趋势科技

Deep Security 9.0
产品安装标准程序（SOP）

趋势科技技术支持部

路亦民

2013 年 6 月

Contents

企业为了与合作伙伴、员工、供货商或客户有更实时的连接，有越来越多的在线数据中心，而这些应用正面临着日益增加的网络攻击。与传统的威胁相比，这些针对目标性攻击的威胁数量更多也更复杂，所以对于数据安全的遵循就变得更加严格。而您的公司则更坚固的安全防护，让您的虚拟和实体数据中心，以及云端运算不会因信息威胁而造成性能的降低。

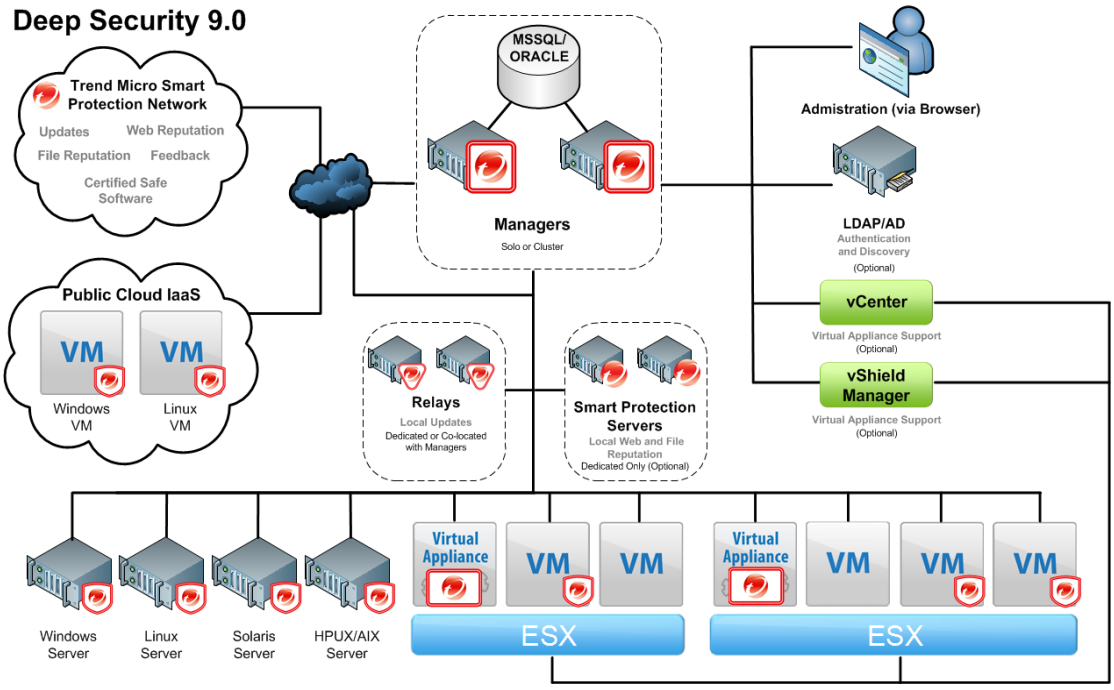
虚拟化能够帮助用户显著地节省数据中心运营成本，用户减少硬件成本和能源需求并且可以在部署关键应用方面获得更大的灵活性和可用性。在虚拟化中，IT人员所面对的最大挑战是应用安全机制，即如何能使用户充分利用其在虚拟化方面的投资。这包括如何使用户能够在相同的物理服务器上将虚拟机设置成不同的安全等级，在使用诸如vMotion机制的同时提供持续的防护，当虚拟机在休眠或离线状态下仍能对其进行防护，并且使用户能够扩展其虚拟化环境以充分利用云计算技术。

Trend Micro Deep Security是一种在虚拟、云计算和传统的数据中心环境之间统一安全性的服务器和应用程序防护软件。它帮助组织预防针对操作系统和应用程序漏洞的非法入侵，监控系统的完整性，并集中管理风险日志，符合包括 PCI 在内的关键法规和标准，并有助于降低运营成本。

趋势科技Deep Security不但可以对物理服务器上的操作系统、应用程序和数据进行防护，同时利用VMware vShield技术来保护处于运行状态和休眠状态的虚拟机，同时提供集中的控管平台，获得最大化的性能和操作灵活性。

一、 Deep Security 9.0 如何保护客户端？

Deep Security(DS) 9.0是由Deep Security Manager(DSM)、Deep Security Virtual Appliance(DSVA)、Deep Security Relay和 Deep Security Agent(DSA)等四个组件构成。



1. 各个组件的定义

1）Deep Security Manager （DSM）

DSM功能强大的、集中式管理，是为了使管理员能够创建安全概要文件与将它们应用于服务器、显示器警报和威胁采取的预防措施、分布服务器，安全更新和生成报告。新事件标注功能简化了管理的高容量的事件。

2）Deep Security Agent （DSA）

一个非常轻小的代理软件组件，部署于服务器及被保护的虚拟机器上，能有效协助执行数据中心的安全政策(IDS/IPS、网络应用程序保护、应用程序控管、防火墙、完整性监控及审查日志)。

3）Deep Security Virtual Agent(DSVA)

与Deep Security Agent 相互协调合作，有效且透明化地的在VMwarevSphere虚拟机器上执行IDS/IPS、病毒防护、WEB应用程序保护、应用程序控管及防火墙保护等安全政策和完整性监控。

4）Deep Security Relay(DSR)

用于从趋势科技全球更新源更新Deep Security的组件。至少要求有一台Deep Security Relay用于更新DSM的DPI Rules。DSA和DSVA 可以通过Deep Security Relay 提升更新组件的性能，并且DSR本身也包含有DSA完整的功能。

