TREND MICRO

9.5 趋势科技服务器深度安全防护系统

安装指南 基本组件

专为物理、虚拟和云服务器而设计的高级防护

Cloud & Data Center

Complete End User

Cyber Threats

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 t- 球徽标、Deep Security、Control Server Plug-in、Damage Cleanup Services、eServer Plug-in、InterScan、Network VirusWall、ScanMail、ServerProtect 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。

文档版本：1.2
文档编号：APCM96702/141014
发布日期：2014 年 11 月
文档生成时间：Dec 4, 2014 (10:20:55)

目录

简介 4

关于本文档 5

关于趋势科技服务器深度安全防护系统 7

趋势科技服务器深度安全防护系统 9.5 中的新增功能 10

准备 11

系统要求 12

所需条件（基础组件） 14

数据库部署注意事项 17

安装 19

安装趋势科技服务器深度安全防护系统管理中心 20

安装趋势科技服务器深度安全防护系统客户端 27

安装和配置已启用中继的客户端 34

数据库部署注意事项 17

快速入门 37

快速入门：系统配置 38

快速入门：保护计算机 46

附录 53

趋势科技服务器深度安全防护系统管理中心内存使用 54

趋势科技服务器深度安全防护系统管理中心静默安装 55

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 57

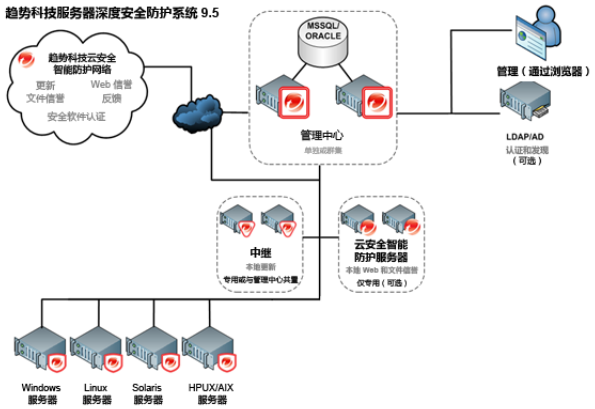
趋势科技服务器深度安全防护系统管理中心性能特点 62

创建 SSL 认证证书 64

简介

关于本文档

趋势科技服务器深度安全防护系统 9.5 安装指南（基础）



本文档讲述了如何安装和配置为您的计算机提供基于客户端的基础保护所需的趋势科技服务器深度安全防护系统 9.5 基础软件组件：

1. 趋势科技服务器深度安全防护系统管理中心
2. 趋势科技服务器深度安全防护系统客户端（带可选的中继功能）

本文档内容包括：

1. 系统要求
2. 准备
3. 数据库配置指南
4. 安装趋势科技服务器深度安全防护系统管理中心管理控制台
5. 安装趋势科技服务器深度安全防护系统客户端
6. 使用“安全策略”和“漏洞扫描（推荐设置）”进行趋势科技服务器深度安全防护系统防护
7. 监控和维护趋势科技服务器深度安全防护系统安装的指南

目标受众

本文档面向想实施基于客户端的趋势科技服务器深度安全防护系统 9.5 保护的任何人。其中信息是针对经验丰富的系统管理员编写的，这些管理员具有丰富的软件部署和脚本语言经验。

其他趋势科技服务器深度安全防护系统 9.5 文档

- 趋势科技服务器深度安全防护系统 9.5 安装指南（云）
- 趋势科技服务器深度安全防护系统 9.5 安装指南 (VMware NSX)
- 趋势科技服务器深度安全防护系统 9.5 安装指南 (VMware vShield)
- 趋势科技服务器深度安全防护系统 9.5 用户指南
- 趋势科技服务器深度安全防护系统 9.5 支持的功能和平台

- 趋势科技服务器深度安全防护系统 9.5 支持的 Linux 内核

关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针对物理、虚拟或云服务器提供了高级服务器安全。无需紧急修补即可保护企业应用程序和数据免遭破坏和业务中断。这种全面的集中管理平台可帮助您简化安全操作，同时确保管理合规并加快推进虚拟化和云项目的 ROI。以下紧密集成的模块可轻松扩展此平台，确保物理、虚拟或云服务器以及虚拟桌面的服务器、应用程序及数据安全性。

防护模块

防恶意软件

与 VMware 环境集成以进行无客户端防护，或提供在本地模式下可保护物理服务器和虚拟桌面的客户端。

集成新的 VMware vShield Endpoint API 可为 VMware 虚拟机提供无客户端防恶意软件防护，无需占用客户虚拟机。帮助避免完全系统扫描和特征码更新过程中常见的安全漏洞。另外，还提供基于客户端的防恶意软件，可在本地模式下保护物理服务器、基于 Hyper-V 和 Xen 的服务器、公共云服务器以及虚拟桌面。协调无客户端和基于客户端的服务器规格的保护，提供自适应安全防护，以便在服务器在数据中心和公共云之间移动时保护虚拟服务器。

Web 信誉

加强服务器及虚拟桌面对 Web 威胁的防护。

与趋势科技云安全智能防护网络 Web 信誉功能集成，通过阻止对恶意 URL 的访问来保护用户和应用程序。通过同一虚拟设备提供与无客户端模式下的虚拟环境相同的功能，该虚拟设备还提供了无客户端安全防护技术，以便在不增加占用内存的情况下提高安全性。

防火墙

减少物理和虚拟服务器的攻击面。

使用双向状态防火墙对服务器防火墙策略进行集中式管理。支持虚拟机分区，阻止拒绝服务攻击。针对所有基于 IP 的协议和帧类型，以及端口和 IP 及 MAC 地址的细粒度过滤提供广泛的覆盖范围。

入侵防御

在已知漏洞修复之前，屏蔽漏洞以免遭受无限制的入侵。

帮助实现对已知和零时差攻击的及时防护。使用漏洞规则屏蔽已知漏洞（例如 Microsoft 每月公布的漏洞），以免遭受无限制的入侵。针对 100 多个应用程序（包括数据库、Web、电子邮件和 FTP 服务器）提供现成的漏洞防护。自动提供屏蔽数小时内新发现漏洞的规则，并在几分钟内将此规则推送至数千台服务器，无需重新启动系统。

抵御 Web 应用程序漏洞

确保符合 PCI 要求 6.6，以保护 Web 应用程序及其处理的数据。抵御 SQL 注入攻击、跨站点脚本攻击以及其他 Web 应用程序漏洞。屏蔽漏洞直到代码修复完成。

识别访问网络的恶意软件

加强对访问网络的应用程序的监视或控制。识别访问网络的恶意软件，减少服务器的漏洞入侵。

完整性监控

实时检测并报告对文件和系统注册表的恶意及意外更改。目前无客户端服务器规格中提供。

使管理员能够跟踪对实例进行的授权和未授权更改。检测未授权更改的功能是云安全策略中的关键部分，因为该功能可监视可能指示实例被损坏的更改。

日志审查

显示日志文件中隐藏的重要安全事件。

优化对整个数据中心多个日志条目中隐藏的重要安全事件的识别功能。将可疑事件转发到 SIEM 系统或集中式日志记录服务器，以进行关联、报告及归档。利用并增强开放源代码软件的功能（该软件位于 OSSEC）。

趋势科技服务器深度安全防护系统组件

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以及向强制组件部署防护的基于 Web 的集中式管理控制台：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，可为虚拟机以无客户端的方式提供防恶意软件、Web 信誉服务、防火墙、入侵防御和完整性监控防护。
- **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，可为安装了它的计算机提供防恶意软件、Web 信誉服务、防火墙、入侵防御、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客户端包含**中继模块**。已启用中继的客户端在趋势科技服务器深度安全防护系统组件组成的整个网络中分发软件和安全更新。
- **趋势科技服务器深度安全防护系统通知程序**是一种 Windows 系统托盘应用程序，可在本地计算机上传达有关安全状态和事件的信息，对于趋势科技服务器深度安全防护系统中继，还可以提供有关正从本地计算机分发的安全更新的信息。

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（以下简称“管理中心”）是一个强大的基于 Web 的集中式管理系统，安全管理员可以通过它来创建和管理全面的安全策略，跟踪威胁并记录针对这些威胁所采取的预防处理措施。趋势科技服务器深度安全防护系统管理中心可与数据中心的不同部分（包括 VMware vCenter 和 Microsoft Active Directory）进行集成。为了帮助部署和集成到客户和合作伙伴的环境中，趋势科技服务器深度安全防护系统有公开的 Web 服务 API，允许使用不依赖任何语言的简单方法从外部访问数据和编程配置。

策略

策略是可指定要为一台或多台计算机自动配置和执行的设置和安全规则的模板。这些易于管理的精简规则集可以轻松提供全面安全，而无需费心去管理上千条规则。缺省策略可提供大量常用计算机配置的必要规则。

控制台

使用可定制的、基于 Web 的 UI 可轻松地快速导航至特定信息并对其进行详细分析。它将提供：

- 大范围的系统、事件和计算机报告
- 主要度量的图表，包含趋势
- 详细事件日志
- 保存多个个性化控制台版面配置的功能

内建安全

通过基于角色的访问，多个管理员（或用户，每个管理员或用户均拥有不同的访问权限集和编辑权限）可编辑和监控系统的不同部分，并收到相应的信息。数字签名用于认证系统组件并验证规则的完整性。会话加密可保护在组件之间交换的信息的机密性。

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虚拟设备作为 VMware 虚拟机运行并保护同一 ESXi Server 上的其他虚拟机，且每台虚拟设备均拥有各自的安全策略。

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客户端（以下简称“客户端”）是精巧型的高性能软件组件，安装在计算机上可提供防护。

趋势科技服务器深度安全防护系统客户端包含**中继模块**（缺省情况下关闭）。任何趋势科技服务器深度安全防护系统安装中都必须有至少一个已启用中继的客户端，以便在整个趋势科技服务器深度安全防护系统网络中分发安全更新和软件更新。可以启用多个中继并将它们组织到层次组中，更有效地在整个网络中分发更新。

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，可将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传达给客户端计算机。趋势科技服务器深度安全防护系统客户端开始扫描时，或者阻止恶意软件或阻止访问恶意 Web 页面时，通知程序会显示弹出式用户通知。该通知程序还提供了一个控制台工具，方便用户查看事件和配置是否显示弹出通知。

趋势科技服务器深度安全防护系统 9.5 中的新增功能

VMware vSphere 5.5 支持

- 针对网络虚拟化和软件定义的数据中心 NSX 的安全性
- 支持混合模式部署（NSX 和 vShield）

更加智能的轻量型客户端

- 轻量型安装程序
- 根据安全策略要求有选择地向客户端部署防护模块，使客户端占用空间更小
- 自动支持新的 Linux 内核

趋势科技控制管理中心的增强功能

- 更多带有详细分析功能的控制台 Widget
- 防恶意软件和 Web 信誉服务的综合全面的事件

Linux 支持

- 新的分发版本：CloudLinux、Oracle Unbreakable
- 适用于所有分发版本的按需防恶意软件扫描功能
- 适用于 Red Hat 和 SuSE 的实时防恶意软件功能
- Linux AWS 内核在 Amazon 将它们发布到 EC2 上时定期更新。趋势科技服务器深度安全防护系统会自动分发更新以保持用户处于最新状态。

注意： *有关软件平台支持的趋势科技服务器深度安全防护系统功能的列表，请参阅**《趋势科技服务器深度安全防护系统 9.5 支持的功能和平台》**文档。有关每个平台支持的特定 Linux 内核的列表，请参阅**《趋势科技服务器深度安全防护系统 9.5 支持的 Linux 内核》**的文档。*

安全性和软件更新管理方面的改进

- 改进了安全和软件更新状态的可见性
- 提高了软件更新的可访问性

多租户改进

- 以租户身份登录
- 安全模式使用情况报告

准备

系统要求

趋势科技服务器深度安全防护系统管理中心

- **内存：**8GB，其中包括：
  - 4GB 堆内存
  - 1.5GB JVM 系统开销
  - 2GB 操作系统开销
- **磁盘空间：**1.5GB（建议使用 5GB）
- **操作系统：**
  - Windows Server 2012（64 位）、Windows Server 2012 R2（64 位）
  - Windows Server 2008（64 位）、Windows Server 2008 R2（64 位）
  - Windows 2003 Server SP2（64 位）、Windows 2003 Server R2（64 位）
  - Red Hat Linux 5/6（64 位）
- **数据库：**
  - Oracle 11g、Oracle 11g Express
  - Oracle 10g、Oracle 10g Express
  - Microsoft SQL Server 2014、Microsoft SQL Server 2014 Express
  - Microsoft SQL Server 2012、Microsoft SQL Server 2012 Express
  - Microsoft SQL Server 2008、Microsoft SQL Server 2008 Express
  - Microsoft SQL Server 2008 R2、Microsoft SQL Server 2008 R2 Express
- **Web 浏览器：**Firefox 24+、Internet Explorer 9.x、Internet Explorer 10.x、Internet Explorer 11.x、Chrome 33+、Safari 6+。（启用 Cookie。）
  - **显示器：**采用 256 色或更高时，分辨率为 1024 x 768

