前，需要确保未对要升级的趋势科技服务器深度安全防护系统客户端启用客户端自我防护。可以从趋势科技服务器深度安全防护系统管理中心**系统 > 系统设置 > 计算机**执行此操作。在**客户端自我防护**中，取消选中**防止本地最终用户卸载、停止或以其他方式修改客户端**设置或为本地覆盖选择密码。

手动升级适用于 Windows 的 Trend Micro 服务器深度安全防护系统客户端

将安装文件复制到目标计算机并按照新安装操作的步骤运行安装包。

如果进行升级，则将无法更改安装目录。要安装到其他目录，必须首先卸载先前版本。

手动升级适用于 Linux 的 Trend Micro 服务器深度安全防护系统客户端：

使用 "rpm -U" 从先前安装版本升级。此方法将保留您的配置文件设置：

```
# rpm -U Agent-RedHat_2.6.18_8.EL5_i686-8.0.0-xxxx.i386.rpm
```

手动升级适用于 Solaris（所有版本）的 Trend Micro 服务器深度安全防护系统客户端

```
pkgadd -v -a /opt/ds_agent/ds_agent.admin -d Agent-Solaris_5.9_sparc-5.x.x-xxxx.sparc.pkg
```

手动升级适用于 AIX/HPUX 的 Trend Micro 服务器深度安全防护系统客户端

```
/opt/ds_agent/ds_upgrade.sh <软件包的完整路径>
```

从具有无客户端防恶意软件的 DS 7.5 升级（维持 ESX/ESXi 4.1）

以下升级过程适用于由趋势科技服务器深度安全防护系统提供无客户端防恶意软件防护的 VMware 环境。

阶段一：升级 VMware 组件

注意：下面的说明介绍了执行 VMware 和趋势科技服务器深度安全防护系统升级应该遵循的顺序。有关升级 VMware 环境组件的详细说明，请查看您的 VMware 文档。趋势科技服务器深度安全防护系统管理中心 8 发行说明中引用了 VMware Web 站点上的一些位置链接，可以从中找到最新信息和知识库文章。

下表列出了此阶段将要升级的组件：

组件	升级前版本	升级后版本
vCenter Server	4.1 U1+	5.0+
vShield Manager	4.1	5.0+
Endpoint（适用于 ESX）	3.0.8	5.0+
Endpoint 客户虚拟机驱动程序	1.0.0.2	5.0+

步骤 1. 使用 vShield Manager 4.1，从 ESX/ESXi 卸载 vShield Endpoint。

警告：卸载 vShield Endpoint 模块会将 ESX/ESXi 主机置于维护模式并重新启动该主机。将 vShield Manager 和任何其他虚拟机迁移到其他 ESX/ESXi 主机，以避免在重新启动期间关闭这些虚拟机。

步骤 2. 使用每个 VM 上的**添加/删除程序**，从 ESX/ESXi 上的 VM 卸载 vShield Endpoint 客户虚拟机驱动程序。

步骤 3. 通过运行 VMware VIM 安装程序升级 vCenter Server。（按照 VMware 提供的说明进行操作。）

- 步骤 4. 按照 VMware 的 *vShield_Quick_Start_Guide.pdf* 中的说明升级 vShield Manager。
- 步骤 5. vShield Manager 的升级完成并且 vShield Manager 已重新启动后，登录到 vShield Manager 控制台并添加将其与 vCenter 重新集成所需的配置信息。
- 步骤 6. 使用 vShield Manager 在 ESX/ESXi 上安装 vShield Endpoint。
- 步骤 7. 使用 VMware Tools 在 VM 上安装 vShield Endpoint 客户虚拟机驱动程序（“vShield 驱动程序”）。

重新启动 ESX/ESXi 后，确认 vCenter 的所有组件都工作正常，然后继续升级过程的阶段二，升级趋势科技服务器深度安全防护系统组件。确保已升级组件的版本号与步骤开头表格中**升级后版本**一列的版本号相匹配。

阶段二：升级趋势科技服务器深度安全防护系统组件

下表列出了此阶段将要升级的组件。必须将软件从趋势科技下载专区下载到某个位置，从该位置可以将该软件导入到趋势科技服务器深度安全防护系统管理中心。

组件	升级前版本	升级后版本
趋势科技服务器深度安全防护系统管理中心	7.5	8.0 (1448+)
趋势科技服务器深度安全防护系统过滤器驱动程序	7.5	8.0 (1680+)
趋势科技服务器深度安全防护系统虚拟设备	7.5	8.0 (1199+)
趋势科技服务器深度安全防护系统客户端	7.5	8.0 (1201+)
趋势科技服务器深度安全防护系统中继	n/a	8.0 (1201+)

注意：必须已经成功完成了此升级过程的阶段一“升级 VMware 组件”，然后才能升级趋势科技服务器深度安全防护系统组件。

注意：趋势科技服务器深度安全防护系统过滤器驱动程序和趋势科技服务器深度安全防护系统虚拟设备必须始终升级到相同版本。升级其中一个而不升级另一个会使得两者均无法工作。

- 步骤 1. 将趋势科技服务器深度安全防护系统管理中心升级到版本 8.0。按照[安装趋势科技服务器深度安全防护系统管理中心](#)中所述的过程执行操作
- 步骤 2. 遵循[部署趋势科技服务器深度安全防护系统中继](#)中所述的说明执行操作
- 步骤 3. 在趋势科技服务器深度安全防护系统管理中心中的**计算机**窗口中，右键单击 vCenter 并选择**属性**。在 vCenter **属性**窗口上，单击**常规**选项卡上的**添加/更新证书...** 为 vCenter 添加证书，然后单击 **vShield Manager** 选项卡上的**添加/更新证书...** 为 vShield Manager 添加证书
- 步骤 4. 在趋势科技服务器深度安全防护系统管理中心中，转至**系统 > 更新 > 软件包**，然后导入趋势科技服务器深度安全防护系统过滤器驱动程序 8 以及趋势科技服务器深度安全防护系统虚拟设备 8 安装包
- 步骤 5. 在趋势科技服务器深度安全防护系统管理中心的**计算机**窗口上，右键单击 ESX，然后选择**操作 > 升级过滤器驱动程序...**
- 步骤 6. 在趋势科技服务器深度安全防护系统管理中心的**计算机**窗口中，右键单击趋势科技服务器深度安全防护系统虚拟设备，然后选择**操作 > 升级设备...**（此时不激活 VM。）
- 步骤 7. 在趋势科技服务器深度安全防护系统管理中心的**计算机**窗口中，右键单击趋势科技服务器深度安全防护系统虚拟设备，然后选择**操作 > 停用设备**
- 步骤 8. 在趋势科技服务器深度安全防护系统管理中心的**计算机**窗口中，右键单击趋势科技服务器深度安全防护系统虚拟设备，然后选择**操作 > 激活设备**

升级 VMware 和具有无客户端防护的趋势科技服务器深度安全防护系统现已完成。

从具有无客户端防恶意软件的 DS 7.5 升级 (将 ESX/ESXi 4.1 升级到 5.0)

以下升级过程适用于由趋势科技服务器深度安全防护系统提供无客户端防恶意软件防护的 VMware 环境。

趋势科技服务器深度安全防护系统 8.0 支持 ESX/ESXi 版本 4.1 和 5.0。但是，要使用趋势科技服务器深度安全防护系统 8.0 在这两个版本的 ESX/ESXi 上实现无客户端防恶意软件或无客户端完整性监控，必须将您的 VMware 基础架构的剩余部分（vCenter、vShield Manager、vShield Endpoint 和 vShield Endpoint 驱动程序）升级到版本 5.0。

升级过程摘要

注意：此过程中的步骤顺序非常重要。请确保至少通读一遍全文并按照编写顺序执行这些步骤。

此过程包括两个阶段：首先，升级 VMware 组件，然后，升级趋势科技服务器深度安全防护系统组件。

在第一个阶段，升级 VMware 组件将包括以下步骤：

1. 停用 ESX/ESXi 上的趋势科技服务器深度安全防护系统虚拟设备
2. 恢复 ESX（以卸载趋势科技服务器深度安全防护系统过滤器驱动程序）
3. 从 ESX/ESXi 卸载 vShield Endpoint
4. 从 ESX 上的 VM 卸载 vShield Endpoint 客户虚拟机驱动程序
5. 升级 vCenter
6. 如果您要使用 ESXi 5.0，请升级 ESX/ESXi 并应用 patch “ESXi 5.0 (build 474610 或更高版本)”
7. 升级 vShield Manager
8. 配置 vShield Manager 来与 vCenter 集成
9. 在 ESX/ESXi 上安装 vShield Endpoint

10. 在 VM 上安装 vShield Endpoint 驱动程序（位于随 ESXi 5.0 提供的 VMware Tools 中）
11. 重新启动 ESX/ESXi

注意：卸载 vShield Endpoint 模块（步骤 3）会将 ESX/ESXi 主机置于维护模式并重新启动该主机。将 vShield Manager 和任何其他虚拟机迁移到其他 ESX/ESXi 主机，以避免在重新启动期间关闭这些虚拟机。

注意：升级 vCenter 上的 vShield Manager 时，将需要停用该 vCenter 上运行的所有虚拟设备。这是因为每个 vCenter 上仅有一个 vShield Manager，该 vCenter 上的所有虚拟设备需要活动的 vShield Manager。停用为 VM 提供无客户端防护的虚拟设备所需的时间取决于正在保护的 VM 数目。估计升级过程将要花费的时间量时需考虑此项。

注意：停用趋势科技服务器深度安全防护系统虚拟设备时，ESX/ESXi 上的 VM 将没有无客户端防护。

第二阶段升级趋势科技服务器深度安全防护系统组件将包括以下步骤：

1. 升级趋势科技服务器深度安全防护系统管理中心
2. 部署和配置趋势科技服务器深度安全防护系统中继
3. 为 vCenter 和 vShield Manager 向趋势科技服务器深度安全防护系统管理中心添加安全证书
4. 将趋势科技服务器深度安全防护系统 8 安装包导入趋势科技服务器深度安全防护系统管理中心
5. 准备 ESX/ESXi（此操作将在 ESX/ESXi 上安装趋势科技服务器深度安全防护系统过滤器驱动程序）
6. 在为升级做准备时重新激活趋势科技服务器深度安全防护系统虚拟设备
7. 升级 ESX/ESXi 上的趋势科技服务器深度安全防护系统虚拟设备
8. 激活 ESX/ESXi 上的客户 VM
9. 部署趋势科技服务器深度安全防护系统客户端（如果需要）