2. Deep Security 9.0各模块概述

以下表为Deep Security各个模块在不同组件上的运行状态：

模块	功能	DS 客户端 9.0 SP1					DS 虚拟设备 9.0 SP1
		Windows	Linux	Solaris	AIX	HP-UX	ESXi 5.x
防恶意软件	文件扫描	●	●				●
	注册表扫描	●					
	内存扫描	●					
	云安全扫描	●	●				●
	实时	●					●
		Windows	Linux	Solaris	AIX	HP-UX	ESXi 5.x
Web 信誉服务	全部功能	●					●
		Windows	Linux	Solaris	AIX	HP-UX	ESXi 5.x
防火墙	全部功能	●	●	●	●		●
		Windows	Linux	Solaris	AIX	HP-UX	ESXi 5.x
入侵防御	入侵防御	●	●	●	●		●
	应用程序控制	●	●	●	●		●
	Web 应用程序防护	●	●	●	●		●
	SSL	●	●	●	●		
		Windows	Linux	Solaris	AIX	HP-UX	ESXi 5.x
完整性监控	文件	●	●	●	●	●	●
	注册表	●					
	其他	●	●	●	●	●	
	实时文件	●					
	实时其他	●	●	●	●	●	
		Windows	Linux	Solaris	AIX	HP-UX	ESXi 5.x
日志审查	全部功能	●	●	●	●	●	

模块	功能	DS 客户端 9.0 SP1					DS 虚拟设备 9.0 SP1
		Windows	Linux	Solaris	AIX	HP-UX	ESXi 5.x
		Windows	Linux	Solaris	AIX	HP-UX	ESXi 5.1
漏洞扫描 (推荐设置)	全部功能	●	●	●	●	●	●
		Windows	Linux	Solaris	AIX	HP-UX	ESXi 5.x
用户通知	全部功能	●					● （使用通知程序）

注意：DSVA 不支持日志审查功能

1）病毒保护功能

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。

2）Web 信誉服务

加强服务器及虚拟桌面对 Web 威胁的防护。

与趋势科技™ 云安云安全智能防护网络 Web 信誉功能集成，可通过阻止对恶意 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。

3）Deep Packet Inspection（DPI）深度封包检查

检查所有未遵照协议进出的通信，内含可能的攻击及政策违反。

在侦测或预防模式下运作，以保护操作系统和企业应用程序漏洞。

能够防御应用层攻击、SQL Injection 及Cross-site 跨网站程序代码改写的攻击。

提供有价值的信息，包含攻击来源、攻击时间及试图利用什么方式进行攻击。

当事件发生时，会立即自动通知管理员。

防止已知漏洞来抵挡已知及零时差攻击，避免无限制的攻击。

每小时自动防堵发现到的最新漏洞，无须重新开机，即可在几分钟内就可防御部署至成

千上万的服务器上。

提供数据库、网页、电子邮件和FTP 服务器等100 多个应用程序的漏洞保护。智能防御规则提供零时差的保护，透过检测不寻常及内含恶意程序的通讯协议数据码，以确保不受未知的漏洞攻击。

4）防火墙

减少实体、云端运算及虚拟服务器被攻击的机会。

集中管理服务器防火墙政策，包括最常见的服务器类型。

微粒的筛选特色（IP 与MAC 地址、通讯端口），可针对每个网络设计不同接口和位置政策。

防止DDos攻击，提供事先弱点扫描侦测。

可保护所有基于IP 通讯协议（TCP、 UDP、 ICMP 等）和所有框架类型（IP、ARP 等)。

5）Integrity Monitoring 完整监控

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。

6）Log Inspection 日志审查

收集和分析操作系统和应用程序日志中的安全事件。

协助企业遵循法规(PCI DSS 6.6) 来优化埋在多个日志项目的重要安全事件

将事件转至SIEM 系统或集中日志记录的服务器，作关联性分析、报告和存盘。

可侦测可疑行为、收集数据中心的安全事件和管理操作，并使用OSSEC语法来建立进阶规则。

7）Smart Protection Network云安全智能防护网络

Deep Security 使用趋势科技Smart Protection Network（SPN）提供实时来自云端的实时安全防护。

SPN对于Deep Security提供以下服务：

- Web Reputation Technology
- File reputation Technology
- Smart Feedback

- Global Update Server

要了解更多以上SPN服务的信息请访问：

http://us.trendmicro.com/us/trendwatch/cloud/smart-protection-network/

8）Deep Security Relayes(DSR)

DSR提供了由Deep Security 环境到趋势全球更新服务的更新链路。

9）Smart Protection Servers智能云安全服务器

趋势科技云安全智能防护服务也可以被部署在Deep Security环境中以提供可选的用于Deep Security的本地智能防护服务。

二、 DS9.0安装的各个组件的需求

本章节将介绍Deep Security的各个组件安装需要的最低要求和推荐的要求。

1. Deep Security Manager （DSM）

内存：8GB，其中包括：

1) 4GB 堆内存
2) 1.5GB JVM 系统开销
3) 2GB 操作系统开销

磁盘空间：1.5GB（建议使用 5GB）

操作系统：Microsoft Windows 2012（64 位）、Windows Server 2008（64 位）、Windows Server 2008 R2（64 位）、Windows 2003 Server SP2（64 位）、Red Hat Linux 5/6（64 位）

数据库：Oracle 11g、Oracle 10g、Microsoft SQL Server 2012（所有 Service Pack）、Microsoft SQL Server 2008（所有 Service Pack）。

Web 浏览器：Firefox 12+、Internet Explorer 8.x、Internet Explorer 9.x、Internet Explorer 10.x、Chrome 20+、Safari 5+。（必须启用所有浏览器中的 Cookie。）

注意：这些要求的前提是数据库已安装到单独的服务器上

2. Deep Security Agent(DSA)

内存：128M(不启用防病毒功能)