趋势科技服务器深度安全防护系统客户端

- **内存：**
  - **具有防恶意软件防护：**512MB
  - **没有防恶意软件防护：**128MB
- **磁盘空间：**
  - **具有防恶意软件防护：**1GB
  - **没有防恶意软件防护：**500MB
  - **启用了中继功能：**8GB
- **Windows：**
  - Windows Server 2012（64 位）、Windows Server 2012 R2（64 位）
  - Windows 8.1（32 位和 64 位）
  - Windows 8（32 位和 64 位）
  - 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 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）
- **启用了中继功能：**所有上述 64 位 Windows 版本

- **Linux：**
  - Red Hat 5（32 位和 64 位）
  - Red Hat 6（32 位和 64 位）
  - Oracle Linux 5（32 位和 64 位）
  - Oracle Linux 6（32 位和 64 位）
  - CentOS 5（32 位和 64 位）
  - CentOS 6（32 位和 64 位）
  - SuSE 10 SP3 和 SP4（32 位和 64 位）
  - SuSE 11 SP1、SP2 和 SP3（32 位和 64 位）
  - CloudLinux 5（32 位和 64 位）
  - CloudLinux 6（32 位和 64 位）
  - Oracle Linux 5（64 位）Unbreakable 内核
  - Oracle Linux 6（64 位）Unbreakable 内核
  - Amazon Red Hat Enterprise 6 EC2（32 位和 64 位）
  - Amazon SuSE 11 EC2（32 位和 64 位）
  - Amazon Ubuntu 12 EC2（32 位和 64 位）
  - Amazon AMI Linux EC2（32 位和 64 位）
  - Ubuntu 10.04 LTS（64 位）
  - Ubuntu 12.04 LTS（64 位）
  - Ubuntu 14.04 LTS（64 位）
  - **启用了中继功能：**所有上述 64 位 Linux 版本

注意： *CentOS 客户端软件包括在 Red Hat 客户端软件包中。要在 CentOS 上安装趋势科技服务器深度安全防护系统客户端，需使用 Red Hat 客户端安装程序。*

注意： *有关软件平台支持的趋势科技服务器深度安全防护系统功能的列表，请参阅**《趋势科技服务器深度安全防护系统 9.5 支持的功能和平台》**文档。有关每个平台支持的特定 Linux 内核的列表，请参阅**《趋势科技服务器深度安全防护系统 9.5 支持的 Linux 内核》**的文档。*

所需条件（基础组件）

趋势科技服务器深度安全防护系统软件包

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一份趋势科技服务器深度安全防护系统管理中心安装包：

http://downloadcenter.trendmicro.com/?regs=CH

注意：	*要手动确认您拥有的每个安装包是否是合法版本，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。*

趋势科技服务器深度安全防护系统客户端：安装趋势科技服务器深度安全防护系统管理中心后，请立即使用它为要保护的平台导入趋势科技服务器深度安全防护系统客户端软件包。

注意：	*任何趋势科技服务器深度安全防护系统安装，无论其是否提供无客户端或基于客户端的防护，都要求安装至少一个已启用中继的客户端，以下载和分发安全和软件更新。任何 64 位 Windows 或 Linux 客户端都可提供中继功能*

要导入趋势科技服务器深度安全防护系统客户端软件，请参阅*安装趋势科技服务器深度安全防护系统客户端 （第 27页）*和*安装和配置已启用中继的客户端（第 34页）*。

还提供有其他“支持”包（如 Linux 内核支持更新）供下载，但是如果您已经下载客户端软件，则这些包将根据需要自动导入趋势科技服务器深度安全防护系统。有关导入客户端软件的说明，请参阅**安装趋势科技服务器深度安全防护系统客户端**。

使用授权（激活码）

如果要完成安装，则防护模块需要趋势科技服务器深度安全防护系统激活码，多租户需要单独的激活码。

（VMware 组件还需要 VMware 使用授权。）

管理员/Root

必须在将安装趋势科技服务器深度安全防护系统软件组件的计算机上拥有管理员/Root 权限。

SMTP 服务器

您将需要 SMTP 服务器发送警报电子邮件。缺省情况下，DSM 使用端口 25 来连接到 SMTP 服务器。

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 数据库服务器端口。
- **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 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。
- **端口 514：**与 Syslog 服务器双向通信（可配置）。
- **端口 443：**与 VMware vCloud、vCenter、vShield/NSX Manager 和 Amazon AWS 通信。

注意： *有关趋势科技服务器深度安全防护系统如何使用每个端口的更多详细信息，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客户端、已启用中继的客户端和设备上

您必须确保运行已启用中继的客户端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：**用于内部通信。不应对外开放。
- **端口 80、443：**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：**与 Syslog 服务器双向通信（可配置）。

趋势科技服务器深度安全防护系统管理中心自动实施特定防火墙规则，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。

网络通信

缺省情况下，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已启用中继的客户端、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，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和已启用中继的客户端的主机名。这可能要求趋势科技服务器深度安全防护系统管理中心和已启用中继的客户端计算机拥有 DNS 项或在客户端/设备计算机的 hosts 文件中存在对应项。

注意： *系统将要求您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提供此主机名。如果没有 DNS，请在安装期间输入 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。

性能建议

请参阅*趋势科技服务器深度安全防护系统管理中心性能特点（第 62页）*。

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（例如更新和“漏洞扫描（推荐设置）”）需要使用较高的 CPU 和较多的内存资源。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。

数据库应该安装在与性能最好的趋势科技服务器深度安全防护系统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。

有关更多信息，请参阅*数据库部署考虑事项（第 17页）*。

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。建议管理中心和数据库之间的连接延迟为 2 毫秒或更低。

高可用性环境

如果使用 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。必须在所有 ESXi 虚拟机监控程序（包括用于恢复操作的 ESXi 虚拟机监控程序）上部署趋势科技服务器深度安全防护系统。在所有虚拟机监控程序上部署趋势科技服务器深度安全防护系统将确保在 HA 恢复操作之后防护仍然有效。

注意：	*如果在使用 VMware 分布式资源计划程序 (DRS) 的 VMware 环境中部署虚拟设备，重要的是在 DRS 进程中该设备不与虚拟机一起 vMotion。必须将虚拟设备“固定”到其特定的 ESXi Server。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 ESXi 服务器的更多信息，请查看 VMware 文档。*

注意：	*如果虚拟机由 DRS 从受 DSVA 保护的 ESXi vMotion 到不受 DSVA 保护的 ESXi，则该虚拟机将不受保护。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**基于事件的任务**部分。*

数据库部署注意事项

有关数据库安装和部署的说明，请参阅数据库提供商的文档，但是在与趋势科技服务器深度安全防护系统集成时，请记住以下注意事项。

版本

对于企业部署，趋势科技服务器深度安全防护系统要求使用 Microsoft SQL Server 2012 或 2008，或者 Oracle Database 11g 或 10g。趋势科技服务器深度安全防护系统管理中心自带一个内置的 Apache Derby 数据库，但该数据库仅适用于评估目的。（您无法从 Apache Derby 升级至 SQL Server 或 Oracle Database。）

在趋势科技服务器深度安全防护系统之前安装

在安装趋势科技服务器深度安全防护系统管理中心*之前*，必须安装数据库软件、为趋势科技服务器深度安全防护系统创建数据库实例（如果您不想使用缺省实例），以及为趋势科技服务器深度安全防护系统创建用户帐户。

位置

数据库必须位于与趋势科技服务器深度安全防护系统管理中心相同的网络上，在 LAN 上的连接速度为 1Gb/s。（不建议使用 WAN 连接。）

专用服务器

应将数据库安装在单独的专用计算机上。

Microsoft SQL Server

- 启用“远程 TCP 连接”。（请参阅 http://msdn.microsoft.com/en-us/library/bb909712(v=vs.90).aspx）
- 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帐户必须具有 db_owner 权限。
- 如果使用多租户，则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帐户必须具有 dbcreator 权限。
- 为数据库选择“简单”恢复模型属性。（请参阅 http://technet.microsoft.com/en-us/library/ms189272.aspx）

Oracle 数据库

- 启动“Oracle 监听器”服务并确保其接受 TCP 连接。
- 必须为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帐户授予 CONNECT 和 RESOURCE 角色，以及 UNLIMITED TABLESPACE、CREATE SEQUENCE、CREATE TABLE 和 CREATE TRIGGER 系统权限。
- 如果使用多租户，则必须为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帐户授予 CREATE USER、DROP USER、ALTER USER、GRANT ANY PRIVILEGE 和 GRANT ANY ROLE 系统权限。

传输协议

建议的传输协议为 TCP。

如果使用**命名管道**连接到 SQL Server，则趋势科技服务器深度安全防护系统管理中心的主机与 SQL Server 主机之间必须存在经适当认证的 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。
- 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。用于 AWS Marketplace 的趋势科技服务器深度安全防护系统管理中心不支持。

趋势科技服务器深度安全防护系统管理中心安装期间使用的连接设置

在趋势科技服务器深度安全防护系统管理中心安装期间，系统将要求您提供数据库连接详细信息。在“主机名”下输入数据库主机名，并在“数据库名称”下输入为趋势科技服务器深度安全防护系统预创建的数据库。

安装支持 SQL 和 Windows 认证。使用 Windows 认证时，单击“高级”按钮以显示其他选项。

避免在数据库用户名中出现特殊字符 (Oracle)

虽然 Oracle 允许在配置数据库用户对象时使用以引号括起来的特殊字符，但趋势科技服务器深度安全防护系统不支持为数据库用户使用特殊字符。

保持数据库名称简短 (SQL Server)

使用多租户时，保持主数据库名称简短可使租户的数据库名称更易于读取。（即，如果主数据库是 "MAINDB"，则第一个租户的数据库名称将是 "MAINDB_1"，第二个租户的数据库名称将是 "MAINDB_2"，依此类推。）

Oracle RAC 支持

趋势科技服务器深度安全防护系统支持：

- SUSE Linux Enterprise Server 11 SP1 和 Oracle RAC 11g R2 (v11.2.0.1.0)
- Red Hat Linux Enterprise Server 5.8 和 Oracle RAC 11g R2 (v11.2.0.1.0)

注意：	*将缺省 Linux 服务器趋势科技服务器深度安全防护系统策略应用于 Oracle RAC 节点时，应该不会造成与 Oracle 自动存储管理 (ASM) 和群集服务的通信问题。但是，如果出现问题，请尝试根据 Oracle RAC 文档中的端口要求定制防火墙设置，或完全禁用防火墙。* *http://docs.oracle.com/cd/E11882_01/install.112/e41962/ports.htm#BABECFJF*

高可用性

只要未对数据库架构进行任何修改，趋势科技服务器深度安全防护系统数据库便会与数据库故障转移保护兼容。例如，某些数据库复制技术会在复制期间向数据库表中添加列，从而导致严重故障。

因此，建议使用数据库镜像，而不要进行数据库复制。

安装

安装趋势科技服务器深度安全防护系统管理中心

准备工作

数据库

在安装趋势科技服务器深度安全防护系统管理中心之前，必须先安装数据库软件，为要使用的趋势科技服务器深度安全防护系统管理中心创建数据库和用户帐户。有关安装数据库的信息，请参阅*数据库部署注意事项（第 17页）*。

已启用共置的中继的客户端

趋势科技服务器深度安全防护系统部署需要至少一个趋势科技服务器深度安全防护系统中继（已启用中继功能的趋势科技服务器深度安全防护系统客户端）。中继会将软件和安全更新分发至客户端/设备，从而保持您的防护功能为最新。趋势科技建议将已启用中继的客户端安装在趋势科技服务器深度安全防护系统管理中心所在的计算机上，以保护主机计算机并充当本地中继。

在安装趋势科技服务器深度安全防护系统管理中心期间，安装程序将在其本地目录中查找客户端安装包（完整的 zip 软件包而非核心客户端安装程序）。如果在本地没有找到安装包，安装程序将尝试通过 Internet 连接至趋势科技下载专区，从中找到客户端安装包。如果在上述任一位置找到安装包，则在安装趋势科技服务器深度安全防护系统管理中心期间您可以选择安装共置的已启用中继的客户端。（如果在两个位置均找到客户端安装包，则将选择两个版本中的最新版本。）客户端可用于保护趋势科技服务器深度安全防护系统管理中心主机，但是，最初仅在已启用中继模块的情况下安装客户端。要启用防护，必须应用适当的安全策略。

如果无可用的客户端安装包，则趋势科技服务器深度安全防护系统管理中心安装过程将不使用它继续进行（但是之后必须安装已启用中继的客户端）。

注意：	*可在之后安装其他已启用中继的客户端，由您的环境决定。（有关安装已启用中继的客户端的说明，请参阅安装趋势科技服务器深度安全防护系统客户端（第 27页）和配置中继（第 34页）。）*

代理服务器信息

如果趋势科技服务器深度安全防护系统将需要使用代理服务器通过 Internet 连接至趋势科技更新服务器，请准备好代理服务器地址、端口和登录凭证。

多节点管理中心

可将 Vulnerability Protection 趋势科技服务器深度安全防护系统管理中心作为使用单个数据库并行工作的多个节点运行。将管理中心作为多节点运行可提供更高的可靠性、冗余可用性、几乎无限的可扩展性以及更好的性能。

每个节点均能执行所有任务，且所有节点的重要性相同。用户可登录任意节点以执行任务。任意一个节点出现故障不会导致任何任务无法执行。任意一个节点出现故障不会导致任何数据丢失。