阶段一：升级 VMware 组件

注意：下面的说明提供了执行 VMware 和趋势科技服务器深度安全防护系统升级应该遵循的顺序。有关升级 VMware 环境组件的详细说明，请查看您的 VMware 文档。趋势科技服务器深度安全防护系统管理中心 8 发行说明中引用了 VMware Web 站点上的一些位置链接，可以从中找到最新信息和知识库文章。

下表列出了此阶段将要升级的组件：

组件	升级前版本	升级后版本
vCenter Server	4.1 U1+	5.0+
ESX（升级可选）	4.1 U1+	5.0+
vShield Manager	4.1	5.0+
Endpoint（适用于 ESX）	3.0.8	5.0+
Endpoint 客户虚拟机驱动程序	1.0.0.2	5.0+

- 步骤 1. 在趋势科技服务器深度安全防护系统管理中心中，转至**计算机**窗口，右键单击虚拟设备并选择**操作 > 停用设备**。
- 步骤 2. 在趋势科技服务器深度安全防护系统管理中心的**计算机**窗口上，右键单击 ESX/ESXi 并选择**操作 > 恢复 ESX...**，然后按照向导中的步骤操作。（此过程将从 ESX/ESXi 卸载 7.5 趋势科技服务器深度安全防护系统过滤器驱动程序。）
- 步骤 3. 卸载 vShield Endpoint 模块会将 ESX/ESXi 主机置于维护模式并重新启动该主机。

注意：将 vShield Manager 和任何其他虚拟机迁移到其他 ESX/ESXi 主机，以避免在重新启动期间关闭这些虚拟机。

使用 vShield Manager 4.1，从 ESX/ESXi 卸载 vShield Endpoint。

- 步骤 4. 使用每个 VM 上的**添加/删除程序**，从 ESX/ESXi 上的 VM 卸载 vShield Endpoint 客户虚拟机驱动程序。
- 步骤 5. 按照 VMware 提供的说明运行 VIM 安装程序。
- 步骤 6. (可选) 将 ESX/ESXi 升级到 ESXi 5.0 并应用 patch “ESXi 5.0 (build 474610 或更高版本)”。
- 步骤 7. 按照 VMware 的 *vShield_Quick_Start_Guide.pdf* 中的说明升级 vShield Manager。
- 步骤 8. vShield Manager 的升级完成并且 vShield Manager 已重新启动后，登录到 vShield Manager 控制台并添加将其与 vCenter 重新集成所需的配置信息。
- 步骤 9. 使用 vShield Manager 在 ESX/ESXi 上安装 vShield Endpoint。
- 步骤 10. 使用 VMware Tools 在 VM 上安装 vShield Endpoint 客户虚拟机驱动程序 (“vShield 驱动程序”)。
- 步骤 11. 重新启动 ESX/ESXi 来完成升级过程的 VMware 阶段。

重新启动 ESX/ESXi 后，确认 vCenter 的所有组件都工作正常，然后继续升级过程的阶段二，升级趋势科技服务器深度安全防护系统组件。确保已升级组件的版本号与步骤开头表格中**升级后版本**一列的版本号相匹配。

阶段二：升级趋势科技服务器深度安全防护系统组件

下表列出了此阶段将要升级的组件。必须将软件从趋势科技下载专区下载到某个位置，从该位置可以将该软件导入到趋势科技服务器深度安全防护系统管理中心。

组件	升级前版本	升级后版本
趋势科技服务器深度安全防护系统管理中心	7.5	8.0 (1448+)
趋势科技服务器深度安全防护系统过滤器驱动程序	7.5	8.0 (1189+)
趋势科技服务器深度安全防护系统虚拟设备	7.5	8.0 (1199+)

组件	升级前版本	升级后版本
趋势科技服务器深度安全防护系统客户端	7.5	8.0 (1201+)
趋势科技服务器深度安全防护系统中继	n/a	8.0 (1201+)

注意：必须已经成功完成了此升级过程的阶段一“升级 VMware 组件”，然后才能升级趋势科技服务器深度安全防护系统组件。

注意：趋势科技服务器深度安全防护系统过滤器驱动程序和趋势科技服务器深度安全防护系统虚拟设备必须始终升级到相同版本。升级其中一个而不升级另一个会使得两者均无法工作。

- 步骤 1. 将趋势科技服务器深度安全防护系统管理中心升级到版本 8.0。按照[安装趋势科技服务器深度安全防护系统管理中心](#)中所述的过程执行操作。
- 步骤 2. 遵循[部署趋势科技服务器深度安全防护系统中继](#)中所述的说明执行操作。
- 步骤 3. 在趋势科技服务器深度安全防护系统管理中心中的**计算机**窗口中，右键单击 vCenter 并选择**属性**。在 vCenter **属性**窗口上，单击**常规**选项卡上的**添加/更新证书...**为 vCenter 添加证书，然后单击 **vShield Manager** 选项卡上的**添加/更新证书...**为 vShield Manager 添加证书。
- 步骤 4. 在趋势科技服务器深度安全防护系统管理中心中，转至**系统 > 更新 > 软件包**并导入趋势科技服务器深度安全防护系统客户端 8、趋势科技服务器深度安全防护系统中继 8、趋势科技服务器深度安全防护系统过滤器驱动程序 8 和趋势科技服务器深度安全防护系统虚拟设备 8 安装包。
- 步骤 5. ESX 将处于“未准备”状态。遵循[为趋势科技服务器深度安全防护系统虚拟设备部署准备 ESX/ESXi](#)中的说明准备 ESX/ESXi。
- 步骤 6. 在趋势科技服务器深度安全防护系统管理中心中的**计算机**窗口中，右键单击趋势科技服务器深度安全防护系统虚拟设备并选择**操作 > 激活设备**。此时不激活 VM。

- 步骤 7. 在趋势科技服务器深度安全防护系统管理中心中的**计算机**窗口中，右键单击趋势科技服务器深度安全防护系统虚拟设备并选择**操作 > 升级设备...**
- 步骤 8. 激活 ESX 上的客户 VM。遵循[激活客户虚拟机](#)中所述的说明执行操作。
- 步骤 9. 部署趋势科技服务器深度安全防护系统客户端（如果需要）。遵循[部署趋势科技服务器深度安全防护系统客户端](#)中所述的说明执行操作。
- 升级 VMware 和具有无客户端防护的趋势科技服务器深度安全防护系统现已完成。

从仅具有无客户端防火墙和 DPI 的 DS 7.5 升级 (维持 ESX/ESXi 4.1)

以下升级过程适用于由趋势科技服务器深度安全防护系统仅提供 *无客户端防火墙和 DPI 防护* 的 VMware 环境。

如果要在 VMware vSphere 4 环境中升级到趋势科技服务器深度安全防护系统 8 并且仅实施无客户端防火墙和 DPI 防护，则只需升级趋势科技服务器深度安全防护系统软件。但是，如果您决定升级到 ESXi 5.0，则您的所有 VMware 组件都需要升级到版本 5.0，以与趋势科技服务器深度安全防护系统 8 兼容。

阶段一：升级 VMware 组件

下表列出了此阶段将要升级的组件（如果要升级到 VMware 5.0）：

组件	升级前版本	升级后版本
vCenter Server	4.1 U1+	5.0+

步骤 1. 通过按照 VMware 提供的说明运行 VIM 安装程序来升级 vCenter Server。

确认 vCenter 的所有组件都工作正常，然后继续升级过程的阶段二，升级趋势科技服务器深度安全防护系统组件。确保已升级组件的版本号与步骤开头表格中 **升级后版本** 一列的版本号相匹配。

阶段二：升级趋势科技服务器深度安全防护系统组件

下表列出了此阶段将要升级的组件。必须将软件从趋势科技下载专区下载到某个位置，从该位置可以将该软件导入到趋势科技服务器深度安全防护系统管理中心。

组件	升级前版本	升级后版本
趋势科技服务器深度安全防护系统管理中心	7.5	8.0 (1448+)
趋势科技服务器深度安全防护系统过滤器驱动程序	7.5	8.0 (1680+)
趋势科技服务器深度安全防护系统虚拟设备	7.5	8.0 (1199+)
趋势科技服务器深度安全防护系统客户端	7.5	8.0 (1201+)
趋势科技服务器深度安全防护系统中继	n/a	8.0 (1201+)

注意：必须已经成功完成了此升级过程的阶段一“升级 VMware 组件”，然后才能升级趋势科技服务器深度安全防护系统组件。

注意：趋势科技服务器深度安全防护系统过滤器驱动程序和趋势科技服务器深度安全防护系统虚拟设备必须始终升级到相同版本。升级其中一个而不升级另一个会使得两者均无法工作。

- 步骤 1. 将趋势科技服务器深度安全防护系统管理中心升级到版本 8.0。按照[安装趋势科技服务器深度安全防护系统管理中心](#)中所述的过程执行操作。
 - 步骤 2. 在趋势科技服务器深度安全防护系统管理中心中的**计算机**窗口中，右键单击 vCenter 并选择**属性**。在 vCenter **属性**窗口上，单击**常规**选项卡上的**添加/更新证书...**为 vCenter 添加证书，然后单击 **vShield Manager** 选项卡上的**添加/更新证书...**为 vShield Manager 添加证书。
 - 步骤 3. 在趋势科技服务器深度安全防护系统管理中心中，转至**系统 > 更新 > 软件包**，然后导入趋势科技服务器深度安全防护系统过滤器驱动程序 8 以及趋势科技服务器深度安全防护系统虚拟设备 8 安装包。
 - 步骤 4. 在趋势科技服务器深度安全防护系统管理中心的**计算机**窗口上，右键单击 ESX，然后选择**操作 > 升级过滤器驱动程序...**
 - 步骤 5. 在趋势科技服务器深度安全防护系统管理中心中的**计算机**窗口中，右键单击趋势科技服务器深度安全防护系统虚拟设备并选择**操作 > 升级设备...**
 - 步骤 6. 遵循[部署趋势科技服务器深度安全防护系统中继](#)中所述的说明执行操作。
 - 步骤 7. 遵循[激活客户虚拟机](#)中所述的说明执行操作。
- 升级仅具有无客户端防火墙和 DPI 防护的趋势科技服务器深度安全防护系统 8 现已完成。