512M(启用防病毒功能）

硬盘空间：500MB（启用防恶意软件防护时建议使用 1GB）

Windows： Windows Server 2012（64 位）、Windows 8（32 位和 64 位）、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）、Windows XP Embedded

Solaris： Solaris 9、10 和 11（64 位 Sparc）、Solaris 10 和 11（64 位x86）

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）、SuSE 10（32 位和 64 位）、SuSE 11（32 位和 64位）、Ubuntu 10.04 LTS（64 位）、Ubuntu 12.04 LTS（64 位）、CentOS 5（32 位和 64位）、CentOS 6（32 位和 64 位）、Amazon Linux（32 位和 64 位）。

注意：32 位版本的 Linux 上不支持基于客户端的防恶意软件

AIX： AIX 5.3、6.1（AIX 客户端不支持防恶意软件或 Web 信誉服务防护。）

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：运行在Windows XP 和 Windows2003 上的DSA 不兼容IPV6环境

3. Deep Security Virtual Appliance(DSVA)

CPU： 64-bit, Intel-VT present and enabled in BIOS

支持的vSwitch： standard vSwitch标准虚拟机交换机或第三方vSwitch虚拟交换机–Cisco Nexus 1000v

内存：2G（内存容量需求取决于DSVA被保护的虚拟机数量）

硬盘空间：20G

操作系统：VMware vCenter 5.x 和 ESXi 5.x

其他VMware工具：VMware Tools、VMware vShield Manager 5.x 和 VMware vShield Endpoint Security 5.x（适用于 vShield Endpoint 驱动程序的 ESXi5 Patch ESXi500-201109001 或更高版本）。

VMware Endpoint Protection 支持的操作系统：Windows Server 2008（32 位和 64 位）、Windows Server 2008 R2（64 位）、Windows 7（32 位和 64 位）、Windows Vista（32 位和 64 位）、Windows Server 2003 SP2 R2（32 位和 64 位）、Windows Server

2003 SP2（32 位和 64 位）、Windows XP SP2（32 位和 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。）

TPM 虚拟机监控程序完整性监控要求具有 ESXi 5.1，在 ESXi 5.0 上不受支持。

注意：VMware 不支持在生产环境中运行嵌套的 ESXi/ESX 服务器

4. Deep Security Relay(DSR)

内存：512MB

磁盘空间：500MB（启用防恶意软件防护时建议使用 1GB）

操作系统：

Windows：Windows Server 2012（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 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）

5. 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 Server 2012（64 位，非核心）、Windows 8（32 位和 64 位）、Windows7（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 SP2（32 位和 64 位）、Windows Server 2003 R2 SP2（32 位和 64 位）、Windows XP（32 位和 64 位）

注意：在受虚拟设备保护的 VM 上，必须对防恶意软件模块进行授权和启用，趋势科技服务器深度安全防护系统通知程序才能显示信息。

三、 Deep Security 9.0安装前的准备工作

1. Deep Security 各组件安装包

下载地址：

DSM：http://downloadcenter.trendmicro.com/index.php?clk=tbl&clkval=4382&regs=CH&lang_loc=15

DSVA：http://downloadcenter.trendmicro.com/index.php?regs=CH&clk=latest&clkval=4383&lang_loc=15

DSA&DSR：http://downloadcenter.trendmicro.com/index.php?regs=CH&clk=latest&clkval=4384&lang_loc=15

2. 通信与端口

在Deep Security Manager主机上开放下列端口的访问权限

- Port 4119: 连接到DSM使用的端口号
- Port 4120: Deep Security Agent 与Deep Security Manager 之间的通信
- Port 1433 and 1434:与Microsoft SQL Server 双向通信的端口
- Port 1521:与Oracle Database server 双向通信的端口
- Port 514 (可选):与 Syslog server双向通信的端口
- Port 389:（可选）与LDAP连接用于Active Directory集成环境
- Port 80,443 (可选)连接到趋势科技Deep Security 9.0传统更新服务器
- Port 53：用于DNS 查询

用于Deep Security Relay,Agent和Appliance的通讯端口：

- Port 4122:用于把更新信息转发到Agent /Appliance
- Port 4118:DSM 与 Agent/Appliance 之间通讯端口
- Port 80，443：连接到趋势科技更新服务器和趋势科技智能云安全服务器
- Port 514(可选)：与SYSLOG 服务器双向通讯

3. 激活码和更新认证帐号

在购买Deep Security 的时候会得到一个激活码，如果没有这个产品激活许可证，将无法获得最新的安全更新。

注意：你还需要获取Vmware 相关组件的激活码，如需要使用Deep Security 无代理病毒防护功能必须获得Vmware vShield Endpoint 激活号

4. 网络连接

需要注意的是，Deep Security Manager 和Deep Security Agent/Virtual Appliance之间的通信是通过解析对方的机器名完成，所以要保证Manager 和Agent 能正常解析IP 地址和机器

名。建议在内网部署DNS 服务器并且建议Deep Security Manager,Deep Security Virtual Appliance 以标准的FQDN名称命名。

例如：

DSM.DomainName.com

DSVA.DomainName.com

注意：如果您的网络环境中没有DNS 服务器建议在部署Deep Security Manager时使用IP 地址方式部署

5. 可靠时间戳同步

Deep Security 各组件在的计算机时间必须与一个可靠的时间同步源同步。例如，可以通过NTP协议定期与NTP 服务器进行时间同步。DSR,DSVA,DSA 与DSM 上的时间必须与DSM 的时间周期在24小时以内。