每个节点必须运行相同版本的管理中心软件。执行管理中心软件升级时，要升级的第一个管理中心将接管所有 Vulnerability Protection 趋势科技服务器深度安全防护系统管理中心职责，并关闭所有其他 Vulnerability Protection 趋势科技服务器深度安全防护系统管理中心节点。它们将在**系统信息**页面的**系统活动**面板中的**带有活动表的网络拓扑图**中显示为“脱机”，并表明需要升级。在其他节点上执行升级后，这些节点会自动返回联机状态，并开始分担 DSM 任务。

要将 Vulnerability Protection 趋势科技服务器深度安全防护系统管理中心节点添加到您的安装，请在新计算机上运行管理中心安装包。出现提示时，键入使用的数据库的位置和登录凭证。当安装程序连接到数据库后，就可以继续将节点添加到系统。

注意：	*必须使用 MS SQL Server 或 Oracle Database 才能运行多个节点。*

注意：	*在任何时候都不应同时运行多个安装程序实例。这样做会导致不可预测的结果，包括数据库损坏。*

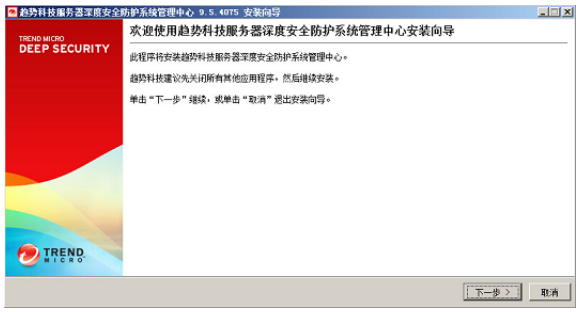
下载安装包

从趋势科技下载专区下载最新版本的趋势科技服务器深度安全防护系统管理中心（也可选择下载趋势科技服务器深度安全防护系统客户端）软件，网址为：

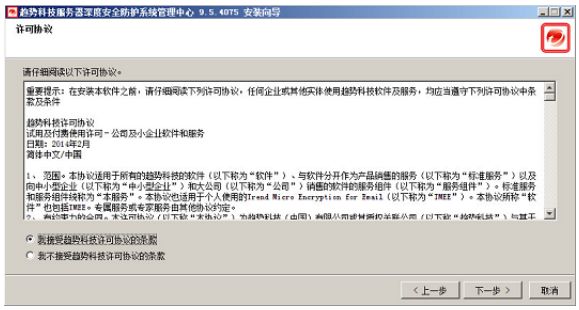
http://downloadcenter.trendmicro.com/?regs=CH

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

1. 将趋势科技服务器深度安全防护系统管理中心安装包复制到目标计算机。通过双击安装包来启动趋势科技服务器深度安全防护系统管理中心安装程序。



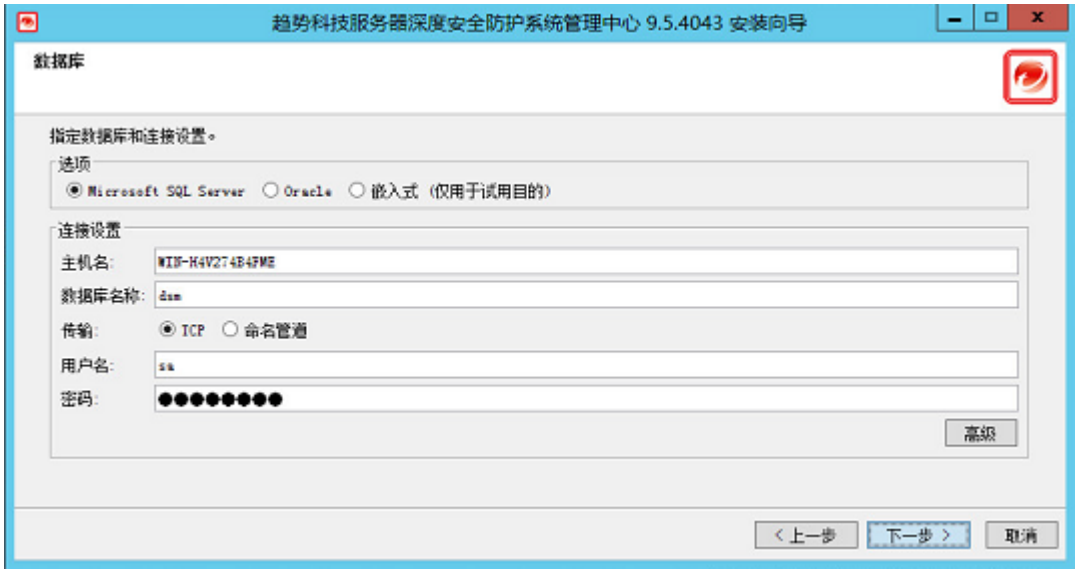
2. **许可协议：**如果您同意许可协议的条款，请选择**我接受趋势科技许可协议的条款**。



3. **安装路径：**选择用于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并单击**下一步**。



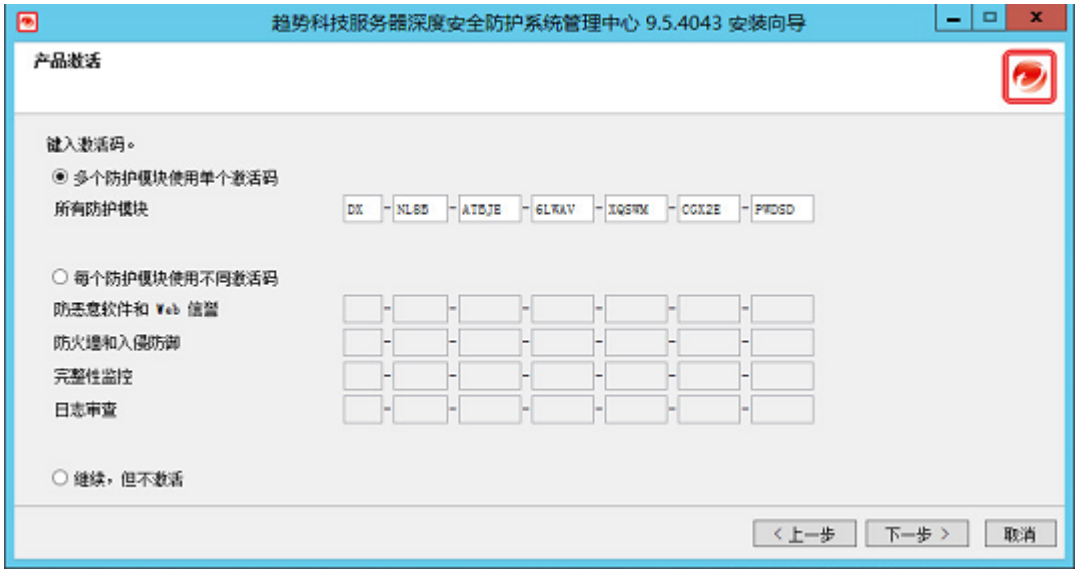
4. **数据库：**选择之前安装的数据库。



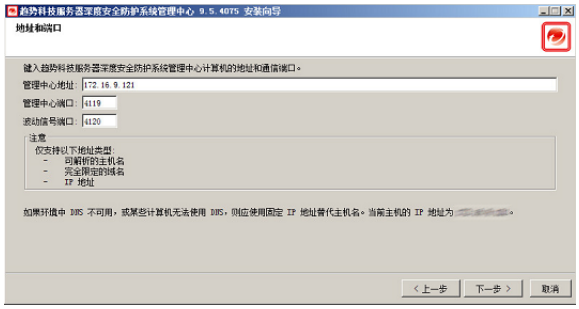
如果数据库为 SQL Server 且正在使用已命名实例，请单击**高级**输入具体信息。



5. **产品激活：**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**管理 > 使用授权**输入首个激活码或添加激活码。）



6. **地址和端口：**输入此计算机的主机名、URL 或 IP 地址。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。

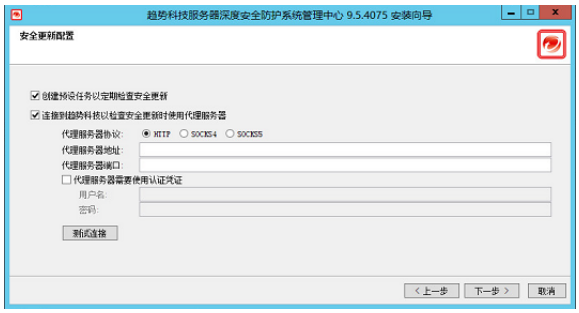


7. **管理员帐户：**输入主管理员帐户的用户名和密码。选中“强制使用强密码”（建议）会要求此管理员及以后创建的管理员的密码包括大写和小写字母、非字母数字字符以及数字，并且要求使用最小字符数。

> *注意：* *如果拥有管理中心主机的 admin 权限，则可以使用 `dsm_c -action unlockout -username USERNAME -newpassword NEWPASSWORD` 命令重置帐户密码。*

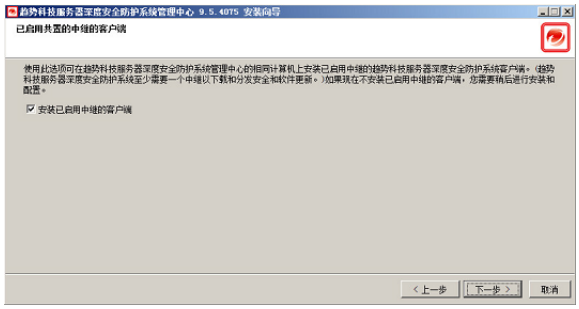


8. **自动更新：**选择**创建预设任务**选项将创建预设任务，自动从趋势科技检索最新的安全和软件更新并将其分发至客户端和设备。（以后可以使用趋势科技服务器深度安全防护系统管理中心配置更新。）如果趋势科技服务器深度安全防护系统管理中心将需要使用代理通过 Internet 连接至趋势科技更新服务器，请选择**连接到趋势科技以检查安全更新时使用代理服务器**并输入代理信息。

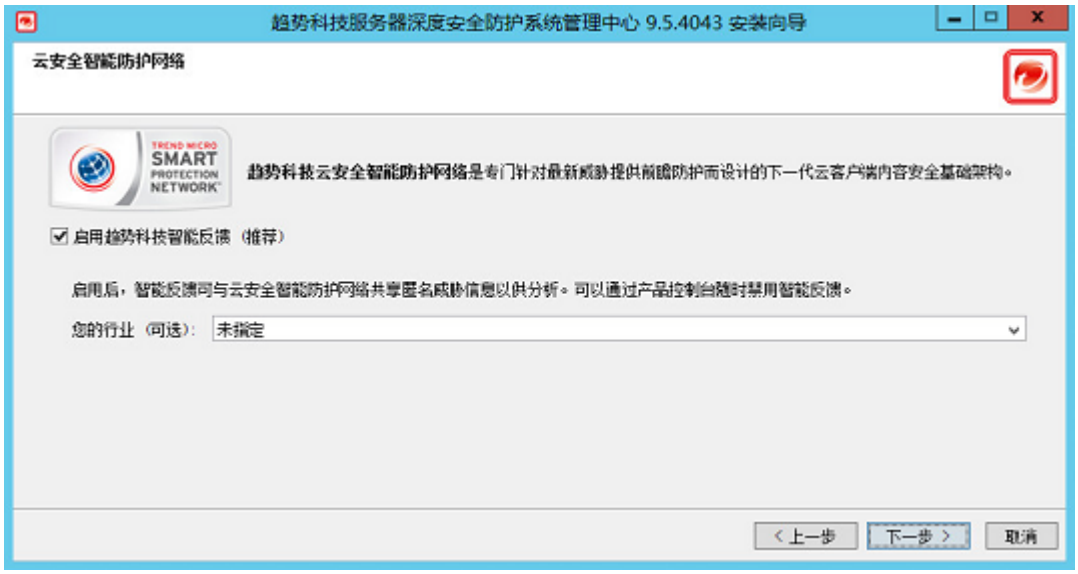


9. **共置的已启用中继的客户端：**如果在本地文件夹或从趋势科技下载专区可以找到客户端安装包，则可以选择安装共置的已启用中继的客户端。任何趋势科技服务器深度安全防护系统安装均至少需要一个中继来下载和分发安全和软件更新。如果现在不安装已启用中继的客户端，则需要稍后进行安装。