从仅具有无客户端防火墙和 DPI 的 DS 7.5 升级 (将 ESX/ESXi 4.1 升级到 5.0)

以下升级过程适用于由趋势科技服务器深度安全防护系统仅提供无客户端防火墙和 DPI 防护的 VMware 环境。

如果要在 VMware vSphere 4 环境中升级到趋势科技服务器深度安全防护系统 8 并且仅实施无客户端防火墙和 DPI 防护，则只需升级趋势科技服务器深度安全防护系统软件。但是，如果您决定升级到 ESXi 5.0，则您的所有 VMware 组件都需要升级到版本 5.0，以与趋势科技服务器深度安全防护系统 8 兼容。

升级过程摘要

注意：此过程中的步骤顺序非常重要。请确保至少通读一遍全文并按照编写顺序执行这些步骤。

如果您要升级到 ESXi 5.0，那么此过程包括两个阶段：首先，升级 VMware 组件，然后，升级趋势科技服务器深度安全防护系统组件。

在第一个阶段，升级 VMware 组件将包括以下步骤：

1. 停用 ESX/ESXi 上的趋势科技服务器深度安全防护系统虚拟设备
2. 恢复 ESX/ESXi（以卸载趋势科技服务器深度安全防护系统过滤器驱动程序）
3. 升级 vCenter
4. 升级 ESX/ESXi 并应用 patch "ESXi 5.0 (build 474610)"

第二阶段升级趋势科技服务器深度安全防护系统组件将包括以下步骤：

1. 升级趋势科技服务器深度安全防护系统管理中心
2. 为 vCenter 和 vShield Manager 向趋势科技服务器深度安全防护系统管理中心添加安全证书
3. 将趋势科技服务器深度安全防护系统 8 安装包导入趋势科技服务器深度安全防护系统管理中心
4. 准备 ESX/ESXi（此操作将在 ESX/ESXi 上安装趋势科技服务器深度安全防护系统过滤器驱动程序）

5. 在为升级做准备时重新激活趋势科技服务器深度安全防护系统虚拟设备
6. 升级 ESX/ESXi 上的趋势科技服务器深度安全防护系统虚拟设备
7. 部署和配置趋势科技服务器深度安全防护系统中继
8. 激活 ESX/ESXi 上的客户 VM
9. 部署趋势科技服务器深度安全防护系统客户端（如果需要）

阶段一：升级 VMware 组件

下表列出了此阶段将要升级的组件（如果要升级到 VMware 5.0）：

组件	升级前版本	升级后版本
vCenter Server	4.1 U1+	5.0+
ESX/ESXi	4.1 U1+	5.0+

- 步骤 1. 在趋势科技服务器深度安全防护系统管理中心中，转至**计算机**窗口，右键单击虚拟设备并选择**操作 > 停用设备**。
- 步骤 2. 在趋势科技服务器深度安全防护系统管理中心的**计算机**窗口上，右键单击 ESX 并选择**操作 > 恢复 ESX...**，然后按照向导中的步骤操作。
- 步骤 3. 按照 VMware 提供的说明运行 VIM 安装程序。
- 步骤 4. 将 ESX/ESXi 升级到 ESXi 5.0 并应用 patch “ESXi 5.0 Patch (build 474610 或更高版本)”。

确认 vCenter 的所有组件都工作正常，然后继续升级过程的阶段二，升级趋势科技服务器深度安全防护系统组件。确保已升级组件的版本号与步骤开头表格中**升级后版本**一列的版本号相匹配。

阶段二：升级趋势科技服务器深度安全防护系统组件

下表列出了此阶段将要升级的组件。必须将软件从趋势科技下载专区下载到某个位置，从该位置可以将该软件导入到趋势科技服务器深度安全防护系统管理中心。

组件	升级前版本	升级后版本
趋势科技服务器深度安全防护系统管理中心	7.5	8.0 (1448+)
趋势科技服务器深度安全防护系统过滤器驱动程序	7.5	8.0 (1189+)
趋势科技服务器深度安全防护系统虚拟设备	7.5	8.0 (1199+)
趋势科技服务器深度安全防护系统客户端	7.5	8.0 (1201+)
趋势科技服务器深度安全防护系统中继	n/a	8.0 (1201+)

注意： 必须已经成功完成了此升级过程的阶段一“升级 VMware 组件”，然后才能升级趋势科技服务器深度安全防护系统组件。

注意： 趋势科技服务器深度安全防护系统过滤器驱动程序和趋势科技服务器深度安全防护系统虚拟设备必须始终升级到相同版本。升级其中一个而不升级另一个会使得两者均无法工作。

- 步骤 1. 将趋势科技服务器深度安全防护系统管理中心升级到版本 8.0。按照[安装趋势科技服务器深度安全防护系统管理中心](#)中所述的过程执行操作。
- 步骤 2. 在趋势科技服务器深度安全防护系统管理中心中的**计算机**窗口中，右键单击 vCenter 并选择**属性**。在 vCenter **属性**窗口上，单击**常规**选项卡上的**添加/更新证书...**为 vCenter 添加证书，然后单击 **vShield Manager** 选项卡上的**添加/更新证书...**为 vShield Manager 添加证书。
- 步骤 3. 在趋势科技服务器深度安全防护系统管理中心中，转至**系统 > 更新 > 软件包**并导入趋势科技服务器深度安全防护系统客户端 8、趋势科技服务器深度安全防护系统中继 8、趋势科技服务器深度安全防护系统过滤器驱动程序 8 和趋势科技服务器深度安全防护系统虚拟设备 8 安装包。
- 步骤 4. 在阶段一升级 ESX/ESXi 后，ESX/ESXi 将处于“未准备”状态。遵循[为趋势科技服务器深度安全防护系统虚拟设备部署准备 ESXi](#)中的说明准备 ESX/ESXi。
- 步骤 5. 在趋势科技服务器深度安全防护系统管理中心中的**计算机**窗口中，右键单击趋势科技服务器深度安全防护系统虚拟设备并选择**操作 > 激活设备**。此时不激活 VM。
- 步骤 6. 在趋势科技服务器深度安全防护系统管理中心中的**计算机**窗口中，右键单击趋势科技服务器深度安全防护系统虚拟设备并选择**操作 > 升级设备...**
- 步骤 7. 遵循[部署趋势科技服务器深度安全防护系统中继](#)中所述的说明执行操作。
- 步骤 8. 遵循[激活客户虚拟机](#)中所述的说明执行操作。
- 步骤 9. 遵循[部署趋势科技服务器深度安全防护系统客户端](#)中所述的说明执行操作。

升级仅具有无客户端防火墙和 DPI 防护的趋势科技服务器深度安全防护系统 8 现已完成。

从仅具有基于客户虚拟机客户端的防护的趋势科技服务器深度安全防护系统 7.5 升级

以下升级过程适用于由趋势科技服务器深度安全防护系统提供 *仅基于客户虚拟机客户端的防护* 的 VMware 环境。

如果在 VMware vSphere 4 环境中运行趋势科技服务器深度安全防护系统 7.5 并且仅实施基于客户虚拟机客户端的防护，则只需将趋势科技服务器深度安全防护系统组件升级到 8.0。

升级过程

下表列出了要升级的组件。必须将这些软件安装包从趋势科技下载专区下载到某个位置，从该位置可以将这些软件包导入到趋势科技服务器深度安全防护系统管理中心。

组件	升级前版本	升级后版本
趋势科技服务器深度安全防护系统管理中心	7.5	8.0 (1448+)
趋势科技服务器深度安全防护系统过滤器驱动程序	7.5	8.0 (1189+)
趋势科技服务器深度安全防护系统客户端	7.5	8.0 (1201+)
趋势科技服务器深度安全防护系统中继	n/a	8.0 (1201+)

仅提供基于客户虚拟机客户端的防护时，用于在 VMware 环境中从趋势科技服务器深度安全防护系统 7.5 升级到趋势科技服务器深度安全防护系统 8.0 的过程如下所示：

- 步骤 1. 将趋势科技服务器深度安全防护系统管理中心从 7.5 升级到 8.0
遵循[安装趋势科技服务器深度安全防护系统管理中心](#)中所述的说明执行操作。
- 步骤 2. 导入趋势科技服务器深度安全防护系统 8 安装包
转至**系统 > 更新 > 软件包**并导入趋势科技服务器深度安全防护系统客户端 8.0、中继 8.0、过滤器驱动程序 8.0 和虚拟设备 8.0 安装包。

- 步骤 3. 部署至少一个趋势科技服务器深度安全防护系统中继
按照[部署趋势科技服务器深度安全防护系统中继](#)中所述的说明执行操作。
- 步骤 4. 升级任何趋势科技服务器深度安全防护系统客户端
遵循[部署趋势科技服务器深度安全防护系统客户端](#)中所述的说明执行操作。

升级仅具有基于客户虚拟机客户端的防护的趋势科技服务器深度安全防护系统 7.5 现已完成。

趋势科技服务器深度安全防护系统管理中心设置属性文件

本节包含有关属性文件内容的信息，可以在趋势科技服务器深度安全防护系统管理中心的命令行安装（如 Windows 静默安装）中使用该文件。

设置属性文件

设置属性文件中每个条目的格式如下：

```
<Screen Name>.<Property Name>=<Property Value>
```

设置属性文件具有一些强制条目和一些可选条目。

注意：对于可选条目，如果输入的属性值不是允许值之一，则 DSM 安装将改用缺省值。

强制设置**LicenseScreen**

输入适用的激活码。

属性	可接受的值	缺省值	注意
LicenseScreen.License.-1=<value>	<用于所有模块的 AC>	空白	空白是不可接受的

或者

属性	可接受的值	缺省值	注意
LicenseScreen.License.0=<value>	<用于防恶意软件的 AC>	空白	空白是不可接受的
LicenseScreen.License.1=<value>	<用于防火墙/DPI 的 AC>	空白	空白是不可接受的
LicenseScreen.License.2=<value>	<用于完整性监控的 AC>	空白	空白是不可接受的
LicenseScreen.License.3=<value>	<用于日志审查的 AC>	空白	空白是不可接受的