6. 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。

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。

7. 数据库

Deep Security Manager（DSM） 内部已集成 Apache Derby 数据库，可以在DSM 安装时直接安装嵌入式数据库。

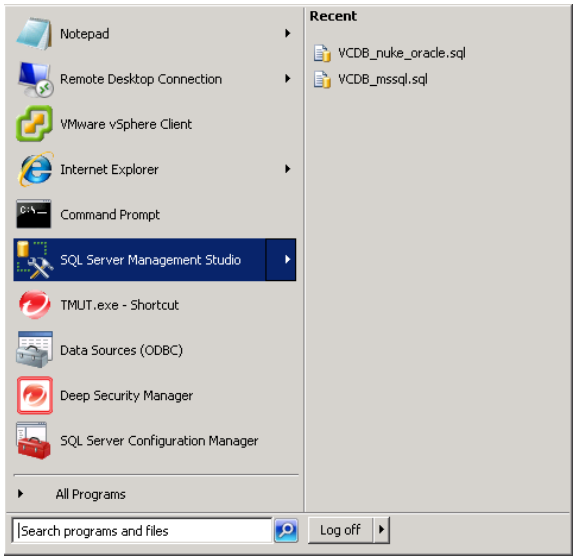
注意，Apache Derby 数据库只适用于受Deep Security保护终端小于10台的测试环境。

为了保证Deep Security Manager在企业网络环境中长期可靠运行，建议Deep Security Manager 在正式部署时采用企业级后端数据库系统例如：SQL Server 2008或 Oracle 11g。

如果选择安装独立的MS SQL Server 或 Oracle 数据库，需要在数据库管理控制台中先手动建立DSM 数据库实例。

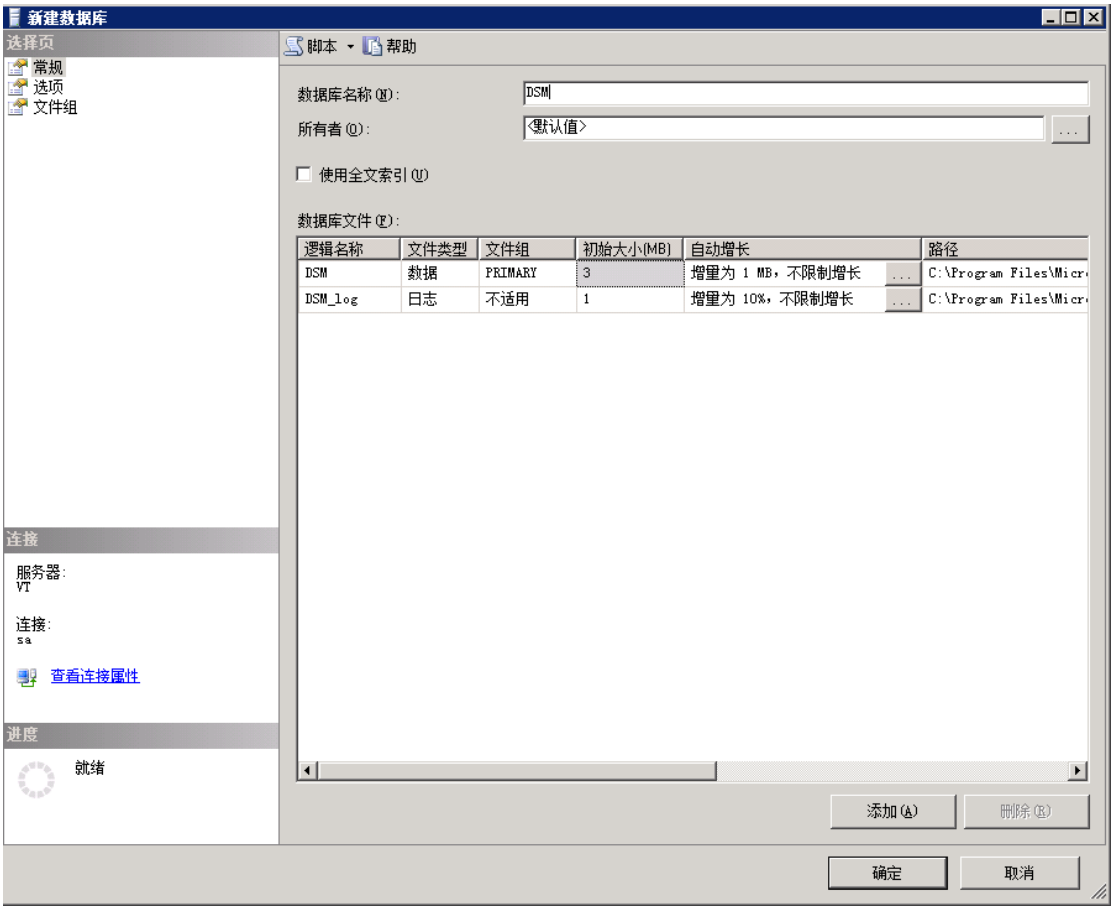
示例：在 SQL 2008 Server Management Studio 中建立 DSM 数据库实例

1) 打开 SQL 2008 Server Management Studio 管理控制台



2) 右键点击“数据库”选择 “新建数据库”

3) 输入数据库名称，例如“DSM”



4) 按“确定”按钮，完成数据库实例创建

8. Vmware 高可用性(HA)环境

如果您打算采用Vmware High Availability(HA)功能，请确保在Deep Security 9 安装以前已经完成Vmware HA的搭建。所有会进行故障恢复操作的ESXi 主机必须导入到与DSM 集成的vCenter环境，并且这些ESXi主机必须被置于“prepared”状态，每台ESXi主机上还必须部署一台DSVA。通过以上配置可以确保在Vmware执行恢复操作时Deep Security 防护的有效性。

注意：

当一台虚拟设备(DSVA)被部署在使用Vmware 分布式资源调度(DRS)的Vmware环境中。请确保DSVA 不会被DRS 调度而被执行vMotion迁移动作。DSVA 必须被“固定”在DSVA 所对应的ESXi主机上. 您还可以通过把DSVA 部署在ESXi主机的本地存储上来避免DSVA由于DRS调度而导致的vMotion迁移动作。