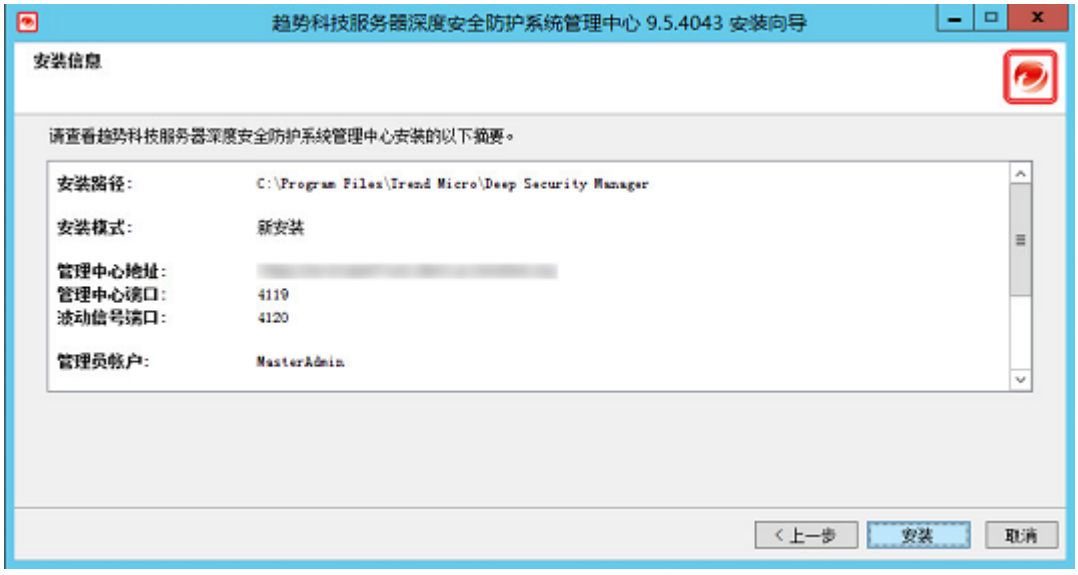
> *注意：* *强烈建议安装共置的已启用中继的客户端。*



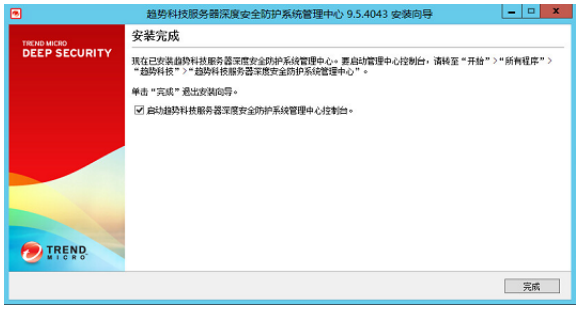
10. **云安全智能防护网络：**选择是否要启用“趋势科技智能反馈（推荐）”。（以后可以使用趋势科技服务器深度安全防护系统管理中心启用或配置智能反馈）。（可选）通过从下拉列表中进行选择来输入行业。



11. **安装信息：**验证输入的信息，然后单击**安装**继续。



12. 选择**启动趋势科技服务器深度安全防护系统管理中心控制台**，以在设置完成后打开 Web 浏览器访问趋势科技服务器深度安全防护系统管理中心 URL。单击**完成**关闭安装向导。



趋势科技服务器深度安全防护系统管理中心服务会在安装完成时启动。 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，应注意此 URL。

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

在带 X Window 系统的 Linux 操作系统上安装趋势科技服务器深度安全防护系统管理中心的步骤顺序与 Windows（以上所述）的步骤相同。有关执行 Linux 静默安装的信息，请参阅*静默安装趋势科技服务器深度安全防护系统管理中心（第 55页）*。

> *注意：* *如果在已启用 iptables 的 Linux 上安装趋势科技服务器深度安全防护系统管理中心，则需要将 iptables 配置为允许通过 TCP 端口 4119 和 4120 通信。*

启动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服务在安装后自动启动。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 (MS Windows) 或 K 菜单 (X Windows) 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。（在安装期间创建的凭证可用于登录并创建其他用户帐户。）

> *注意：* *趋势科技服务器深度安全防护系统管理中心会为与客户端/设备、中继和用户 Web 浏览器的连接创建为期 10 年的自签名证书。但是，对于已添加的安全，可以使用可信证书颁发机构 (CA) 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之后会保留此类证书。）有关使用来自 CA 的证书的信息，请参阅创建 SSL 认证证书（第 64页）。*

手动导入其他趋势科技服务器深度安全防护系统软件

可从趋势科技服务器深度安全防护系统管理中心的**管理** > **更新** > **软件** > **下载专区**页面，导入趋势科技服务器深度安全防护系统客户端及其支持的软件包。其他软件包必须从趋势科技下载专区网站 (http://downloadcenter.trendmicro.com/?regs=CH) 手动导入。

将其他趋势科技服务器深度安全防护系统软件导入趋势科技服务器深度安全防护系统管理中心：

1. 从趋势科技下载专区网站将软件下载至本地目录。
2. 在趋势科技服务器深度安全防护系统管理中心，转至**管理** > **更新** > **软件** > **本地**页面，然后在工具栏中单击**导入...**，以显示**导入软件**向导。

3. 使用**浏览...**选项导航至已下载的软件并选择它。
4. 单击**下一步**然后单击**完成**，退出向导。

软件现已导入趋势科技服务器深度安全防护系统管理中心。

安装趋势科技服务器深度安全防护系统客户端

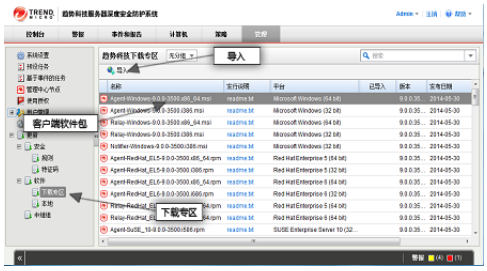
本节介绍如何安装和激活趋势科技服务器深度安全防护系统客户端以及如何启用中继功能（如果需要）。

导入客户端软件

初始安装趋势科技服务器深度安全防护系统客户端时仅包含核心功能。只有在客户端上启用防护模块后，才会下载和安装该模块需要的插件。*因此，必须将客户端软件包导入趋势科技服务器深度安全防护系统管理中心后，才可以在计算机上安装客户端。*（需要将客户端导入趋势科技服务器深度安全防护系统管理中心的第二个原因是，可以使用趋势科技服务器深度安全防护系统管理中心的用户界面轻松地从该软件包中提取客户端安装程序。）

将客户端软件包导入趋势科技服务器深度安全防护系统：

1. 在趋势科技服务器深度安全防护系统管理中心，转至**管理** > **更新** > **软件** > **下载专区**。**下载专区**页面将显示趋势科技提供的所有客户端软件的最新版本。
2. 从列表中选择所需的客户端软件包，然后在菜单栏中单击**导入**。趋势科技服务器深度安全防护系统将开始从趋势科技下载专区将该软件下载至趋势科技服务器深度安全防护系统管理中心。



3. 软件下载完成后，在对应该客户端的**已导入**列中将显示绿色勾选标记。



导出客户端安装程序：

1. 在趋势科技服务器深度安全防护系统管理中心，转至**管理** > **更新** > **软件** > **本地**。
2. 从列表中选择所需的客户端，然后在菜单栏中选择**导出** > **导出安装程序...**。

> *注意：* *如果您拥有适用于同一平台的客户端的较旧版本，则该软件的最新版本将在**为最新**列中有绿色勾选标记。*



3. 将客户端安装程序保存到本地文件夹中。

> *注意：* *仅单独使用已导出的客户端**安装程序**包（.msi 或 .rpm 文件）来安装趋势科技服务器深度安全防护系统客户端。如果提取出完整的客户端 zip 软件包，然后从包含其他压缩的客户端组件的文件夹运行客户端安装程序，则将会安装所有安全模块（但不会打开）。如果您使用核心客户端安装程序，则将从趋势科技服务器深度安全防护系统管理中心下载各个模块并根据需要进行安装，以尽可能降低对本地计算机的影响。*

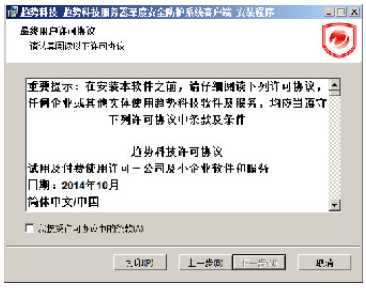
趋势科技服务器深度安全防护系统客户端 "zip" 文件在趋势科技下载专区中提供，供需要手动将客户端导入其趋势科技服务器深度安全防护系统环境的用户下载，因为这些客户的趋势科技服务器深度安全防护系统管理中心留有“间隙”，无法直接连接至下载专区网站。对于其趋势科技服务器深度安全防护系统管理中心可连接至下载专区的用户，强烈建议使用趋势科技服务器深度安全防护系统管理中心界面导入其客户端软件包。如果在相应软件包尚未导入趋势科技服务器深度安全防护系统管理中心的情况下尝试安装客户端，则会导致出现严重问题。

安装 Windows 客户端

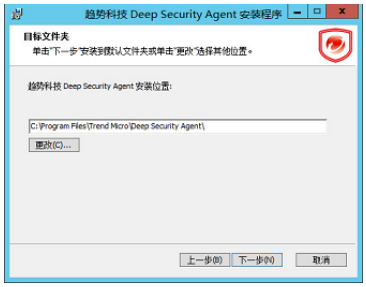
1. 将客户端安装程序文件复制到目标计算机，然后双击安装文件以运行安装包。在“欢迎使用”窗口中，单击**下一步**开始安装。



2. **最终用户许可协议：**如果您同意许可协议的条款，请选择**我接受许可协议的条款**并单击**下一步**。



3. **目标文件夹：**选择要安装趋势科技服务器深度安全防护系统客户端的位置，然后单击**下一步**。



4. **趋势科技服务器深度安全防护系统客户端安装准备就绪：**单击**安装**继续安装。



5. **已完成：**在成功完成安装后，单击**完成**。



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 Red Hat、SuSE 或 Oracle Linux 客户端

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

注意： *必须以 "root" 身份登录才能安装客户端。或者，可以使用 "sudo"。*

1. 将安装文件复制到目标计算机。
2. 使用 "rpm -i" 安装 ds_agent 软件包：

```
# rpm -i <package name>
Preparing...########################################### [100%]
1:ds_agent ########################################### [100%]
Loading ds_filter_im module version ELx.x [ 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）

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。

安装 Ubuntu 客户端

要在 Ubuntu 上安装，请将安装文件复制到目标计算机并使用以下命令：

```
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：

启动客户端：

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

停止客户端：

```
/etc/init.d/ds_agent stop
/etc/init.d/ds_filter stop
```

重置客户端：

```
/etc/init.d/ds_agent reset
```

重新启动客户端：

```
/etc/init.d/ds_agent restart
```

使用部署脚本安装客户端

向趋势科技服务器深度安全防护系统中受保护的资源列表中添加计算机并实施保护需要多个步骤才能完成。大多数这些步骤都可以在计算机上从命令行本地执行，因此也可以编写脚本。趋势科技服务器深度安全防护系统管理中心的部署脚本生成器可通过管理中心的“帮助”菜单访问。

生成部署脚本：

1. 启动部署脚本生成器，方法是从趋势科技服务器深度安全防护系统管理中心的“帮助”菜单（位于趋势科技服务器深度安全防护系统管理中心窗口右上方）单击**部署脚本...**。
2. 选择要将软件部署到的平台。

   注意： *下拉菜单中列出的平台将对应您导入到趋势科技服务器深度安全防护系统管理中心的软件。*

3. 选择**自动激活客户端**。（可选，但是趋势科技服务器深度安全防护系统管理中心必须在实施保护策略前激活客户端。）
4. 选择要在计算机上实施的策略（可选）
5. 选择计算机组（可选）
6. 选择中继组

做出以下选择后，部署脚本生成器将生成脚本，您可以将该脚本导入到您选择的部署工具中。

注意： *部署脚本生成器还可以通过位于**管理** > **更新** > **软件** > **本地**页面中的菜单栏启动。*



注意： *趋势科技服务器深度安全防护系统管理中心为 Windows 客户端生成的部署脚本必须在 Windows Powershell 第 2.0 版或更高版本中运行。您必须以管理员身份运行 Powershell，并且可能需要运行以下命令才能运行脚本：*

Set-ExcecutionPolicy RemoteSigned

注意： *在 Windows 计算机上，部署脚本将使用与本地操作系统相同的代理服务器设置。如果已将本地操作系统配置为使用代理服务器且趋势科技服务器深度安全防护系统管理中心仅可通过直接连接进行访问，则部署脚本将失败。*

Linux 上的 Iptables

linux 上的 Iptables 受支持且仅在 9.5 版本中保持启用状态。如果您的客户端版本较旧，则必须按照以下所述进行操作：

要在不影响 iptables 的情况下运行趋势科技服务器深度安全防护系统客户端，请创建以下空文件：

/etc/use_dsa_with_iptables

如果趋势科技服务器深度安全防护系统客户端检测到存在该文件，则在启动 ds_filter 服务时将不会影响 iptables。

对于 SuSE 11，开始安装过程之前，在目标计算机上执行以下操作：

在

/etc/init.d/jexec

中的

Required-Start:$local_fs

之后添加以下行：

Required-Stop:

激活客户端

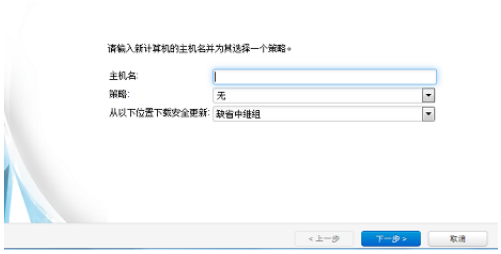
必须在趋势科技服务器深度安全防护系统管理中心激活客户端后，才能将其配置为充当中继或保护主机计算机。