CredentialsScreen

属性	可接受的值	缺省值	注意
CredentialsScreen.Administrator. Username=<value>	<主管理员的用户名>	空白	空白是不可接受的
CredentialsScreen.Administrator. Password=<value>	<主管理员的密码>	空白	空白是不可接受的

可选设置**UpgradeVerificationScreen**

注意：除非检测到现有的安装，否则不会使用此窗口/设置。

属性	可接受的值	缺省值	注意
UpgradeVerificationScreen.Overwrite=<value>	True	False	True 选择全新的管理中心安装，丢弃所有的现有数据
	False		

注意：如果将此值设置为 **True**，则安装将覆盖数据库中的任何现有数据。执行此操作时将不会进行任何进一步的提示。

DatabaseScreen

此窗口可用于定义数据库类型，也可以定义访问某些数据库类型所需的参数。

注意：交互式安装提供了一个“高级”对话框，以定义 Microsoft SQL Server 的实例名称和域，但是由于无人参与的安装不支持对话框，因此这些参数包括在下面的 DatabaseScreen 设置中。

属性	可接受的值	缺省值	注意
DatabaseScreen.DatabaseType=<value>	已嵌入	已嵌入	
	Microsoft SQL Server		
	Oracle		
DatabaseScreen.Hostname=<value>	数据库主机的名称或 IP 地址	当前的主机名	
DatabaseScreen.DatabaseName=<value>	任何字符串	dsm	嵌入式不需要
DatabaseScreen.Transport=<value>	命名管道	命名管道	仅对 SQL Server 是必需的
	TCP		
DatabaseScreen.Username=<value>		空白	空白不是可接受的值。 嵌入式不需要
DatabaseScreen.Password=<value>		空白	空白不是可接受的值。 嵌入式不需要

属性	可接受的值	缺省值	注意
DatabaseScreen.SQLServer.Instance= <value>		空白	空白表示缺省实例。可选，仅对 SQL Server 是必需的
DatabaseScreen.SQLServer.Domain= <value>		空白	可选，仅对 SQL Server 是必需的
DatabaseScreen.SQLServer.UseDefaultCollation=<value>	True	False	可选，仅对 SQL Server 是必需的
	False		

AddressAndPortsScreen

此窗口定义此计算机的主机名、URL 或 IP 地址并定义管理中心的端口。在交互式安装程序中，此窗口还支持将新的管理中心添加到现有的数据库，但是在无人参与的安装中不支持此选项。

属性	可接受的值	缺省值	注意
AddressAndPortsScreen.ManagerAddress= <value>	<管理中心主机的主机名、URL 或 IP 地址>	<当前的主机名>	
AddressAndPortsScreen.ManagerPort= <value>	<有效的端口号>	4119	
AddressAndPortsScreen.HeartbeatPort= <value>	<有效的端口号>	4120	

属性	可接受的值	缺省值	注意
AddressAndPorts.NewNode=<value>	True	False	<p>True 表示当前安装为新节点。</p> <p>如果安装程序在数据库中找到现有数据，则它会将此安装作为新节点添加。（多节点安装始终是静默安装。）</p> <p>注意：有关现有数据库的“新节点”安装信息通过 Database Screen 属性提供。</p>
	False		

Credentials Screen

属性	可接受的值	缺省值	注意
CredentialsScreen.UseStrongPasswords=<value>	True	True	<p>True 表示 DSM 应该设置为强制使用强密码。</p>
	False		

SecurityUpdateScreen

属性	可接受的值	缺省值	注意
SecurityUpdateScreen.UpdateComponents=<value>	True	True	True 表示您希望趋势科技服务器深度安全防护系统管理中心自动检索最新的组件。
	False		
SecurityUpdateScreen.UpdateSoftware=<value>	True	True	True 表示您希望设置一个任务以自动检查新软件。
	False		

RelayScreen

此值控制共置的趋势科技服务器深度安全防护系统中继服务器的安装。

属性	可接受的值	缺省值	注意
RelayScreen.Install=<value>	True	True	如果找到合适的趋势科技服务器深度安全防护系统中继安装包（与 DSM 安装程序位于相同的位置），且此标志设置为 True ，则将自动安装中继服务器。
	False		

SmartProtectionNetworkScreen

此窗口可定义是否要启用趋势科技智能反馈，也可以选择定义您的行业。

属性	可接受的值	缺省值	注意
SmartProtectionNetworkScreen.Enable Feedback=<value>	True	True	True 表示启用趋势科技智能反馈
	False		
SmartProtectionNetworkScreen.IndustryType= <value>	未指定	空白	空白对应于未指定
	银行		
	通信传媒		
	教育		
	能源		
	快速消费品 (FMCG)		
	财务		
	食品饮料		
	政府		
	卫生保健		
	保险		
	制造		
	材料		
	媒体		
	石油和天然气		
	房地产		
零售			
科技			
电信			

属性	可接受的值	缺省值	注意
	运输		
	公用事业		
	其他		

安装输出

本节显示了一个成功安装的示例输出，后跟一个失败安装（使用授权无效）的示例输出。跟踪中的 **[Error]** 标记用于清晰地表示故障。

成功的安装

```

Stopping Trend Micro Deep Security Manager Service...
Detecting previous versions of Trend Micro Deep Security Manager...
Upgrade Verification Screen settings accepted...
Database Screen settings accepted...
License Screen settings accepted...
Address And Ports Screen settings accepted...
Credentials Screen settings accepted...
All settings accepted, ready to execute...
Uninstalling previous version
Stopping Services
Extracting files...
Setting Up...
Connecting to the Database...
Creating the Database Schema...
Updating the Database Data...
Creating MasterAdmin Account...
Recording Settings...
Creating Temporary Directory...
Installing Reports...
Creating Help System...
Setting Default Password Policy...
Importing Example Security Profiles...
Applying Security Update...
Assigning IPS Filters to Example Security Profiles...
Correcting the Port for the Manager Security Profile...
Correcting the Port List for the Manager...
Creating IP List to Ignore...
Creating Scheduled Tasks...
Creating Asset Importance Entries...
Creating Auditor Role...
Auditing...
Optimizing...

```

```
Recording Installation...
Creating Properties File...
Creating Shortcut...
Configuring SSL...
Configuring Service...
Configuring Java Security...
Configuring Java Logging...
Cleaning Up...
Starting Deep Security Manager...
Finishing installation...
```

失败的安装

此示例显示当属性文件包含无效的使用授权字符串时生成的输出：

```
Stopping Trend Micro Deep Security Manager Service...
Detecting previous versions of Trend Micro Deep Security Manager...
Upgrade Verification Screen settings accepted...
Database Screen settings accepted...
Database Options Screen settings accepted...
[ERROR] The license code you have entered is invalid.
[ERROR] License Screen settings rejected...
Rolling back changes...
```

趋势科技服务器深度安全防护系统管理中心内存使用

配置安装程序的最大内存使用量

缺省情况下，将安装程序配置为使用 1GB 连续内存。如果安装程序无法运行，您可以尝试将安装程序配置为使用较少的内存。

为安装程序配置可用的内存量：

- 步骤 1. 转至安装程序所在的目录。
- 步骤 2. 创建一个名为 "Manager-Windows-8.0.xxxx.xxx.vmoptions" 或 "Manager-Linux-8.0.xxxx.xxx.vmoptions" 的新文本文件，具体取决于您的安装平台
(其中 "xxxx.xxx" 是安装程序和平台的 Build 号)。
- 步骤 3. 通过添加以下行来编辑该文件："-Xmx800m" (在本示例中，安装程序可以使用 800MB 内存。)
- 步骤 4. 保存文件并启动安装程序。

配置趋势科技服务器深度安全防护系统管理中心的最大内存使用量

趋势科技服务器深度安全防护系统管理中心最大内存使用量的缺省设置是 4GB。可以更改此设置。

为趋势科技服务器深度安全防护系统管理中心配置可用的内存量：

- 步骤 1. 转至趋势科技服务器深度安全防护系统管理中心目录（Deep Security Manager.exe 所在目录），例如 C:\Program Files\Trend Micro\Deep Security Manager。
- 步骤 2. 创建名为 "Deep Security Manager.vmoptions" 的新文件。
- 步骤 3. 通过添加以下行来编辑该文件：**"-Xmx3g"**（在本示例中，"3g" 将为 DSM 分配 3GB 可用内存。）
- 步骤 4. 保存文件并重新启动 DSM。
- 步骤 5. 您可以通过转至**系统 > 系统信息**来验证新设置，然后在**系统详细信息**区域中，展开**管理中心节点 > 内存**。**最大内存**值现应指示新的配置设置。

趋势科技服务器深度安全防护系统虚拟设备内存使用

下表列出了基于受保护的 VM 数量建议的趋势科技服务器深度安全防护系统虚拟设备最低内存分配量：

趋势科技服务器深度安全防护系统虚拟设备保护的虚拟机数量	建议的内存分配量
1 到 32 台 VM	1GB
33 到 64 台 VM	4GB
65 个以上的 VM	8GB

配置趋势科技服务器深度安全防护系统虚拟设备的内存分配量

注意：更改趋势科技服务器深度安全防护系统虚拟设备的内存分配设置需要关闭 DSVA 虚拟机。在重新打开这些受虚拟设备保护的虚拟机之前，它们将不受保护。

配置趋势科技服务器深度安全防护系统虚拟设备的内存分配量：

- 步骤 1. 在 VMware vSphere Client 中，右键单击 DSVA，然后选择 **Power > Shut Down Guest**。
- 步骤 2. 再次右键单击 DSVA，然后选择 **Edit Settings...**。此时将显示 "Virtual Machine Properties" 窗口。
- 步骤 3. 在 **Hardware** 选项卡上，选择 **Memory** 并将内存分配量更改为所需值。
- 步骤 4. 单击**确定**。
- 步骤 5. 再次右键单击 DSVA，然后选择 **Power > Power On**。