请在vCenter控制台上设置DSVA 的DRS 为手动或关闭（推荐设置），这就是之前所知的“固定”在指定的ESXi主机上。要想了解更多有关DRS设定请参考Vmware 相关文档。

注意：

如果一台虚拟机由HA 控制从一台受到DSVA保护的ESXi主机上vMotion迁移到另外一台不受DSVA保护的ESXi主机，那么这台虚拟机将不再受到Deep Security的保护。如果一台虚拟机从不受DSVA保护的ESXi主机vMotion迁移到受DSVA 保护的虚拟机时，这台虚拟机不会自动进入“被保护”状态，除非您开启了Event-base 任务—当被保护的虚拟机发生vMotion迁移时Deep Security会自动对虚拟机执行激活动作。

四、 虚拟环境无客户端防护部署

1. 推荐环境概述

以下内容描述了Deep Security如何部署在一个典型的Vmware 虚拟化环境。

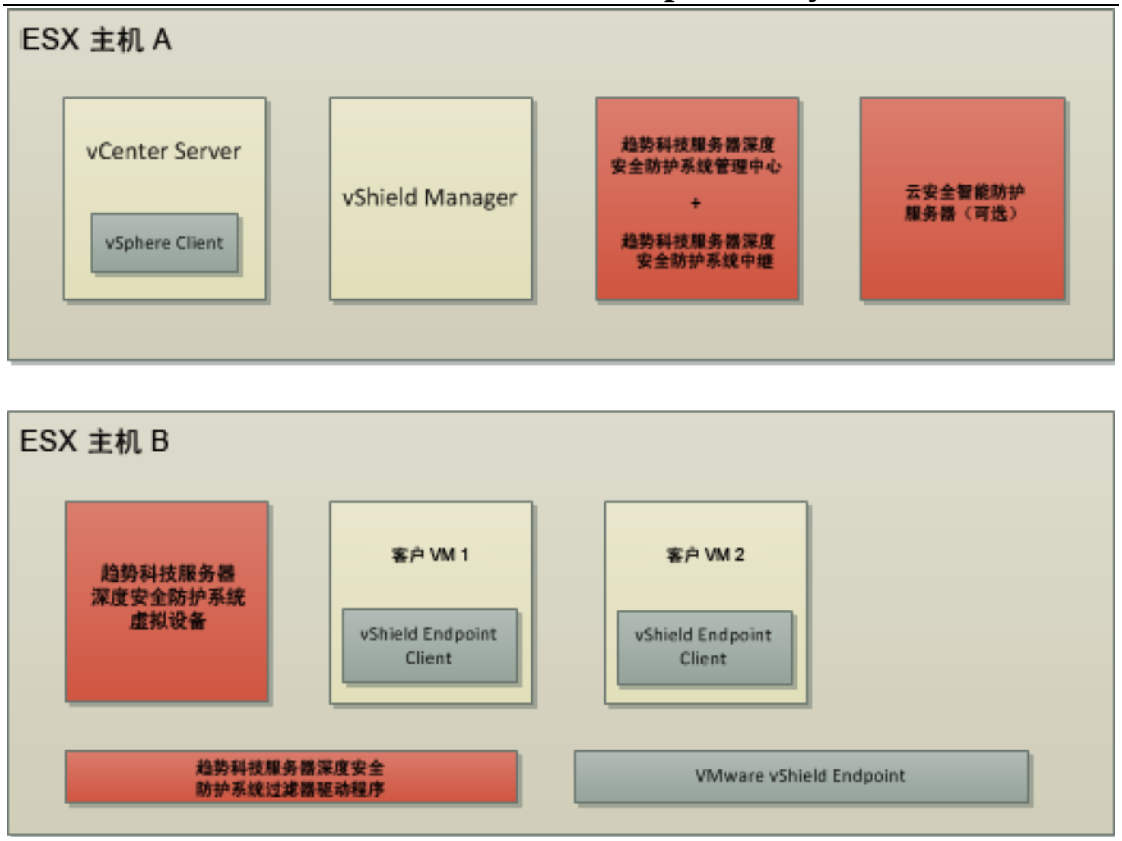
注意：vCenter Server、vShield Manager 和趋势科技服务器深度安全防护系统管理中心安装在单独的 ESXi 上，因为在趋势科技服务器深度安全防护系统部署期间必须重新启动受保护的ESXi。另请注意，趋势科技服务器深度安全防护系统数据库未显示在下图中。它还可以安装在物理计算机上或安装在 VM 上。

典型环境描述：有两台 ESXi 主机

HostA：是 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9.0、vShield Manager 5.x 和 vCenter Server 5.x 的单个虚拟机 (VM)。（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。

HOSTB：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虚拟设备 (DSVA) 和需要防护的 VM。

典型虚拟化防护环境图示：



所需资源核对清单：

检查	软件要求	注意
	VMware vCenter 5.x	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.x	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 9.0 (DSM)	产品安装期间需要使用授权。
	VMware vShield Endpoint 5.x	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 9.0 (FD)	
	趋势科技服务器深度安全防护系统虚拟设备 9.0 (DSVA)	
	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 ESXi 5 patch ESXi500-201109001 开始，vShield Endpoint 驱动程序包括在 VMware Tools 中。）

2. 准备 Deep Security 虚拟化防护环境准备标准步骤

任务一：安装 ESXi 5.X

任务二：安装 vCenter Server (VC)5.X
任务三：安装 vShield Manager (vSM)5.X
任务四：准备一台虚拟机用于 DSM 后台数据库
任务五：在 HostA　ESXi 5.X 上准备一台虚拟机用于 DSM 9.0
任务六：客户机准备，确认客户机 Windows 2003 或 Windows XP 操作系统已经安装 SP2 补丁，确保每台被保护的虚拟机已经安装对应版本的 Vmtool，具体参考以下列表。