激活新安装的客户端：

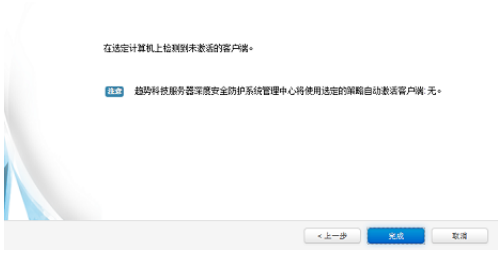
1. 在趋势科技服务器深度安全防护系统管理中心，转至“计算机”页面，然后单击**新建** > **新计算机...**，以显示**新计算机向导**。



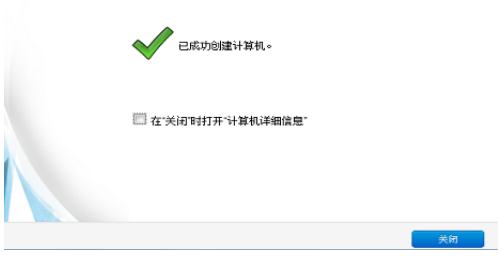
2. 输入计算机的主机名或 IP 地址。如果要使用客户端为主机计算机提供保护以及提供中继功能，请从**策略**菜单选择“趋势科技服务器深度安全防护系统策略”。否则请将**策略**设置保留为“无”。



3. 向导将确认它将在计算机上激活客户端并应用“安全策略”（如果已选择一个）。



4. 在最后的窗口中，取消选择“在“关闭”时打开“计算机详细信息””，然后单击**关闭**。



5. 客户端现已激活。在趋势科技服务器深度安全防护系统管理中心，转至**计算机**窗口并检查计算机状态。该状态应显示为“被管理（联机）”。



启用中继功能

所有激活的 64 位 Windows 或 Linux 客户端均可配置为中继，下载并分发安全和软件更新。

> *注意：* *在客户端上启用中继功能后将无法禁用。*

启用中继功能：

1. 在趋势科技服务器深度安全防护系统管理中心，转至**计算机**页面，双击具有新激活的客户端的计算机，显示其**详细信息**编辑器窗口。
2. 在计算机编辑器中，转至**概述** > **操作** > **软件**区域，然后单击**启用中继**。单击**关闭**关闭编辑器窗口。



3. 在趋势科技服务器深度安全防护系统管理中心的“计算机”页面上，该计算机的图标将从普通计算机 （ ） 变为具有已启用中继的客户端的计算机 （ ）。单击**预览**图标，显示“预览窗格”，可在其中查看中继模块将分发的更新组件的数量。



安装和配置已启用中继的客户端

趋势科技服务器深度安全防护系统中继是已启用中继功能的趋势科技服务器深度安全防护系统客户端。中继会将安全和软件更新下载并分发至您的趋势科技服务器深度安全防护系统客户端和设备。为使您的防护保持最新，必须至少拥有一个趋势科技服务器深度安全防护系统中继。

安装并激活趋势科技服务器深度安全防护系统客户端

如果尚未在计算机上安装客户端，请按照*安装趋势科技服务器深度安全防护系统客户端 (第 27页)*中的说明进行安装。请向前跳至“手动安装”一节。

安装完客户端后，需要将其激活。

激活客户端：

1. 在趋势科技服务器深度安全防护系统管理中心，转至“计算机”页面。
2. 在菜单栏中，单击**新建 > 新计算机...**，显示**新计算机**向导。
3. 对于**主机名**，请输入刚刚在其上安装了客户端的计算机的主机名或 IP 地址。
4. 对于**策略**，请基于计算机的操作系统选择相应的策略。
5. 对于**从以下位置下载安全更新**，请保留缺省设置（缺省中继组）。
6. 单击**完成**。趋势科技服务器深度安全防护系统管理中心会将该计算机导入其“计算机”页面并激活客户端。

在趋势科技服务器深度安全防护系统客户端上启用中继功能

在已安装的趋势科技服务器深度安全防护系统客户端上启用中继功能：

1. 应已通过打开计算机的**编辑器**窗口完成添加新计算机和激活过程。如果该窗口未打开，请按照下面的步骤 2 将其打开。
2. 在趋势科技服务器深度安全防护系统管理中心，转至**计算机**窗口，找到要启用中继功能的客户端，然后进行双击以打开其**计算机编辑器**窗口。
3. 在**计算机编辑器**窗口中，转至**概述 > 操作 > 软件**，然后单击**启用中继**。

> *注意：* *如果未显示**启用中继**按钮，请转至**管理 > 更新 > 软件 > 本地**，检查是否已导入相应软件包。还请确保计算机运行的客户端为 64 位版本。*

趋势科技服务器深度安全防护系统管理中心将安装中继模块所需的插件，之后客户端将开始作为趋势科技服务器深度安全防护系统中继运行。

> *注意：* *如果您正在运行 Windows 防火墙或 iptables，则还需要添加允许在中继的端口 4122 上进行 TCP/IP 通信的防火墙规则。*

> *注意：* *中继会被组织成**中继组**。新的中继会自动分配至**缺省中继组**。“缺省中继组”配置为从趋势科技服务器深度安全防护系统管理中心的 **管理 > 系统设置 > 更新**选项卡上定义的主安全更新源中检索安全和软件更新。（缺省情况下，主更新源是趋势科技的更新服务器，但这是可配置的。）*

数据库部署注意事项

有关数据库安装和部署的说明，请参阅数据库提供商的文档，但是在与趋势科技服务器深度安全防护系统集成时，请记住以下注意事项。

版本

对于企业部署，趋势科技服务器深度安全防护系统要求使用 Microsoft SQL Server 2012 或 2008，或者 Oracle Database 11g 或 10g。趋势科技服务器深度安全防护系统管理中心自带一个内置的 Apache Derby 数据库，但该数据库仅适用于评估目的。（您无法从 Apache Derby 升级至 SQL Server 或 Oracle Database。）

在趋势科技服务器深度安全防护系统之前安装

在安装趋势科技服务器深度安全防护系统管理中心*之前*，必须安装数据库软件、为趋势科技服务器深度安全防护系统创建数据库实例（如果您不想使用缺省实例），以及为趋势科技服务器深度安全防护系统创建用户帐户。

位置

数据库必须位于与趋势科技服务器深度安全防护系统管理中心相同的网络上，在 LAN 上的连接速度为 1Gb/s。（不建议使用 WAN 连接。）

专用服务器

应将数据库安装在单独的专用计算机上。

Microsoft SQL Server

- 启用“远程 TCP 连接”。（请参阅 http://msdn.microsoft.com/en-us/library/bb909712(v=vs.90).aspx）
- 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帐户必须具有 db_owner 权限。
- 如果使用多租户，则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帐户必须具有 dbcreator 权限。
- 为数据库选择“简单”恢复模型属性。（请参阅 http://technet.microsoft.com/en-us/library/ms189272.aspx）

Oracle 数据库

- 启动“Oracle 监听器”服务并确保其接受 TCP 连接。
- 必须为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帐户授予 CONNECT 和 RESOURCE 角色，以及 UNLIMITED TABLESPACE、CREATE SEQUENCE、CREATE TABLE 和 CREATE TRIGGER 系统权限。
- 如果使用多租户，则必须为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帐户授予 CREATE USER、DROP USER、ALTER USER、GRANT ANY PRIVILEGE 和 GRANT ANY ROLE 系统权限。

传输协议

建议的传输协议为 TCP。

如果使用**命名管道**连接到 SQL Server，则趋势科技服务器深度安全防护系统管理中心的主机与 SQL Server 主机之间必须存在经适当认证的 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。
- 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。用于 AWS Marketplace 的趋势科技服务器深度安全防护系统管理中心不支持。

趋势科技服务器深度安全防护系统管理中心安装期间使用的连接设置

在趋势科技服务器深度安全防护系统管理中心安装期间，系统将要求您提供数据库连接详细信息。在“主机名”下输入数据库主机名，并在“数据库名称”下输入为趋势科技服务器深度安全防护系统预创建的数据库。

安装支持 SQL 和 Windows 认证。使用 Windows 认证时，单击“高级”按钮以显示其他选项。

避免在数据库用户名中出现特殊字符 (Oracle)

虽然 Oracle 允许在配置数据库用户对象时使用以引号括起来的特殊字符，但趋势科技服务器深度安全防护系统不支持为数据库用户使用特殊字符。

保持数据库名称简短 (SQL Server)

使用多租户时，保持主数据库名称简短可使租户的数据库名称更易于读取。（即，如果主数据库是 "MAINDB"，则第一个租户的数据库名称将是 "MAINDB_1"，第二个租户的数据库名称将是 "MAINDB_2"，依此类推。）

Oracle RAC 支持

趋势科技服务器深度安全防护系统支持：

- SUSE Linux Enterprise Server 11 SP1 和 Oracle RAC 11g R2 (v11.2.0.1.0)
- Red Hat Linux Enterprise Server 5.8 和 Oracle RAC 11g R2 (v11.2.0.1.0)

注意： *将缺省 Linux 服务器趋势科技服务器深度安全防护系统策略应用于 Oracle RAC 节点时，应该不会造成与 Oracle 自动存储管理 (ASM) 和群集服务的通信问题。但是，如果出现问题，请尝试根据 Oracle RAC 文档中的端口要求定制防火墙设置，或完全禁用防火墙。*

http://docs.oracle.com/cd/E11882_01/install.112/e41962/ports.htm#BABECFJF

高可用性

只要未对数据库架构进行任何修改，趋势科技服务器深度安全防护系统数据库便会与数据库故障转移保护兼容。例如，某些数据库复制技术会在复制期间向数据库表中添加列，从而导致严重故障。

因此，建议使用数据库镜像，而不要进行数据库复制。

快速入门

快速入门：系统配置

本快速入门指南介绍了在可以开始保护计算机资源之前所需的 Vulnerability Protection 趋势科技服务器深度安全防护系统初始基本系统配置。

要完成 Vulnerability Protection 趋势科技服务器深度安全防护系统的基本系统配置，您将需要：

1. 请确保已启用中继的客户端可运行
2. 将 Vulnerability Protection 趋势科技服务器深度安全防护系统配置为从趋势科技检索更新
3. 检查是否有预设任务来定期执行更新
4. 设置重要事件的电子邮件通知

1. 将 Vulnerability Protection 趋势科技服务器深度安全防护系统配置为从趋势科技检索更新
2. 检查是否有预设任务来定期执行更新
3. 设置重要事件的电子邮件通知

请确保已启用中继的客户端可运行

注意： *中继负责从趋势科技检索安全更新并将其分发至受保护的计算机。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，如果未安装共置的已启用中继的客户端，则需要在开始操作前安装已启用中继的客户端。（请参阅安装和配置已启用中继的客户端（第 34页）。）*

启动趋势科技服务器深度安全防护系统管理中心管理控制台，然后导航至**计算机**页面。已启用中继的客户端应显示在**计算机**列表中，由“计算机”图标标识，图标上有中继标记（ ）的。其状态栏应显示“被管理（联机）”。





注意： *Vulnerability Protection 客户端的 Windows 版本具有可以从**计算机编辑器**窗口启用的内置中继功能。*

中继会始终组织成中继组，即使这是唯一的“缺省中继组”，所有新中继也会全部分配到该中继组。如果您拥有大量计算机并要创建分层中继结构，或者如果您的计算机散布在较广的地理区域，则可以创建多个中继组。有关中继组的更多信息，请参阅联机帮助中的**中继组**。

要查看您的 Vulnerability Protection 趋势科技服务器深度安全防护系统中继，请转至**管理** > **更新** > **中继组**。



此时会在**中继组**页面中显示当前中继组。通常，您仅拥有单个**缺省中继组**。

双击缺省中继组以显示其**中继组属性**窗口：



在**中继组属性**窗口的“成员”区域中，您将看到作为组成员的中继。

注意： *如果“成员”区域中没有任何计算机，请参阅《安装指南》中的**配置 Vulnerability Protection 趋势科技服务器深度安全防护系统中继**。*

将 Vulnerability Protection 趋势科技服务器深度安全防护系统配置为从趋势科技检索更新

您确认具有中继之后，可以在“计算机”列表中查找该中继，并检查它是否可以从趋势科技检索更新。

下一步，检查您是否可以从趋势科技检索更新。

转至**管理** > **更新** > **安全**页面，然后单击**特征码更新**下的**检查更新并下载...**按钮。



此时将显示**下载特征码**向导，该向导会联系趋势科技更新服务器，下载最新防恶意软件特征码更新并将更新分发给计算机。（此为缺省操作。可以在**管理** > **系统设置** > **更新**选项卡上配置自动分发安全更新。）如果向导在完成操作后显示成功消息，则表示您的已启用中继的客户端可以与更新服务器进行通信：