性能功能

性能配置文件

自趋势科技服务器深度安全防护系统管理中心 7.5 SP1 开始，提供了用于优化由管理中心启动的和由客户端/设备启动的操作的性能的新系统。之前，管理中心使用先进先出系统来处理固定数量的并发作业中的所有操作。此方式已被考虑到每个作业对 CPU、数据库和客户端/设备的影响的优化并发计划程序取代。缺省情况下，新安装版本使用针对专用管理中心优化的“主动型”性能配置文件。如果 DSM 安装在装有其他耗费资源的软件的系统上，则优选使用“标准”性能配置文件。可以通过导航至**系统 > 系统信息**，然后单击工具栏中的**管理中心...**按钮来更改性能配置文件。从此窗口中，选择所需的管理中心节点并打开**属性**窗口。可以在此处通过下拉菜单更改性能配置文件。

性能配置文件还控制管理中心将接受的客户端/设备启动的连接的数量。每个性能配置文件的缺省值可以有效地平衡接受的、延迟的和拒绝的波动信号的数量。

磁盘空间不足警报

数据库主机磁盘空间不足

如果趋势科技服务器深度安全防护系统管理中心收到来自数据库的“磁盘已满”错误消息，它将开始将事件写入自身的硬盘驱动器中，并向所有用户发送电子邮件以通知他们该状况。此行为不可配置。

如果运行多个管理中心节点，则会在处理事件的节点中写入事件。（有关运行多个节点的更多信息，请参阅联机帮助或《管理员指南》的**参考**一节中的**多节点管理中心**。）

解决数据库的磁盘空间问题后，管理中心会将本地存储的数据写入数据库中。

管理中心主机磁盘空间不足

管理中心的可用磁盘空间低于 10% 时，管理中心会生成**磁盘空间不足**警报。此警报是正常警报系统的一部分，像其他警报一样可以配置。（有关警报的更多信息，请参阅联机帮助或《管理员指南》的**方法教学**一节中的**警报配置**。）

如果运行多个管理中心节点，会在警报中标识该节点。

当管理中心的可用磁盘空间低于 5MB 时，管理中心会向所有用户发送电子邮件，并且管理中心将关闭。只有在可用磁盘空间大于 5MB 后管理中心才可重新启动。

必须手动重新启动管理中心。

如果运行多个节点，则只有磁盘空间不足的节点会关闭。其他管理中心节点会继续运行。

创建 SSL 认证证书

趋势科技服务器深度安全防护系统管理中心为 Web 浏览器到管理中心之间的连接创建为期 10 年的自签名证书。如果需要，可以使用实际的证书替换此证书。（在趋势科技服务器深度安全防护系统管理中心升级时会保留该证书。）

可以在 [Thawte Tomcat Support](#) 处找到有关生成证书的更多信息。

生成后，该证书应导入到趋势科技服务器深度安全防护系统管理中心安装根目录中的 .keystore 中，且使用别名 "tomcat"。之后，管理中心将使用该证书。

创建 SSL 认证证书：

- 步骤 1. 转到趋势科技服务器深度安全防护系统管理中心安装目录 (C:\Program Files\Trend Micro\Deep Security Manager)，创建名为 "**Backupkeystore**" 的新文件夹
- 步骤 2. 将 **.keystore** 和 **configuration.properties** 复制到新创建的文件夹 Backupkeystore
- 步骤 3. 打开命令提示符并转到以下位置：

```
C:\Program Files\ Trend Micro \Deep Security Manager\jre\bin
```

步骤 4. 运行以下命令，该命令将创建一个自签名证书：

```
C:\Program Files\ Trend Micro \Deep Security  
Manager\jre\bin>keytool -genkey -alias tomcat -keyalg RSA  
-dname cn=dsmsserver
```

步骤 5. 选择密码：changeit

注意：-dname 是 CA 将签发的证书的常用名。某些 CA 要求使用特殊的 cn 来对证书签名请求 (CSR) 进行签名。请咨询您的 CA 管理员以查看是否具有该特殊要求。

步骤 6. 在用户主目录下创建了新的密钥库文件。如果以 "Administrator" 身份登录，则会在 C:\Documents and Settings\Administrator 下看到该 **.keystore** 文件

步骤 7. 使用以下命令查看新生成的证书：

```
C:\Program Files\ Trend Micro \Deep Security  
Manager\jre\bin>keytool -list -v
```

步骤 8. 运行以下命令以创建需要 CA 签名的 CSR：

```
C:\Program Files\ Trend Micro \Deep Security  
Manager\jre\bin>keytool -certreq -keyalg RSA -alias tomcat  
-file certrequest.csr
```

步骤 9. 将 **certrequest.csr** 发送给 CA 以进行签名。将返回两个文件。一个是证书响应，另一个是 CA 证书本身。

步骤 10. 运行以下命令将 CA 证书导入 JAVA 可信密钥库：

```
C:\Program Files\Trend Micro\Deep Security  
Manager\jre\bin>keytool -import -alias root -trustcacerts -file  
cacert.crt -keystore "C:/Program Files/ Trend Micro /Deep  
Security Manager/jre/lib/security/cacerts"
```

步骤 11. 运行以下命令将 CA 证书导入您的密钥库：

```
C:\Program Files\ Trend Micro \Deep Security  
Manager\jre\bin>keytool -import -alias root -trustcacerts -file  
cacert.crt
```

(出现警告消息时单击“是”)

步骤 12. 运行以下命令将证书响应导入您的密钥库：

```
C:\Program Files\Trend Micro\Deep Security
Manager\jre\bin>keytool -import -alias tomcat -file
certresponse.txt
```

步骤 13. 运行以下命令查看密钥库中的证书链：

```
C:\Program Files\Trend Micro\Deep Security
Manager\jre\bin>keytool -list -v
```

步骤 14. 将 .keystore 文件从用户主目录 C:\Documents and Settings\Administrator 复制到 C:\Program Files\Trend Micro\Deep Security Manager\

步骤 15. 打开文件夹 C:\Program Files\Trend Micro\Deep Security Manager 中的 configuration.properties 文件。它将类似于以下内容：

```
keystoreFile=C:\\\\Program Files\\\\Trend Micro\\\\Deep
Security Manager\\\\.keystore port=4119
keystorePass=$1$85ef650a5c40bb0f914993ac1ad855f48216fd0664ed254
4bbec6de80160b2fe9800f79f913f28e80381c8e71f2fed96a2aa522ada039a
7abfa01542d42dbe36 installed=true serviceName= Trend Micro Deep
Security Manager
```

步骤 16. 替换以下字符串中的密码：

```
keystorePass=xxxx
```

其中 "xxxx" 是在步骤五中提供的密码

步骤 17. 保存并关闭该文件

步骤 18. 重新启动 Deep Security Manager 服务

步骤 19. 使用浏览器连接到趋势科技服务器深度安全防护系统管理中心，您将注意到新的 SSL 证书已经过 CA 签名

与客户端和设备版本的互操作性


下表概述了 *当前支持* 的趋势科技服务器深度安全防护系统软件组件版本之间的互操作性。请记住，旧版本的趋势科技服务器深度安全防护系统客户端或趋势科技服务器深度安全防护系统虚拟设备不能提供新版本的趋势科技服务器深度安全防护系统管理中心中引入的功能。


	DSM 8.0	DSM 7.5	DSM 7.0
DSA 8.0	✓	✗	✗
DSA 7.5	✓	✓	✗
DSA 7.0	✓	✓	✓
DSA 6.1	✗	✓	✓
DSVA 8.0	✓	✗	✗
DSVA 7.5	✓	✓	✗
DSVA 7.0	✗	✓	✓

DSM: 趋势科技服务器深度安全防护系统管理中心

DSA: 趋势科技服务器深度安全防护系统客户端

DSVA: 趋势科技服务器深度安全防护系统虚拟设备

: 可互操作

: 不可互操作

故障排除

注意：有关在“故障排除”和 FAQ 两节中未解决的任何问题，请查阅趋势科技服务器深度安全防护系统管理中心、趋势科技服务器深度安全防护系统客户端和趋势科技服务器深度安全防护系统虚拟设备的“自述文件”。

趋势科技服务器深度安全防护系统管理中心

安装

问题

在同一计算机上安装两个趋势科技服务器深度安全防护系统管理中心时遇到问题。

解决方案

在任何给定计算机上只能安装一个趋势科技服务器深度安全防护系统管理中心实例。

问题

无法安装或升级趋势科技服务器深度安全防护系统管理中心。

解决方案

在安装或升级趋势科技服务器深度安全防护系统管理中心过程中，如果在某些平台上打开了“服务”窗口，则无法正确安装该服务。请在安装或升级趋势科技服务器深度安全防护系统管理中心之前关闭“服务”窗口。

如果问题仍然存在，请重新启动计算机。

通信

问题

保护趋势科技服务器深度安全防护系统管理中心的客户端生成“续订”错误，并且/或者您无法远程连接到趋势科技服务器深度安全防护系统管理中心。

解决方案

应用 "Deep Security Manager" 安全配置文件之后，您可能注意到趋势科技服务器深度安全防护系统客户端会返回大量“续订错误” DPI 事件。这是因为客户端无法检测在应用 "Deep Security Manager" 安全配置文件和其 SSL 主机配置之前已存在的 SSL 通信。建议在应用 "Deep Security Manager" 安全配置文件之后重新启动访问趋势科技服务器深度安全防护系统管理中心的所有浏览器会话。