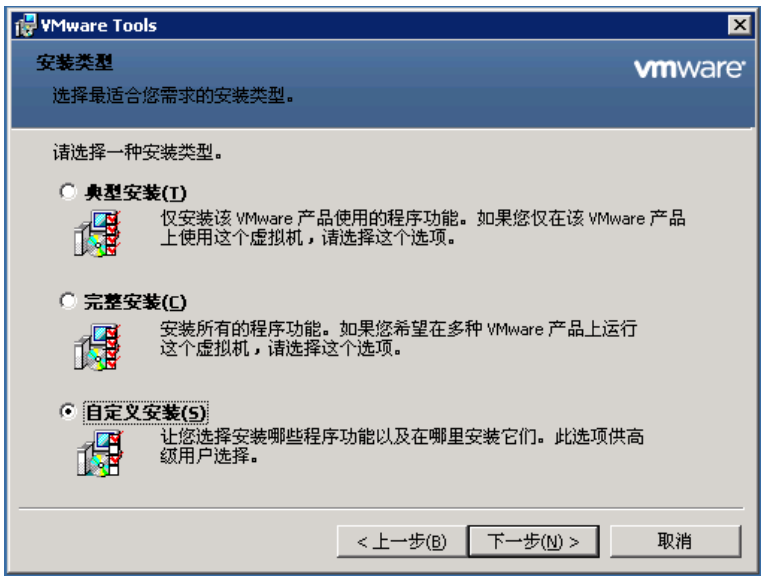
Core Drop or Release info	Date	vCloud	View Manager View Composer	vCenter 4	vCenter 5	ESXi 4	ESXi 5	vShield Manager	vShield Endpoint (For ESX)	vShield Thin Agent (VMWare Tool)
Epsec 3.0										
vSphere 5.1 + vShield 5.1	2013/2/10	N/A	N/A	N/A	5.1.0 799731	N/A	5.1.0 799733	5.1.0-807847	5.1.0-757363	8.9.2-726910
vSphere 5.1 + vShield 5.1.2	2013/2/19	N/A	N/A	N/A	5.1.0 799731	N/A	5.1.0 799733	5.1.2-943471	5.1.0-833297	8.9.2-726910
vCenter 5.1 + ESXi 5.0U3 + vShield 5.1	2013/2/15	N/A	N/A	N/A	5.1.0 799731	N/A	5.0.0 914586	5.1.0-807847	5.1.0-757363	8.6.10-913593
vCenter 5.1 + ESXi 5.0U3 + vShield 5.1.2	2013/2/19	N/A	N/A	N/A	5.1.0 799731	N/A	5.0.0 914586	5.1.2-943471	5.1.0-833297	8.6.10-913593
vSphere 5.0U3 + vShield 5.1	2013/2/17	N/A	N/A	N/A	5.0.0 913577	N/A	5.0.0 914586	5.1.0-807847	5.1.0-757363	8.6.10-913593
vSphere 5.0U3 + vShield 5.1.2	2013/2/18	N/A	N/A	N/A	5.0.0 913577	N/A	5.0.0 914586	5.1.2-943471	5.1.0-833297	8.6.10-913593

注意：Vmware vShield Endpoint 5.0 驱动程序驱动程序默认集成在最新版的 Vmware Tool 中，但是默认部署 Vmtool 时并不会安装 vShield Endpoint 驱动程序这会导致 Deep Security 9.0 的无代理病毒防护功能失效。

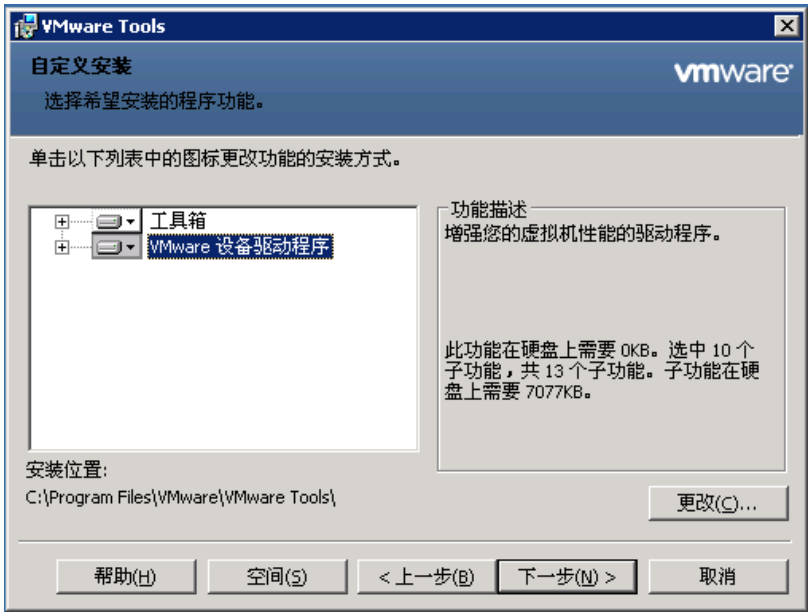
安装 vShield Endpoint 驱动程序请参考以下步骤：

1.运行 Vmtool 安装程序并进行交互式安装

2.在安装时选择“Custom Install”(自定义安装)