检查是否有预设任务来定期执行更新

一旦获知中继可以与更新服务器进行通信，您应创建一个预设任务以定期检索和分发安全更新。

然后，您应创建一个预设任务以定期检索和分发安全更新。

请转至**管理** > **预设任务**。此时，您至少会看到一个称为**缺省检查安全更新任务**的预设任务：



双击该预设任务以查看其**属性**窗口：

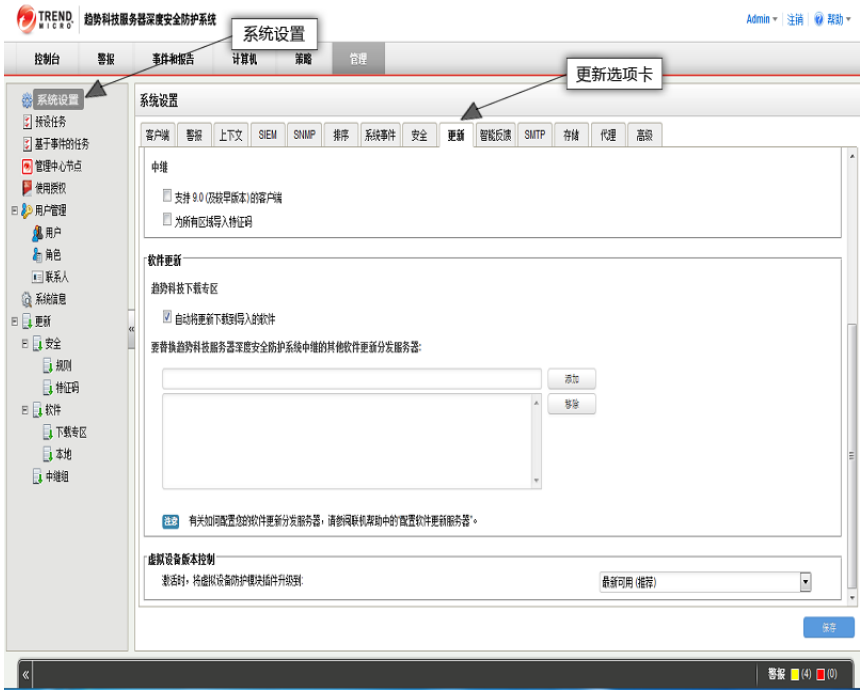


请注意（在此情况下）**每日检查安全更新任务**已被设置为于每日 12:55:00 执行安全更新。

> *注意：* *如果列表中不存在**每日检查安全更新任务**，则可以通过单击“预设任务”页面工具栏上的**新建**并按照**新建预设任务**向导中的说明操作，创建该任务。*

更新系统设置中的配置

要进一步配置更新行为的详细信息，请在趋势科技服务器深度安全防护系统管理中心，转至**管理** > **系统设置**中的**更新**选项卡。



在**安全更新**区域中，您可以配置以下选项（尽管建议采用缺省设置）：

- **主更新源：**此为所有中继组中的中继均会前往的源，以检查是否存在趋势科技服务器深度安全防护系统规则和特征码更新，随后可将它们分发至客户端和虚拟设备。（请仅在支持提供商指示的情况下更改此选项。）
- **特征码：**特征码由防恶意软件模块使用。如果出于某些原因，客户端和虚拟设备无法联系中继或趋势科技服务器深度安全防护系统管理中心，则缺省设置允许它们从主安全更新源（上述）直接下载特征码更新。（例如，由于本地连接问题或者计算机是漫游中的便携式计算机。）
- **规则：**防火墙、入侵防御、日志审查和完整性监控防护模块使用的趋势科技服务器深度安全防护系统规则的更新必须集成到趋势科技服务器深度安全防护系统管理中心级别的策略中，之后才可以将这些规则发送至客户端和虚拟设备。此设置（缺省情况下处于打开状态）会自动将规则更新与趋势科技服务器深度安全防护系统管理中心的策略相集成。

  注意： *在每个安全策略中，如果正在使用的安全策略发生更改，可通过存在的进一步设置（缺省情况下也处于打开状态）自动更新计算机。此设置位于**设置** > **计算机** > **立即发送策略更改**中的“策略/计算机编辑器”（**详细信息**窗口）中。*

- **中继：**“中继”下的两个设置用于确定趋势科技服务器深度安全防护系统是否要导入客户端和设备的较旧 9.0 以及更早版本的更新。从 9.0 开始，安全更新体系结构已发生本质改变，且用于 9.0 和 9.5 的更新的格式不同。请勿下载不使用的较旧客户端的更新，因为会占用不必要的带宽和存储空间。同样，如果客户端或设备在多个区域中运行，则仅下载所有“区域”（取决于语言）的特征码。取消选中此选项将仅分发趋势科技服务器深度安全防护系统管理中心的安装区域设计的软件包。

在**软件更新**区域中，可以配置以下选项（尽管建议采用缺省设置）：

- **趋势科技下载专区：**缺省情况下，趋势科技服务器深度安全防护系统将“自动将更新下载到导入的软件”。趋势科技将定期发布已发布客户端和设备软件的更新版本。设置此选项会自动从趋势科技下载专区（趋势科技下载专区提供的软件可通过**管理** > **更新** > **软件** > **下载专区**页面查看。），将更新下载到已导入趋势科技服务器深度安全防护系统的所有软件（显示在**管理** > **更新** > **软件** > **本地**页面上）。

  注意： *在下载完软件后，必须手动启动软件安装进程。此最后一步无法自动进行。*

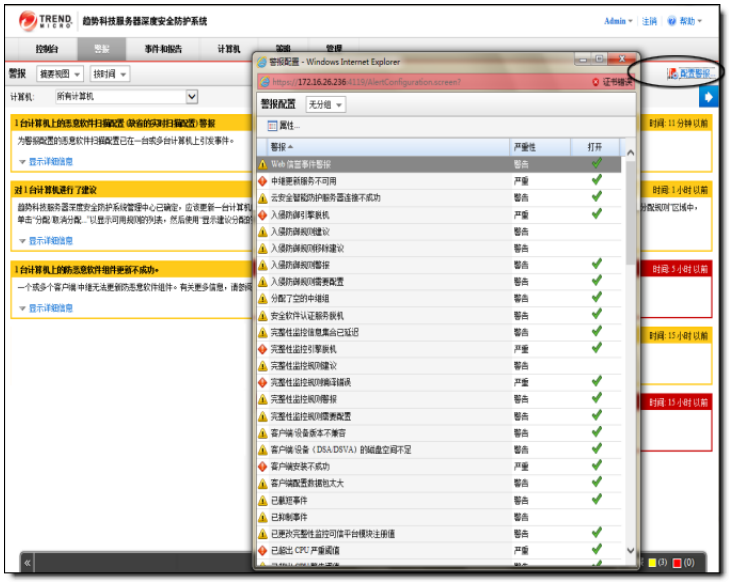
在**虚拟设备版本控制**部分中，可以控制安装在新激活的虚拟设备上的防护模块的版本。趋势科技服务器深度安全防护系统虚拟设备随附有基础版本的防护模块插件。设备依靠随附在 64 位 Red hat 客户端软件包中的插件进行更新。缺省情况下，设备将使用已导入趋势科技服务器深度安全防护系统的 Red Hat 软件包的最新版本（位于**更新** > **软件** > **本地**页面。）但是，如果想控制已安装的防护模块的版本，则可以使用此设置进行控制。

注意： *有关此页面上提供的配置选项的更多信息，请参阅趋势科技服务器深度安全防护系统管理中心与其相关的联机帮助。*

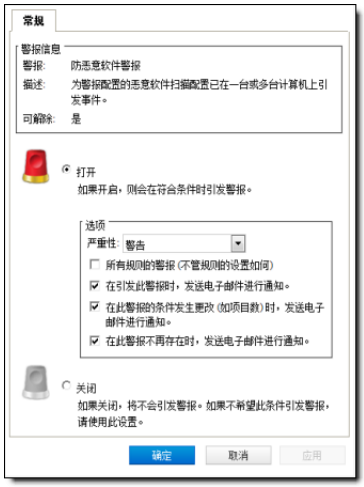
设置重要事件的电子邮件通知

当出现需要特别注意的情况时，会发出 Vulnerability Protection 趋势科技服务器深度安全防护系统警报。发出警报可能是由于安全事件（如在受保护的计算机上检测到恶意软件或异常的重新启动）或系统事件（如 Vulnerability Protection 趋势科技服务器深度安全防护系统管理中心在运行时磁盘空间不足）造成的。Vulnerability Protection 趋势科技服务器深度安全防护系统可以配置为在发出特定警报时发送电子邮件通知。

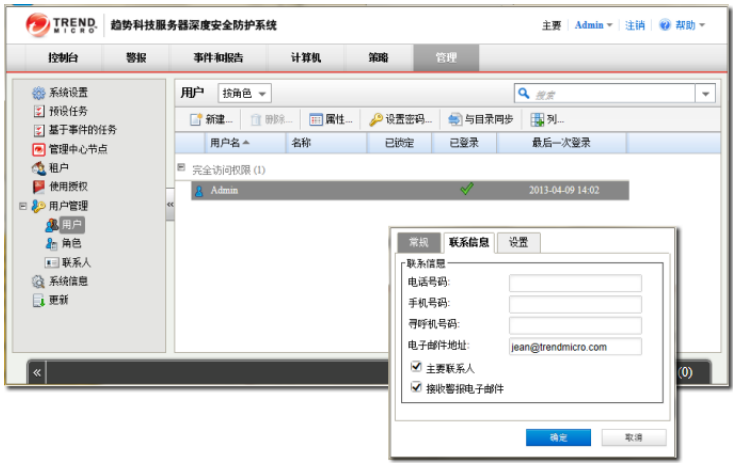
要配置将生成电子邮件通知的警报，请转至**警报**页面，然后单击**配置警报...**以显示 Vulnerability Protection 趋势科技服务器深度安全防护系统警报列表。：



双击警报可查看其**属性**窗口，您可以在该窗口设置电子邮件通知的警报选项。：



现在您需要将用户帐户配置为接收 Vulnerability Protection 趋势科技服务器深度安全防护系统将发出的电子邮件通知。转至**管理 > 用户管理 > 用户**，然后双击用户帐户显示其**属性**窗口。请转至**联系信息**选项卡，输入电子邮件地址，然后选择**接收警报电子邮件**选项。：



为了便于 Vulnerability Protection 趋势科技服务器深度安全防护系统发送电子邮件通知，该防护系统必须能够与 SMTP 服务器进行通信（要发送电子邮件通知，必须能够访问 SMTP 服务器）。要将 Vulnerability Protection 趋势科技服务器深度安全防护系统管理中心连接到 SMTP 服务器，请转至**管理** > **系统设置** > **SMTP** 选项卡。：



填写 **SMTP** 区域中的必填文本框，完成后，按页面底部的“测试 SMTP 设置”，您会看到**测试与 SMTP 服务器的连接成功**消息。：



注意： *如果无法与 SMTP 服务器连接，请确保管理中心可以与端口 25 上的 SMTP 服务器连接。*

基本配置完成

这将完成 Vulnerability Protection 趋势科技服务器深度安全防护系统的基本系统配置。此时，Vulnerability Protection 趋势科技服务器深度安全防护系统会被配置为定期联系趋势科技以获取安全更新并定期分发这些更新，该防护系统将在发出警报时向您发送电子邮件通知。您现在需要将 Vulnerability Protection 趋势科技服务器深度安全防护系统防护应用到计算机。有关保护计算机资源的更多信息，请参阅*快速入门：保护计算机（第 46页）*。

快速入门：保护计算机

下面介绍了如何使用趋势科技服务器深度安全防护系统保护 Windows Server 2008 计算机。

这将涉及以下步骤：

1. 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。
2. 配置和运行“漏洞扫描（推荐设置）”
3. 自动实施“漏洞扫描（推荐设置）”
4. 创建预设任务以定期执行“漏洞扫描（推荐设置）”
5. 使用趋势科技服务器深度安全防护系统管理中心监控活动

注意： *我们将假定您已在计算机上安装了趋势科技服务器深度安全防护系统管理中心，并打算通过该计算机对整个网络的趋势科技服务器深度安全防护系统客户端进行管理。我们还将假定**您已经在希望保护的计算机上安装了（但未激活）趋势科技服务器深度安全防护系统客户端**。最后，我们将假定您具有可用的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可以通过该中继下载最新的安全更新。如果不满足上述任一要求，请参考《安装指南》，了解执行到此阶段的说明。*

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

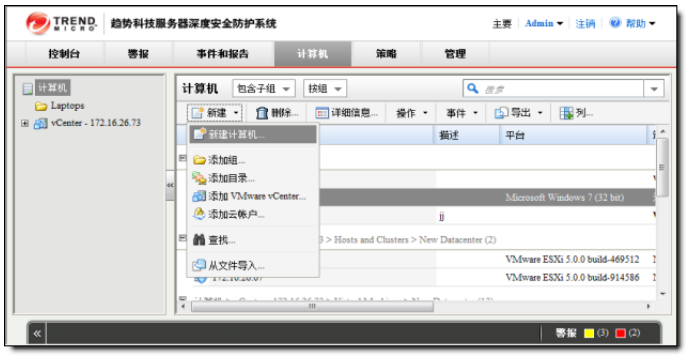
将计算机添加到趋势科技服务器深度安全防护系统管理中心的**计算机**页面的方式有多种。您可以通过以下方式添加计算机：

- 通过指定计算机的 IP 地址或主机名来从本地网络逐个添加计算机
- 通过扫描网络来在本地网络中查找计算机
- 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
- 通过以下云提供程序服务连接到计算资源：
    - Amazon EC2
    - VMware vCloud