问题

趋势科技服务器深度安全防护系统管理中心管理的计算机上发出“检测到通信问题”警报。

或者

准备 ESX 时出现脱机 Bundle.zip 错误。

或者

部署趋势科技服务器深度安全防护系统虚拟设备时出现脱机 Bundle.zip 错误。

或者

激活趋势科技服务器深度安全防护系统设备时出现协议错误。

解决方案

如果遇到上述任何情况，可能是趋势科技服务器深度安全防护系统管理中心管理的计算机无法解析托管趋势科技服务器深度安全防护系统管理中心的计算机的主机名造成的。

确保趋势科技服务器深度安全防护系统管理中心可以解析托管趋势科技服务器深度安全防护系统管理中心的计算机的主机名：

1. 登录到管理客户端的趋势科技服务器深度安全防护系统管理中心
2. 转到**系统 > 系统信息**，在“系统详细信息”中，查看“管理中心节点”条目并记下主机名
3. 登录到存在通信问题的计算机
4. 使用步骤 2 中得到的名称执行 nslookup
5. 如果 nslookup 不成功，您必须修改计算机上的 hosts 文件以使用 DSM 主机名及正确的 IP 地址，或更新指定 DNS 服务器上趋势科技服务器深度安全防护系统管理中心计算机的 DNS 条目

注意：要更改虚拟设备上的 hosts 文件，必须通过 vCenter 进行登录。进入控制台后，按 ALT+F2 进入控制台登录窗口。然后键入：`sudo vi /etc/hosts`

配置

问题

流量分析不起作用。

解决方案

状态配置必须打开，并且启用 TCP 和 UDP 日志记录。

问题

在保护趋势科技服务器深度安全防护系统管理中心使用的数据库的客户端上，触发
了许多 DPI 规则。

解决方案

当趋势科技服务器深度安全防护系统管理中心使用的数据库位于运行趋势科技服
务器深度安全防护系统客户端 (DSA) 的远程计算机上时，可能发生 DPI 误报。误报是
由于触发在 DSA 上运行的 DPI 规则的 DPI 规则的内容（保存到数据库时）造成的。
解决方法是创建应用到其源 IP 是趋势科技服务器深度安全防护系统管理中心的静
态 IP 的数据库服务器的绕过防火墙规则，或是在数据库通道上启用加密。可以通
过将以下内容：

```
database.SqlServer.ssl=require
```

添加到 `\webclient\webapps\ROOT\WEB-INF\dsm.properties` 并重新启动 Deep
Security Manager 服务来对 SQL Server 进行加密。

问题

端口扫描显示端口 25 和 110 始终处于打开状态，不管执行哪些防火墙规则来关闭
它们。

解决方案

Norton Antivirus 的存在可能干扰扫描结果。Norton AV 过滤端口 25 和 110 以检查传
入和传出的电子邮件中是否存在病毒。如果管理中心安装在已启用电子邮件扫描的
计算机上，这会导致大量扫描结果，因为端口 25 和 110 将始终显示为打开状态，不
管在主机上应用了何种过滤器。

问题

端口扫描显示端口 21、389、1002 和 1720 处于打开状态，不管执行哪些防火墙规则
来关闭它们。

解决方案

如果在趋势科技服务器深度安全防护系统管理中心上启用了 Windows 防火墙，则它
可能将干扰端口扫描，从而产生错误的端口扫描结果。Windows 防火墙可以代理端
口 21、389、1002 和 1720，这样不管该主机上放置了任何过滤器，这些端口都始终
显示为打开状态。

趋势科技服务器深度安全防护系统虚拟设备

部署

问题

准备 ESX/ESXi 时发生超时。

解决方案

为了成功安装过滤器驱动程序，必须重新启动正在其上部署的 ESX/ESXi。趋势科技服务器深度安全防护系统管理中心提供了自动重新启动服务器的选项。如果选择了此选项，则必须暂停/停止在此 ESX/ESXi 主机上运行的所有虚拟机，或者将这些虚拟机 vMotion 到范围之外。如果不这样做，则 ESX/ESXi 无法进入维护模式且无法重新启动。如果 ESX/ESXi 无法进入维护模式，趋势科技服务器深度安全防护系统管理中心将报告超时问题。

问题

无法联系趋势科技服务器深度安全防护系统虚拟设备。

解决方案

缺省情况下，趋势科技服务器深度安全防护系统虚拟设备在部署时使用 DHCP 获取 IP 地址。如果在没有 DHCP 服务器的环境中进行部署，则必须为设备分配静态 IP 地址。

为虚拟设备分配静态 IP 地址：

1. 使用 vSphere Client 登录到托管趋势科技服务器深度安全防护系统虚拟设备的 Virtual Center
2. 选择设备，然后单击控制台选项卡
3. 按 F2 并使用缺省用户名和密码 (dsva:dsva) 登录到设备
4. 从菜单中选择“配置管理网络”，然后按 Enter 键
5. 更改主机名、IP 地址、子网掩码、网关和 DNS 条目使之与您的网络相匹配
6. 按 Enter 键保存更改
7. 从主菜单中选择“重新启动系统”来重新启动设备

配置

问题

防恶意软件扫描异常终止。

解决方案

虚拟机必须处于运行状态才能成功完成扫描。此中止可能是由于扫描期间虚拟机被关闭或挂起导致的。请检查虚拟机的状态，然后重试。

当客户 VM 重新启动或进入睡眠或待机模式时，会发生此情况。

趋势科技服务器深度安全防护系统客户端

安装

问题

在安装 Solaris 客户端期间遇到以下错误：

```
## Executing postinstall script.  
devfsadm: driver failed to attach: dsa_filter  
Warning: Driver (dsa_filter) successfully added to system but failed to  
attach  
Starting Trend Micro Deep Security Drivers  
can't load module: Invalid argument
```

解决方案

某些 Solaris Patch 更改了系统上运行的 netinfo 的版本。netinfo 的版本决定了特定系统所需的客户端安装包。

要确定系统的 netinfo 版本，请运行以下命令：

```
modinfo | grep neti
```

文件大小决定了要使用的安装包：

文件大小	安装包
74c	u5sparc
1abc	u7sparc
ec8	u5x86
2600	u7x86

有关更多详细信息，可以查看 `/var/adm/messages`。

以下条目表示您正尝试在需要 U5 客户端的计算机上安装 U7 客户端：

```
Feb 19 11:14:58 Sparc-v210-2 unix: [ID 819705 kern.notice]
/usr/kernel/drv/sparcv9/dsa_filter: undefined symbol
Feb 19 11:14:58 Sparc-v210-2 unix: [ID 826211 kern.notice]
'net_protocol_release'
Feb 19 11:14:58 Sparc-v210-2 unix: [ID 819705 kern.notice]
/usr/kernel/drv/sparcv9/dsa_filter: undefined symbol
Feb 19 11:14:58 Sparc-v210-2 unix: [ID 826211 kern.notice] 'hook_alloc'
Feb 19 11:14:58 Sparc-v210-2 unix: [ID 819705 kern.notice]
/usr/kernel/drv/sparcv9/dsa_filter: undefined symbol
Feb 19 11:14:58 Sparc-v210-2 unix: [ID 826211 kern.notice]
'net_hook_register'
Feb 19 11:14:58 Sparc-v210-2 unix: [ID 819705 kern.notice]
/usr/kernel/drv/sparcv9/dsa_filter: undefined symbol
Feb 19 11:14:58 Sparc-v210-2 unix: [ID 826211 kern.notice] 'hook_free'
Feb 19 11:14:58 Sparc-v210-2 unix: [ID 819705 kern.notice]
/usr/kernel/drv/sparcv9/dsa_filter: undefined symbol
Feb 19 11:14:58 Sparc-v210-2 unix: [ID 826211 kern.notice]
'net_protocol_lookup'
Feb 19 11:14:58 Sparc-v210-2 unix: [ID 819705 kern.notice]
/usr/kernel/drv/sparcv9/dsa_filter: undefined symbol
Feb 19 11:14:58 Sparc-v210-2 unix: [ID 826211 kern.notice]
'net_hook_unregister'
Feb 19 11:14:58 Sparc-v210-2 unix: [ID 472681 kern.notice] WARNING:
mod_load: cannot load module 'dsa_filter'
```

以下条目表示您正尝试在需要 U7 客户端的计算机上安装 U5 客户端：

```
Feb 19 11:19:36 Sparc-v210-1 unix: [ID 819705 kern.notice]
/usr/kernel/drv/sparcv9/dsa_filter: undefined symbol
Feb 19 11:19:36 Sparc-v210-1 unix: [ID 826211 kern.notice]
'net_unregister_hook'
```

```
Feb 19 11:19:36 Sparc-v210-1 unix: [ID 819705 kern.notice]
/usr/kernel/drv/sparcv9/dsa_filter: undefined symbol
Feb 19 11:19:36 Sparc-v210-1 unix: [ID 826211 kern.notice]
'net_register_hook'
Feb 19 11:19:36 Sparc-v210-1 unix: [ID 819705 kern.notice]
/usr/kernel/drv/sparcv9/dsa_filter: undefined symbol
Feb 19 11:19:36 Sparc-v210-1 unix: [ID 826211 kern.notice] 'net_lookup'
Feb 19 11:19:36 Sparc-v210-1 unix: [ID 819705 kern.notice]
/usr/kernel/drv/sparcv9/dsa_filter: undefined symbol
Feb 19 11:19:36 Sparc-v210-1 unix: [ID 826211 kern.notice] 'net_release'
Feb 19 11:19:36 Sparc-v210-1 unix: [ID 472681 kern.notice] WARNING:
mod_load: cannot load module 'dsa_filter'
```

问题

趋势科技服务器深度安全防护系统客户端无法启动。

解决方案

有几种情况可能会使 ds_agent 服务无法启动。原因包括：凭证无效（尚无效、已损坏、已过期、数字签名错误）、无法读取私钥（已损坏、硬件已发生根本改变）、侦听端口已在使用中。

如果 DSA 无法启动，则它将无法向 DSM 报告，因此它将写入 Windows 事件日志。您应该检查 Windows 事件日志以诊断问题。

激活

问题

已安装趋势科技服务器深度安全防护系统客户端，但客户端 UI 显示空白文本框。

解决方案

如果“管理中心 URL”、“管理中心证书名称”和“管理中心证书指纹”文本框为空，则未激活客户端。在趋势科技服务器深度安全防护系统管理中心激活客户端之前，这些文本框将始终为空。在 DSM 的**计算机**列表中找到计算机，右键单击该计算机，然后选择**操作 > 激活/重新激活**。