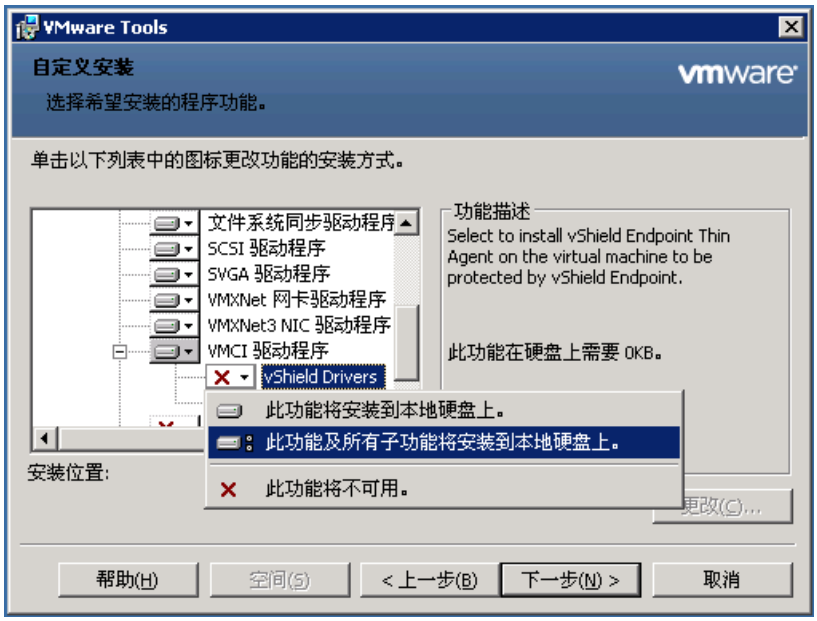


3.展开 Vmware Device Drivers（Vmware 设备驱动程序）



4.展开 VMCI 驱动

5.选择 vShield 驱动并且寻则“This feature will be installed on local driver”(此功能将被安装在本地磁盘)



五、Deep Security 9.0的各个组件的安装

Deep Security 9.0 组件安装主要步骤：

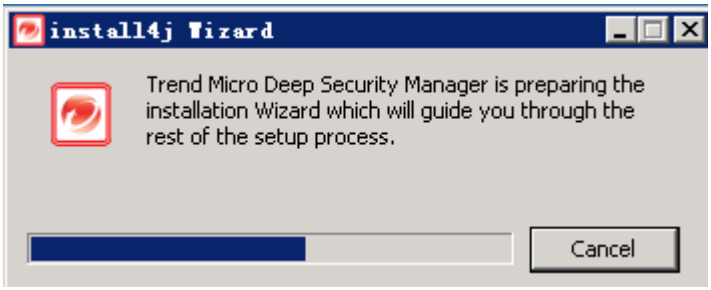
1) 安装数据库用于 Deep Security Manager

- 安装：SQL Server 2008 或 Oracle 11g 数据库软件
- 创建数据库：在 DSM 安装前通过数据库管理软件创建一个 DSM 数据库
- 分配数据库磁盘空间：每增加一台 DSA 客户端大约需要培训 55 MB 的数据库空间。
- 数据库帐号设置：DSM 安装程序在安装时会要求数据库帐号，请确保此数据库帐号允许 DB_Creator Server Roles 并且是 DSM 数据库的 DB_Owner.
- DSM 与数据库通信设置：当 DSM 通过“Named pipes”命名管道连接一台 SQL 服务器时，DSM 主机与 SQL Server 主机之间必须有一个可用的 身份认证的 Microsoft Windows 通讯管道。 这个认证的通讯管道通常存在于以下情况：
  a) SQL Server 与 DSM 安装在同一台服务器
  b) SQL Server 与 DSM 服务器在同一个域中
  c) 两台主机见存在信任关系
  d) 如果通讯管道不可用，那么 DSM 将无法通过“命名管道”与 SQL server 通讯。

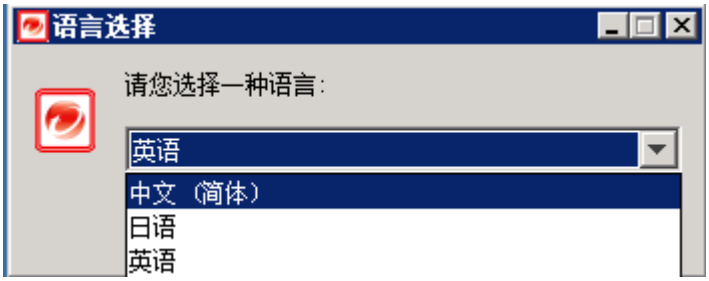
2) 安装 Deep Security Manager 和 Deep Security Relay
3) 配置 DSM 与 vCenter、vShield Manager 集成
4) “Prepare”ESXi5.X 主机并部署 DSVA