出于此练习的目的，我们将从本地网络添加计算机，但一旦将计算机添加到管理中心，防护过程就会相同，而不管计算机位置如何。

从本地网络添加计算机：

1. 在趋势科技服务器深度安全防护系统管理中心控制台中，请转至**计算机**页面，单击工具栏中的**新建**，然后从下拉菜单中选择**新建计算机...**。



2. 在**新建计算机**向导中，输入计算机的主机名或 IP 地址，并从下拉菜单的策略树中选择要应用的相应安全策略。（在此情况下，我们将选择 Windows Server 2008 策略。）单击**下一步**。



3. 该向导将联系计算机，将其添加到“计算机”页面，检测未激活的客户端，将其激活，然后应用所选策略。单击**完成**。



> *注意：　可以将客户端配置为在安装后自动启动自身的激活。有关详细信息，请参阅联机帮助“参考”一节中的**命令行工具**。*

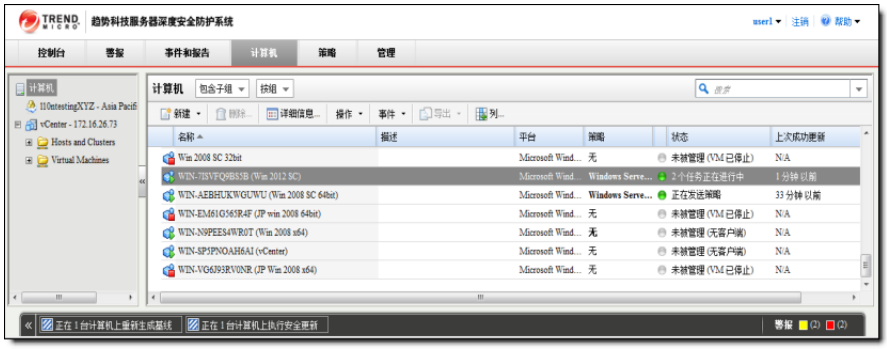
4. 添加计算机后，该向导会显示一条确认消息：



5. 取消选择**在“关闭”时打开“计算机详细信息”**选项，然后单击**关闭**。

此时，计算机会显示在**计算机**页面上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。

激活后，趋势科技服务器深度安全防护系统会自动将最新的安全更新下载到计算机。同样，已向计算机分配的 Windows Server 2008 策略会启用完整性监控，以便可以开始生成计算机的完整性监控基线。您可以在管理中心窗口的状态栏中看到当前正在进行的活动：



趋势科技服务器深度安全防护系统管理中心完成其初始的激活后任务之后，计算机的**状态**应显示为**被管理（联机）**。

注意： *单击菜单栏中的**帮助**按钮可获取更多有关趋势科技服务器深度安全防护系统管理中心各页面的信息。*

配置和运行“漏洞扫描（推荐设置）”

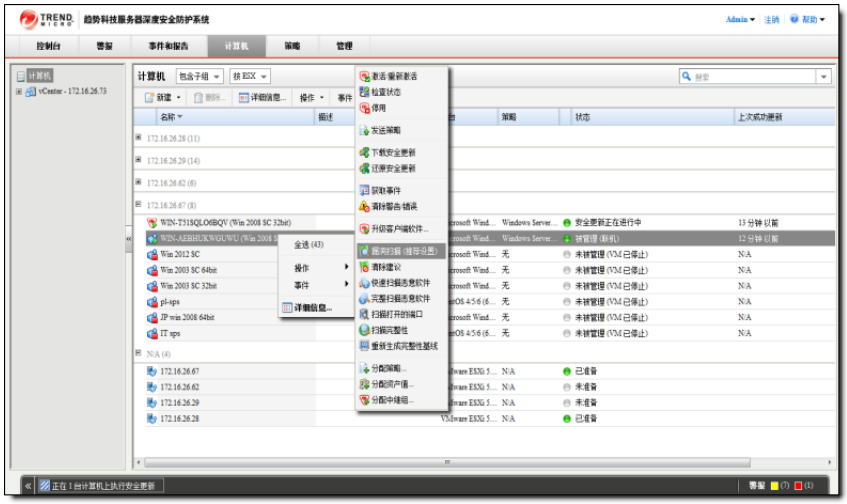
我们向计算机分配的安全策略由专用于运行 Windows Server 2008 操作系统的计算机的一组规则和设置组成。但是，静态策略可能会很快过期。这可能是因为计算机上安装了新软件，查找到了新的操作系统漏洞（趋势科技已针对这些漏洞创建了新的防护规则），或者甚至是因为先前的漏洞已由某个操作系统或软件 Service Pack 更正。由于对计算机的安全要求具有动态性，因此您应定期运行“漏洞扫描（推荐设置）”，这些扫描会评估计算机的当前状态并将该状态与最新趋势科技服务器深度安全防护系统防护模块更新进行比较，以查看是否需要更新当前安全策略。

“漏洞扫描（推荐设置）”会针对以下防护模块提出建议：

- **入侵防御**
- **完整性监控**
- **日志审查**

在计算机上运行“漏洞扫描（推荐设置）”：

1. 转至趋势科技服务器深度安全防护系统管理中心控制台主窗口中的“计算机”页面。
2. 右键单击计算机并选择**操作 > 漏洞扫描（推荐设置）**：



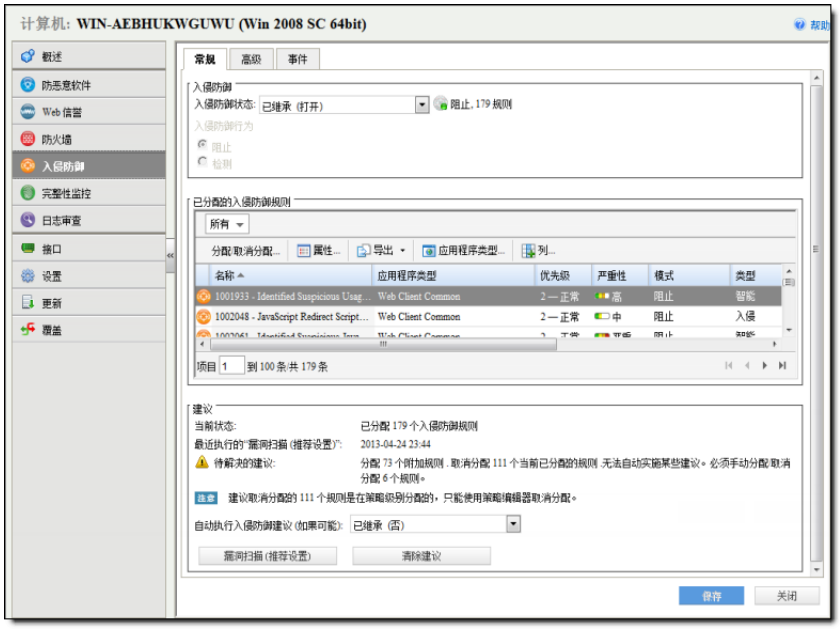
在“漏洞扫描（推荐设置）”期间，计算机的状态会显示**正在执行“漏洞扫描（推荐设置）”**。扫描完成后，如果趋势科技服务器深度安全防护系统提出了任何建议，您会在“警报”窗口上看到一个警报：



查看“漏洞扫描（推荐设置）”的结果：

1. 打开计算机的计算机编辑器（**计算机**页面菜单栏或右键单击菜单中的**详细信息...**）。
2. 在计算机编辑器窗口中，请转至**入侵防御**模块页面。

在**常规**选项卡的**建议**区域，您将看到扫描结果：



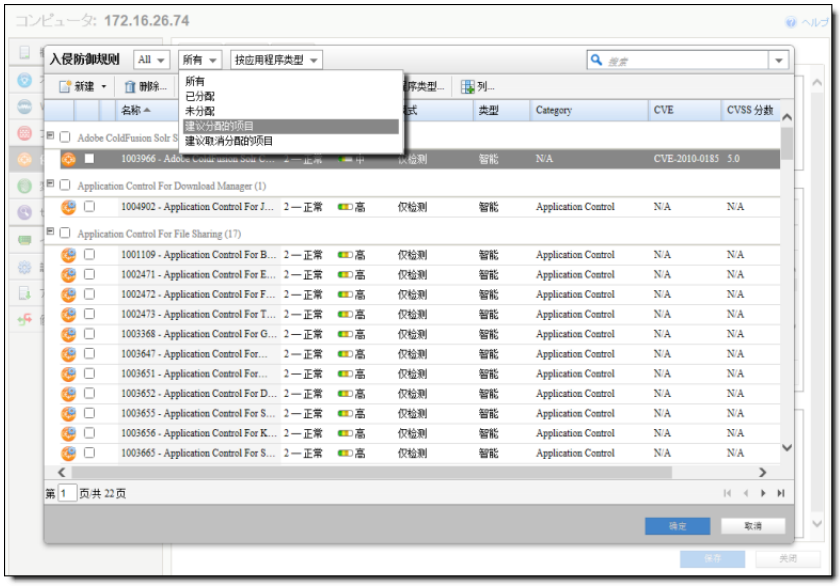
当前状态告知我们当前已向此计算机分配了 179 个入侵防御规则。

最近执行的“漏洞扫描（推荐设置）”告知我们上次扫描于 2012 年 12 月 18 日 09:14 执行。

待解决的建议告知我们由于扫描的原因，趋势科技服务器深度安全防护系统建议另外再分配 28 个入侵防御规则并取消分配 111 个当前已分配的规则。

注意通知我们建议取消分配的规则中有 111 个（所有建议取消分配规则）已在策略级别（而不是直接在此处的计算机级别）进行分配。在策略树以上级别分配的规则仅可以在对其进行分配所在的策略（本案例中为 Windows Server 2008 策略）中取消分配。（如果我们打开了 **Windows Server 2008** 策略编辑器，则我们会看到相同的建议且会从此处对规则进行取消分配。）

我们还被告知建议分配的规则中有 7 个无法自动分配。通常这些规则需要进行配置或易于误报，且其行为应该在仅检测模式下观察并在阻止模式下强制执行。要查看建议分配的规则，请单击**分配/取消分配...**以显示 IPS 规则规则分配模式窗口。然后从第二个下拉过滤列表中选择“建议分配的项目”：



带有小型配置标记的图标 （） 可标识需要进行配置的规则。要查看规则的可配置选项，请双击规则，以打开其**属性**窗口（在本地编辑模式下），然后转至**配置**选项卡。要分配规则，请选择其名称旁边的复选框。

要查看建议取消分配的规则，请通过从同一下拉列表中选择**建议取消分配的项目**来过滤规则列表。要取消分配规则，请取消选择其名称旁边的复选框。

> *注意：* *在计算机上生效的规则无法在本地取消分配，因为它们已在策略树以上的策略中进行分配。取消分配此类规则的唯一方法是编辑最初对其进行分配所在的策略，然后从该策略进行取消分配。有关此类型规则继承的详细信息，请参阅联机帮助“参考”一节中的**策略、继承和覆盖**。*

自动实施“漏洞扫描（推荐设置）”

您可以将趋势科技服务器深度安全防护系统配置为在执行“漏洞扫描（推荐设置）”之后自动分配和取消分配规则。要执行此操作，请打开计算机或策略编辑器，然后转至支持“漏洞扫描（推荐设置）”的各个防护模块页面（入侵、防御、完整性监控和日志审查）。在“常规”选项卡的“建议”区域，将**自动实施入侵防御建议（如果可能）：**设置为“是”。

创建预设任务以定期执行“漏洞扫描（推荐设置）”

定期执行“漏洞扫描（推荐设置）”可确保计算机受最新相关规则集的保护且会移除不再需要的规则集。您可以创建预设任务以自动执行此任务。

创建预设任务：

1. 在趋势科技服务器深度安全防护系统管理中心主窗口中，请转至**管理 > 预设任务**
2. 在菜单栏中，请单击**新建**以显示**新建预设任务**向导。



3. 选择**扫描计算机上有无建议项目**作为扫描类型，然后选择**每周**重复周期。单击**下一步**。
4. 选择开始时间，选择每周一次，然后选择一周中的某一天。单击**下一步**。
5. 当指定要扫描的计算机时，选择最后一个选项（**计算机**），然后选择我们正在保护的 Windows Server 2008 计算机。单击**下一步**。
6. 为新建预设任务键入名称。取消选中**“完成”时运行任务**（因为我们仅运行了“漏洞扫描（推荐设置）”）。单击**完成**。

此时，新建预设任务会显示在预设任务列表中。该任务将一周运行一次，以扫描计算机并为计算机提出建议。如果已为支持该任务的上述每个防护模块设置**自动实施建议**，则趋势科技服务器深度安全防护系统会根据需要分配和取消分配规则。如果规则标识为需要特别注意，则会发出一条警报通知您。

定期预设安全更新

如果您按照*快速入门：系统配置（第 38页）*中介绍的步骤执行操作，则此时会使用趋势科技的最新防护定期更新计算机。

使用趋势科技服务器深度安全防护系统管理中心监控活动

控制台

在为计算机分配了策略并且运行一段时间后，您将会查看该计算机上的活动。检查活动的第一站是控制台。控制台有许多信息面板（"widget"），可显示与趋势科技服务器深度安全防护系统管理中心及其管理的计算机的状态有关的不同信息类型。