问题

在“客户端激活不成功”系统事件中出现以下错误消息：“在从 DSM 到 DSA 协议中发生客户端错误: 收到 HTTP 客户端错误: 证书尚无效”。

解决方案

趋势科技服务器深度安全防护系统客户端计算机上的时钟必须 24 小时与趋势科技服务器深度安全防护系统管理中心同步。如果 DSA 时钟在 DSM 时钟之后，则“客户端激活”操作将不能成功，因为趋势科技服务器深度安全防护系统管理中心为客户端生成的证书尚无效。

配置

问题

在计算机上看到 DSA_IOCTL_SET_FILTER_CONFIG 错误，描述为：

```
Engine command code DSA_IOCTL_SET_FILTER_CONFIG failed with error: 0x0005aa  
(insufficient system resources exist to complete the requested service.).
```

解决方案

这可能是由于以下两个原因之一造成的：

1. 系统正使用 /3GB 启动选项运行。

/3GB 标志减少内核的可用内存量，从而减少了内核中不可分页内存量。确切的数量受众多因素的影响，如 TCP 烟囱卸载、在 4GB 寻址空间上使用大量内存、外部设备驱动程序（如声音、视频）等。

2. 针对驱动程序的可用内核内存量，在计算机应用的规则过多。

在这些情况下，必须减少应用于计算机的防火墙和 DPI 规则的数量，以减少内存占用并改善性能。趋势科技服务器深度安全防护系统的建议扫描功能可起到帮助作用。通过扫描计算机以提供建议，您可以使用计算机的“DPI 规则”页面的“显示建议取消分配的项目”视图，取消分配对于保持适当安全性非必需的 DPI 规则。如果您通过安全配置文件管理计算机，可以使用相同的“显示建议取消分配的项目”视图，但请注意，该视图将仅显示在分配有这些安全配置文件的任何计算机上不建议使用的 DPI 规则，并且可能仍保留一组 DPI 规则，这些 DPI 规则的需求对于某些计算机而言过高。如果安全配置文件本身仍分配有过多 DPI 规则，则有必要创建其他安全配置文件并在它们之间分配计算机，以使得这些安全配置文件可以更好的表示实际上向各种计算机建议应用的 DPI 规则。这可以使您减少分配到所有计算机的 DPI 规则的数量。

诊断信息收集

问题

支持提供商要求提供诊断数据包。

解决方案

在趋势科技服务器深度安全防护系统管理中心中，转至**系统 > 系统信息**，然后单击工具栏中的“创建诊断数据包...”。这将显示“诊断数据包向导”，该向导将创建一个 zip 文件，文件中包含安装/卸载和调试日志、系统信息、数据库内容（与时间相关项目仅包括最后一小时的内容）以及文件列表。可以将此信息提供给您的支持提供商以帮助解决任何问题。

问题

支持提供商要求增加诊断数据包的大小。

解决方案

诊断数据包的缺省最大大小约为 200MB。可使用以下命令行指令来增加诊断数据包的大小：

```
dsm_c -action changesetting -name configuration.diagnosticMaximumFileSize  
-value #####
```

以下示例将数据包的大小增加到 1GB (1000MB)：

```
dsm_c -action changesetting -name configuration.diagnosticMaximumFileSize  
-value 1000
```

不要更改诊断数据包的大小，除非您的支持提供商指示您这样做。

问题

无法使用 Internet Explorer 7 创建诊断数据包。

解决方案

导出文件（CVS、XML、软件或更新）或创建诊断数据包时，Internet Explorer 的“信息栏”可能通知您文件下载已被阻止，趋势科技服务器深度安全防护系统管理中心将指示您“检查 server0.log”。要允许文件下载，请单击信息栏中的“更多信息”并遵循指导信息以允许文件和软件下载。

FAQ

注意：有关在“故障排除”和 FAQ 两节中未解决的任何问题，请查阅趋势科技服务器深度安全防护系统管理中心、趋势科技服务器深度安全防护系统虚拟设备或趋势科技服务器深度安全防护系统客户端的自述文件。

从哪里可以下载趋势科技服务器深度安全防护系统 8.0 的安装包？

趋势科技下载专区 — <http://www.trendmicro.com/download/zh-cn/>

从哪里可以下载趋势科技服务器深度安全防护系统 8.0 的技术文档？

趋势科技下载专区 — <http://www.trendmicro.com/download/zh-cn/>

登录趋势科技服务器深度安全防护系统管理中心控制台所使用的缺省用户名和密码是什么？

在安装期间，系统会提示您输入用户名和密码。登录管理中心控制台的缺省用户名是 "MasterAdmin"（无半角引号）。无缺省密码。用户名和密码均可以在安装期间进行设置。用户名不区分大小写。但密码区分大小写。

我可以重置管理中心控制台登录密码吗？

是的。您可以重置或更改管理中心控制台登录密码。转至**系统 > 用户**，然后右键单击用户并选择**设置密码...**。

如何解锁已锁定的用户？

在管理中心中，转至**系统 > 用户**，然后右键单击用户并选择**解锁用户**。

要从管理中心主机命令行解锁用户，请从趋势科技服务器深度安全防护系统管理中心的安装目录中输入以下命令：

```
dsm_c -action unlockout -username USERNAME [-newpassword NEWPASSWORD]
```

其中，USERNAME 是用户的用户名。可以选择使用 "-newpassword" 为用户设置新密码。

登录管理中心控制台时，我可以使用的域帐户凭证吗？

是的。转至“系统”>“用户”，然后选择“与目录同步”。

如何将客户端成批部署到受保护的计算机？

组织通常使用现有的企业软件分发系统（如 Microsoft System Center™ 或 Novell™ ZENworks™）来安装客户端。

升级到 8.0 版本之后我是否仍然可以使用现有的使用授权或激活码？

将支持您的现有防护模块。从趋势科技服务器深度安全防护系统 7.0 或更低版本升级时，您将需要联系销售代表以获取要在升级过程中输入的新激活码。

我可以从管理中心控制台卸载 DS 客户端吗？

不可以。您可以从 DSM 停用客户端/设备，但必须从本地进行卸载。

趋势科技服务器深度安全防护系统的生命周期多长或支持策略是什么？

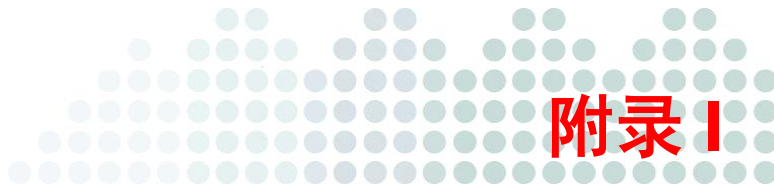
- 自发布起提供为期两年的产品支持，或者
- 发布后续版本之后提供为期 18 个月的产品支持，取以上二者中更长者

如何从命令行停用 DS 客户端？

请参阅《管理员指南》的“手动停用/停止/启动客户端/设备”章节。该操作与平台相关。

如何手动更新未与 DS 管理中心连接的 DS 客户端？

如果未连接到管理中心，则无法更新客户端，因为管理中心必须向客户端发送安全配置详细信息。



已知不兼容软件

注意：有关已知不兼容软件的最新列表，请查阅趋势科技服务器深度安全防护系统管理中心、趋势科技服务器深度安全防护系统虚拟设备或趋势科技服务器深度安全防护系统客户端的自述文件。

卸载趋势科技服务器深度安全防护系统

注意：从被管理计算机卸载激活的客户端或中继时，趋势科技服务器深度安全防护系统管理中心并不知道已卸载该软件。该计算机仍将列在“计算机”列表中，其状态将列为“被管理(脱机)”或者其他等效内容（取决于上下文）。要避免此情况，请在卸载前从管理中心停用客户端或中继，或者只需从列表中删除该计算机。

删除趋势科技服务器深度安全防护系统虚拟设备

删除虚拟设备：

1. 使用趋势科技服务器深度安全防护系统管理中心“停用”虚拟设备。
2. 登录到 vCenter。
3. 停止设备。
4. 从磁盘删除。

从准备好的 ESX/ESXi 移除趋势科技服务器深度安全防护系统过滤器驱动程序

将 ESX/ESXi 恢复到“未准备就绪”状态：

1. 从趋势科技服务器深度安全防护系统管理中心**计算机**列表中，选择 Virtual Center。选择要取消部署的已准备计算机，然后右键单击该计算机并选择**恢复 ESX**。
2. 遵循向导中的步骤，接受缺省值。
3. 选择“是”以使 DSM 自动处理 ESX/ESXi 驱动程序卸载。

注意：趋势科技服务器深度安全防护系统管理中心将尝试使 ESX/ESXi 自动进入和退出维护模式。需要手动关闭所有正在运行的虚拟机。在卸载过程完成时，ESX/ESXi 将自动重新启动并退出维护模式。

或者

选择“否”以手动使 ESX/ESXi 进入/退出维护模式。

注意：ESX/ESXi 进入维护模式后，趋势科技服务器深度安全防护系统管理中心向导将自动启动过滤器驱动程序的卸载过程。在卸载过程完成时，ESX/ESXi 将自动重新启动但仍处于维护模式。

卸载趋势科技服务器深度安全防护系统中继

注意：请记住，在卸载趋势科技服务器深度安全防护系统中继之前，将需要删除客户端自我防护。可以从趋势科技服务器深度安全防护系统管理中心**系统 > 系统设置 > 计算机**执行此操作。在**客户端自我防护**中，取消选中**防止本地最终用户卸载、停止或以其他方式修改客户端**设置或为本地覆盖选择密码。

卸载趋势科技服务器深度安全防护系统中继 (Windows)

从 Windows “控制面板” 中，选择 “添加/删除程序”。双击列表中的**趋势科技服务器深度安全防护系统中继**，然后单击**更改/删除**。

从命令行进行卸载：

```
msiexec /x <软件包名称 (包括扩展名) >
```

(对于静默卸载，请添加 "/quiet")

卸载趋势科技服务器深度安全防护系统中继 (Linux)

要完全移除中继及其创建的任何配置文件，请使用 "rpm -e"：

```
# rpm -ev ds_relay
Stopping ds_agent: [ OK ]
Unloading dsa_filter module [ OK ]
```