在“控制台”页面的右上方，单击**添加/移除 Widget**，查看显示的可用 widget 列表。

目前，我们将从**防火墙**部分添加以下 widget：

- 防火墙活动（已阻止）
- 防火墙 IP 活动（已阻止）
- 防火墙事件历史记录 [2x1]

选择三个 widget 旁边的每个复选框，然后单击**确定**。这些 widget 将显示在控制台上。（生成数据可能需要一段时间。）

- **防火墙活动（已阻止）** widget 可显示拒绝数据包（即某计算机上的客户端阻止数据包到达该计算机）最常见原因的列表，以及被拒绝的数据包的数目。列表中的项将为“数据包拒绝”或“防火墙规则”类型。每个“原因”都是到受拒绝数据包相应日志的链接。
- **防火墙 IP 活动（已阻止）** widget 可显示受拒绝数据包最常见源 IP 的列表。与**防火墙活动（已阻止）** widget 相似，每个源 IP 都是指向相应日志的链接。

- **防火墙事件历史记录** [2x1] widget 可显示一个条形图，表示过去 24 小时内或七天内（取决于所选择的视图）所阻止的数据包数。单击某个条块将显示该条块表示时间段的相应日志。

注意： *请注意**防火墙活动（已阻止）** 和**防火墙 IP 活动（已阻止）** widget 中数值旁边的趋势指示器。正三角或倒三角表示指定时间段内是增加还是减少，水平线表示没有明显变化。*

防火墙和入侵防御事件日志

现在下钻到拒绝数据包最常见原因对应的日志：在**防火墙活动（已阻止）** widget 中，单击拒绝数据包的首个原因。这会将您带到**防火墙事件**页面。

防火墙事件页面将显示所有的防火墙事件，其中**原因**列条目对应于**防火墙活动（已阻止）** widget 中的首个原因（“不允许的策略”）。日志经过过滤，可只显示控制台查看时间段（过去 24 小时或过去七天）的那些事件。关于**防火墙事件**和**入侵防御事件**页面的更多信息，可在这些页面的帮助页面中找到。

注意： *有关不同数据包拒绝原因的含义，请参阅联机帮助“参考”一节中的**防火墙事件**和**入侵防御事件**。*

报告

用户通常期望更高级别的日志数据视图，其中信息得到了汇总，并且以更为浅显易懂的格式呈现。**报告**填补了这一角色，它允许您显示计算机、防火墙和入侵防御事件日志、事件、警报等的详细摘要信息。在**报告**页面中，可以为要生成的报告选择各种选项。

我们将生成一个**防火墙报告**，它将显示在可配置日期范围内防火墙规则和防火墙状态配置活动的记录。从“报告”下拉菜单中选择**防火墙报告**。单击**生成**以在新窗口中启动报告。

通过查看趋势科技服务器深度安全防护系统管理中心以电子邮件形式发送给用户的预设报告、登录到系统并咨询控制台、对特定日志进行仔细分析来执行详细的调查，以及通过配置通知用户关键事件的警报，您可以随时了解网络的运行状况。

附录

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：

1. 转至安装程序所在的目录。
2. 创建一个名为 "Manager-Windows-9.5.xxxx.x64.vmoptions" 或 "Manager-Linux-9.5.xxxx.x64.vmoptions" 的新文本文件，具体取决于您的安装平台（其中，"xxxx" 是安装程序的 Build 号）。
3. 通过添加以下行来编辑该文件："-Xmx800m"（在本示例中，安装程序将使用 800MB 内存。）
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堆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：

1. 转至趋势科技服务器深度安全防护系统管理中心安装目录（与趋势科技服务器深度安全防护系统管理中心可执行文件相同的目录）。
2. 创建一个新文件。为其指定以下名称，具体取决于平台：
   - **Windows**: "Deep Security Manager.vmoptions".
   - **Linux**:"dsm_s.vmoptions".
3. 通过添加以下行来编辑该文件：" **-Xmx10g** "（在本示例中，"10g" 将为趋势科技服务器深度安全防护系统管理中心分配 10GB 可用内存。）
4. 保存文件并重新启动趋势科技服务器深度安全防护系统管理中心。
5. 可通过转至**管理 > 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”值现在应显示新的配置设置。

趋势科技服务器深度安全防护系统管理中心静默安装

Windows

在 Windows 上启动静默安装：

```
Manager-Windows-<Version>.x64.exe -q -console -Dinstall4j.language=<ISO code> -varfile <PropertiesFile>
```

Linux

在 Linux 上启动静默安装：

```
Manager-Linux-<Version>.x64.sh -q -console -Dinstall4j.language=<ISO code> -varfile <PropertiesFile>
```

参数

"-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)。

如果有其他语言可用，利用 -Dinstall4j.language=<ISO code> 选项可以覆盖缺省安装语言（英文）。请使用标准 ISO 语言标识符指定语言：

- 日语：ja
- 简体中文：zh_CN

<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
```

有关可用设置的完整描述，请参阅*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（第 57页）*。

属性文件示例

以下是典型属性文件内容的示例：

```
AddressAndPortsScreen.ManagerAddress=10.201.111.91
AddressAndPortsScreen.NewNode=True
UpgradeVerificationScreen.Overwrite=False
LicenseScreen.License.-1=XY-ABCD-ABCDE-ABCDE-ABCDE-ABCDE-ABCDE
DatabaseScreen.DatabaseType=Oracle
DatabaseScreen.Hostname=10.201.xxx.xxx
DatabaseScreen.Transport=TCP
DatabaseScreen.DatabaseName=XE
```

```
DatabaseScreen.Username=DSM
DatabaseScreen.Password=xxxxxxx
AddressAndPortsScreen.ManagerPort=4119
AddressAndPortsScreen.HeartbeatPort=4120
CredentialsScreen.Administrator.Username=masteradmin
CredentialsScreen.Administrator.Password=xxxxxxxx
CredentialsScreen.UseStrongPasswords=False
SecurityUpdateScreen.UpdateComponents=True
SecurityUpdateScreen.UpdateSoftware=True
RelayScreen.Install=True
SmartProtectionNetworkScreen.EnableFeedback=False
```

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，该文件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（静默安装）中使用。（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（第 55页）*。）

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>
```

设置属性文件具有所需值和可选值。

> *注意：* *对于可选条目，提供无效值将导致使用缺省值。*

所需设置

LicenseScreen

属性	可能值	缺省值	注意
LicenseScreen.License.-1=<value>	<用于所有模块的 AC>	空白	

或

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

CredentialsScreen

属性	可能值	缺省值	注意
CredentialsScreen.Administrator.Username=<value>	<主管理员的用户名>	空白	
CredentialsScreen.Administrator.Password=<value>	<主管理员的密码>	空白	

可选设置

LanguageScreen

属性	可能值	缺省值	注意
sys.languageId=<value>	en_US ja zh_CN	en_US	

UpgradeVerificationScreen

注意：　除非检测到现有的安装，否则不会引用此窗口/设置。

属性	可能值	缺省值	注意
UpgradeVerificationScreen.Overwrite=<value>	True False	False	

注意：　将此值设置为 True 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	可能值	缺省值	注意
DatabaseScreen.DatabaseType=<value>	嵌入式 Microsoft SQL Server Oracle	Microsoft SQL Server	
DatabaseScreen.Hostname=<value>	数据库主机的名称或 IP 地址 当前的主机名	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 TCP	命名管道	仅对 SQL Server 是必需的
DatabaseScreen.Username=<value>			嵌入式不需要
DatabaseScreen.Password=<value>		空白	嵌入式不需要
DatabaseScreen.SQLServer.Instance=<value>			空白表示缺省实例。可选，仅对 SQL Server 是必需的
DatabaseScreen.SQLServer.Domain=<value>			可选，仅对 SQL Server 是必需的
DatabaseScreen.SQLServer.UseDefaultCollation=<value>	True False	False	可选，仅对 SQL Server 是必需的

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	可能值	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	
AddressAndPortsScreen.NewNode=<value>	True False	False	True 表示当前安装为新节点。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。）注意：有关现有数据库的“新节点”安装信息通过 DatabaseScreen 属性提供。

CredentialsScreen

属性	可能值	缺省值	注意
CredentialsScreen.UseStrongPasswords=<value>	true False	False	True 表示 DSM 应该设置为强制使用强密码

SecurityUpdateScreen

属性	可能值	缺省值	注意
SecurityUpdateScreen.UpdateComponents=<value>	True False	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
SecurityUpdateScreen.UpdateSoftware=<value>	True False	True	True 表示您希望设置一个任务以自动检查新软件。

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	可能值	缺省值	注意
SmartProtectionNetworkScreen.EnableFeedback=<value>	True False	False	True 表示启用趋势科技智能反馈。
SmartProtectionNetworkScreen.IndustryType=<value>	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 运输 公用事业 其他	空白	空白对应于“未指定”

属性文件示例

以下是典型属性文件内容的示例：

```
AddressAndPortsScreen.ManagerAddress=10.201.111.91
AddressAndPortsScreen.NewNode=True
UpgradeVerificationScreen.Overwrite=False
LicenseScreen.License.-1=XY-ABCD-ABCDE-ABCDE-ABCDE-ABCDE-ABCDE
DatabaseScreen.DatabaseType=Oracle
DatabaseScreen.Hostname=10.201.xxx.xxx
DatabaseScreen.Transport=TCP
```

```
DatabaseScreen.DatabaseName=XE
DatabaseScreen.Username=DSM
DatabaseScreen.Password=xxxxxxx
AddressAndPortsScreen.ManagerPort=4119
AddressAndPortsScreen.HeartbeatPort=4120
CredentialsScreen.Administrator.Username=masteradmin
CredentialsScreen.Administrator.Password=xxxxxxxx
CredentialsScreen.UseStrongPasswords=False
SecurityUpdateScreen.UpdateComponents=True
SecurityUpdateScreen.UpdateSoftware=True
RelayScreen.Install=True
SmartProtectionNetworkScreen.EnableFeedback=False
```

安装输出

以下是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性能特点

性能配置文件

趋势科技服务器深度安全防护系统管理中心使用一种经过优化的并发作业计划程序，该程序考虑了每个作业对 CPU、数据库和客户端/设备的影响。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。如果趋势科技服务器深度安全防护系统管理中心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。可通过浏览到**管理 > 管理中心节点**来更改性能配置文件。从此窗口中，选择一个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**配置和管理**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。

无客户端防护

扫描缓存

扫描缓存改善了虚拟设备执行的按需扫描的效率。它消除了在大型 VMware 部署中对多个 VM 之间的相同内容所进行的不必要扫描。

此外，

- 完整性监控扫描缓存通过共享完整性监控扫描结果加快完整性监控扫描
- 防恶意软件按需缓存加快了后续克隆/类似 VM 上的扫描
- 防恶意软件实时缓存缩短了 VM 引导和应用程序访问时间
- 并发扫描功能允许同时对多个 VM 执行扫描，从而进一步缩短整体扫描时间

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 ESXi 虚拟机监控程序都必须同其 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，它们必须为“已准备”状态，并且必须在每个 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。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：	*如果在使用 VMware 分布式资源计划程序 (DRS) 的 VMware 环境中部署虚拟设备，重要的是在 DRS 进程中该设备不与虚拟机一起 vMotion。必须将虚拟设备“固定”到其特定的 ESXi Server。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 vMotion。）有关 DRS 以及将虚拟机绑定到特定 ESXi Server 的更多信息，请查看 VMware 文档。*

注意：	*如果虚拟机由 HA 从受 DSVA 保护的 ESXi vMotion 到不受 DSVA 保护的 ESXi，则该虚拟机将不受保护。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，请参阅趋势科技服务器深度安全防护系统管理中心帮助中的“基于事件的任务”。*

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会为与客户端/设备、中继和用户 Web 浏览器的连接创建为期 10 年的自签名证书。但是，对于已添加的安全，可以使用可信证书颁发机构 (CA) 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之后会保留此类证书。）

生成后，CA 证书必须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，趋势科技服务器深度安全防护系统管理中心将使用该证书。

创建 SSL 认证证书：

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（就这些说明而言，我们假设该目录为 "C:\Program Files\Trend Micro\Deep Security Manager"），然后创建名为 Backupkeystore 的新文件夹
2. 将 .keystore 和 configuration.properties 复制到新创建的文件夹 Backupkeystore
3. 从命令提示符转到以下位置：C:\Program Files\Trend Micro\Deep Security Manager\jre\bin
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=dsmserver
   ```

5. 选择密码：changeit

   > *注意：* *注意：-dname 是 CA 将签发的证书的常用名。某些 CA 要求使用特定名称来对证书签名请求 (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。*

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
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
   ```

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
   ```

9. 将 certrequest.csr 发送给 CA 以进行签名。将返回两个文件。一个是“证书回复”，另一个是 CA 证书本身。
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"
    ```

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”）

12. 运行以下命令将证书回复导入您的密钥库：

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

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
```

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\

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$85ef650a5c40bb0f914993ac1ad855f48216fd0664ed2544bbec6de80160b2f
installed=true
serviceName= Trend Micro Deep Security Manager
```

16. 替换以下字符串中的密码：

```
keystorePass=xxxx
```

其中"xxxx" 是在步骤 5 中提供的密码

17. 保存并关闭该文件
18. 重新启动 Deep Security Manager 服务
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。