如果在安装趋势科技服务器深度安全防护系统客户端之前启用了 iptables，则会在卸载客户端后重新启用 iptables。

注意：请记住，从趋势科技服务器深度安全防护系统管理中心的被管理计算机列表中移除中继，并将其从中继组中移除（请参阅[趋势科技服务器深度安全防护系统基本配置](#)）。

卸载趋势科技服务器深度安全防护系统客户端

注意：请记住，在卸载趋势科技服务器深度安全防护系统客户端之前，将需要删除客户端自我防护。可以从趋势科技服务器深度安全防护系统管理中心**系统 > 系统设置 > 计算机**执行此操作。在**客户端自我防护**中，取消选中**防止本地最终用户卸载、停止或以其他方式修改客户端**设置或为本地覆盖选择密码。

卸载趋势科技服务器深度安全防护系统客户端 (Windows)

从 Windows “控制面板” 中，选择 “添加/删除程序”。双击列表中的**趋势科技服务器深度安全防护系统客户端**，然后单击**更改/删除**。

从命令行进行卸载：

```
msiexec /x <软件包名称 (包括扩展名) >
```

(对于静默卸载，请添加 "/quiet")

卸载趋势科技服务器深度安全防护系统客户端 (Linux)

要完全移除客户端及其创建的任何配置文件，请使用 "rpm -e"：

```
# rpm -ev ds_agent
Stopping ds_agent: [ OK ]
Unloading dsa_filter module [ OK ]
```

如果在安装趋势科技服务器深度安全防护系统客户端之前启用了 iptables，则会在卸载客户端后重新启用 iptables。

对于 Ubuntu：

```
$ sudo dpkg -r ds-agent
```

```
Removing ds-agent...
```

```
Stopping ds_agent: .[OK]
```

卸载趋势科技服务器深度安全防护系统客户端 (Solaris)

输入以下命令：

```
pkgrm ds-agent
```

(请注意，卸载可能需要重新启动。)

卸载趋势科技服务器深度安全防护系统客户端 (AIX)

输入以下命令：

```
installp -u ds_agent
```

卸载趋势科技服务器深度安全防护系统客户端 (HP-UX)

输入以下命令：

```
/tmp> swremove ds_agent
```

卸载趋势科技服务器深度安全防护系统通知程序

卸载趋势科技服务器深度安全防护系统通知程序 (Windows)

从 Windows “控制面板” 中，选择“添加/删除程序”。双击列表中的**趋势科技服务器深度安全防护系统通知程序**，然后单击**删除**。

从命令行进行卸载：

```
msiexec /x <软件包名称（包括扩展名）>
```

（对于静默卸载，请添加 "/quiet"）

卸载趋势科技服务器深度安全防护系统管理中心

注意：请记住，在卸载趋势科技服务器深度安全防护系统管理中心之前，应该停用并卸载该管理中心管理的任何趋势科技服务器深度安全防护系统客户端或中继。如果此时不希望卸载客户端，则应该通过从趋势科技服务器深度安全防护系统管理中心**系统 > 系统设置 > 计算机配置**客户端自我保护来确保稍后可以执行此操作。

卸载趋势科技服务器深度安全防护系统管理中心 (Windows)

从 Windows “开始” 菜单中，选择**趋势科技 > 趋势科技服务器深度安全防护系统管理中心卸载程序**，然后按照向导步骤完成卸载。

从命令行进行卸载：

```
Uninstall.exe
```

（对于静默卸载，请添加 "-q"）

注意：在命令行卸载中，卸载程序始终保存配置文件，以便将来的安装可以提供修复/升级选项。

卸载趋势科技服务器深度安全防护系统管理中心 (Linux)

从命令行进行卸载：

```
Uninstall.exe
```

（对于静默卸载，请添加 "-q"）

注意：在命令行卸载中，卸载程序始终保存配置文件，以便将来的安装可以提供修复/升级选项。

如果选择了“否”以在卸载期间保留配置文件并希望重新安装 DSM，则应该先执行手动清理再重新安装。要移除 DSM 安装目录，请输入以下命令：

```
rm -rf <安装位置>
```

（缺省的安装位置是 "/opt/dsm"）。

部署 DSVA 所需的最低 VMware 权限

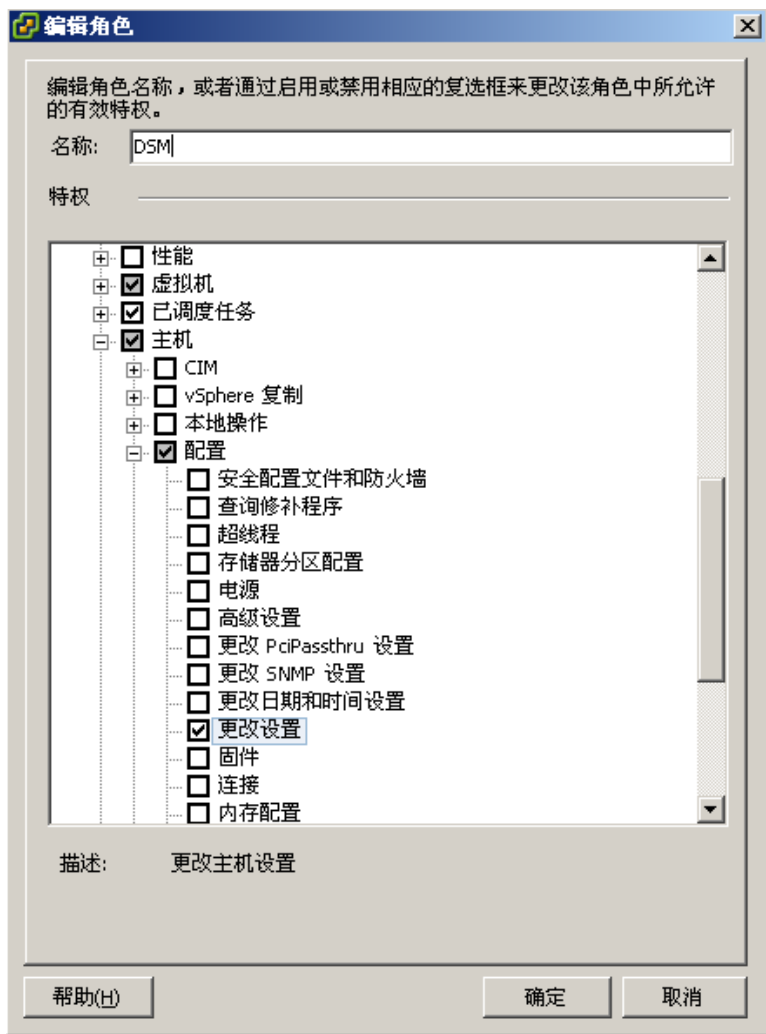
以下各表列出了 VMware 角色所需的 VMware 环境权限，该 VMware 角色被分配给趋势科技服务器深度安全防护系统管理中心部署趋势科技服务器深度安全防护系统虚拟设备所使用的帐户。（该帐户用于在将 vCenter 导入到趋势科技服务器深度安全防护系统管理中心时连接到 vCenter。）

必须在“主机和群集”视图中在数据中心级别上应用这些权限。安装需要获取各种实体的父 ID 的能力。仅在群集级别上应用权限将生成错误。

这些表分为以下四个阶段：

1. **准备 ESX/ESXi 主机。** 在 ESX/ESXi 主机上加载内核驱动程序，并配置单独的 vSwitch 以便于加速 DSVA 的内部连接。
2. **部署虚拟设备。** 虚拟设备本身是从 OVF 文件部署的。
3. **使用趋势科技服务器深度安全防护系统管理中心激活虚拟机。** 向趋势科技服务器深度安全防护系统管理中心注册受虚拟设备保护的计算机并建立安全通信。
4. **持续的操作。** 日常的 trend 趋势科技服务器深度安全防护系统操作。

以下各表列出了必需的权限和需要该权限的功能。要设置权限，请使用 vSphere Client 编辑趋势科技服务器深度安全防护系统管理中心访问 vCenter 所使用的角色的属性。在 VMware Role Editor 的 Privileges 树中可以找到所需的权限。例如，以下窗口截图显示主机 > 配置 > 更改设置权限的位置：



准备 ESX/ESXi 主机

权限	功能
主机 > 配置 > 更改设置	在 ESX/ESXi 上查询模块
主机 > 配置 > 维护	进入和退出维护模式
主机 > 配置 > 网络配置	添加新的虚拟交换机、端口组、虚拟 NIC 等
主机 > 配置 > 高级设置	在 ESX/ESXi 上设置网络以便进行 dvfilter 通信
主机 > 配置 > 查询 Patch	安装过滤器驱动程序
主机 > 配置 > 连接	断开/重新连接主机
主机 > 配置 > 安全配置文件和防火墙	重新配置传出防火墙连接以便允许从 DSM 检索过滤器驱动程序包
全局 > 取消任务	取消任务（需要时）所需

部署虚拟设备

权限	功能
vApp > 导入	从 OVF 文件部署 DSVA
数据存储 > 分配空间	在数据存储上为 DSVA 分配空间
主机 > 配置 > 虚拟机自动启动配置	将 DSVA 设置为在 ESX/ESXi 上自动启动
网络 > 分配网络	将 DSVA 分配给网络
虚拟机 > 配置 > 添加新磁盘	将磁盘添加到 DSVA
虚拟机 > 交互 > 打开	打开 DSVA
虚拟机 > 交互 > 关闭	关闭 DSVA

激活虚拟机（受保护的计算机）

权限	功能
虚拟机 > 配置 > 高级	为 dvfilter 重新配置虚拟机

持续的操作

权限	功能
主机 > 配置 > 更改设置	在 ESX/ESXi 上查询模块
虚拟机 > 配置 > 高级	为 dvfilter 重新配置虚拟机



趋势科技（中国）有限公司

上海市淮海中路 398 号世纪巴士大厦 8 楼

免费技术支持电话：800-820-8839 联系电话：021-6384 8899

传真：021-6384 1899 info@trendmicro.com

www.trendmicro.com

Item Code: APCM85395/120425