1. Deep Security Manager（DSM）安装

1) 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。



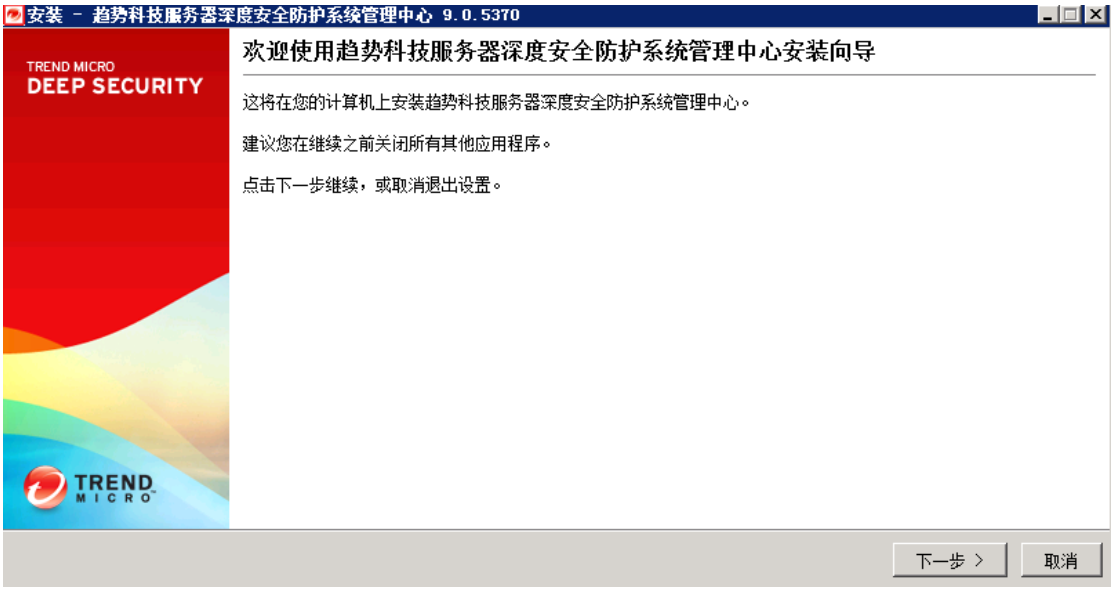
2) 选择安装语言，然后单击确定和下一步。



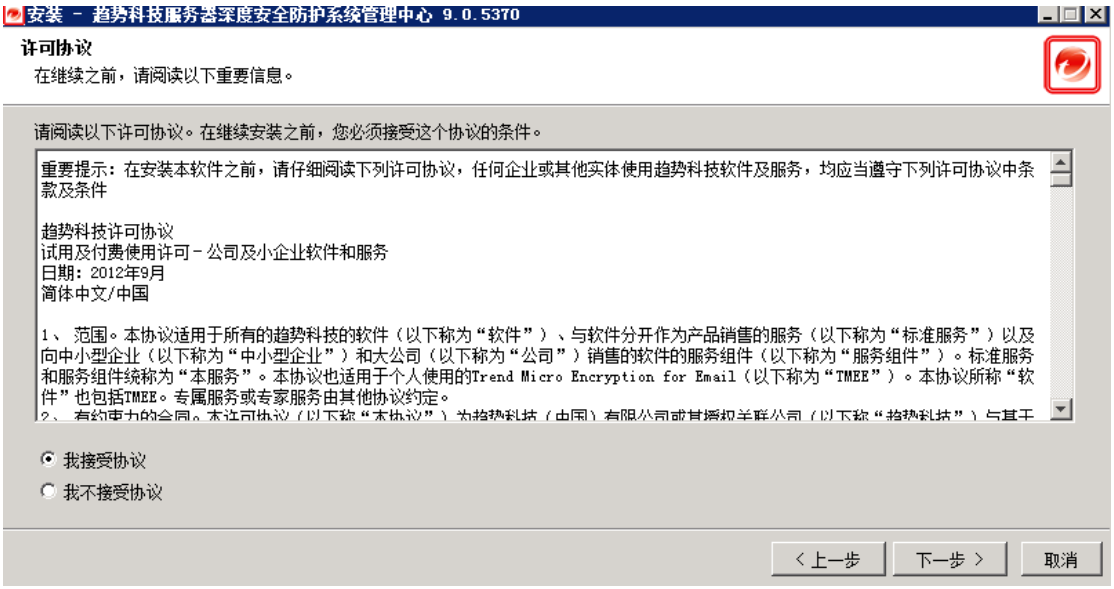
注意：安装后，趋势科技服务器深度安全防护系统用户可以分别设置其用户界面语言。(要更改用户的语言设置，请转至管理 > 用户，然后编辑用户帐户的属性.

3) 弹出安装向导，点击“下一步”如果您同意许可协议的条款，请选择我接受协议并

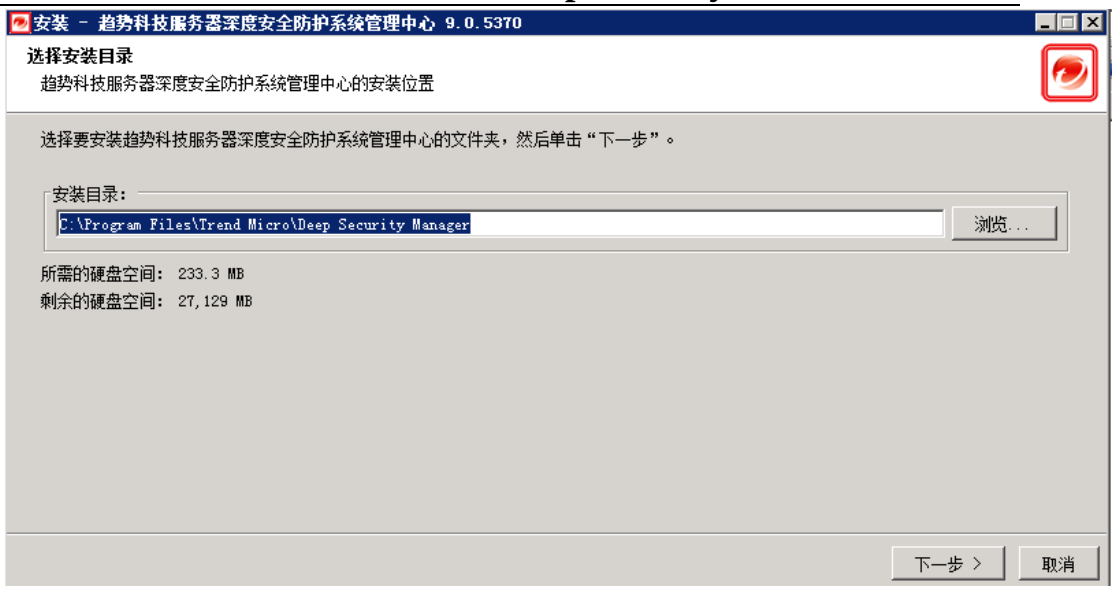
单击下一步。



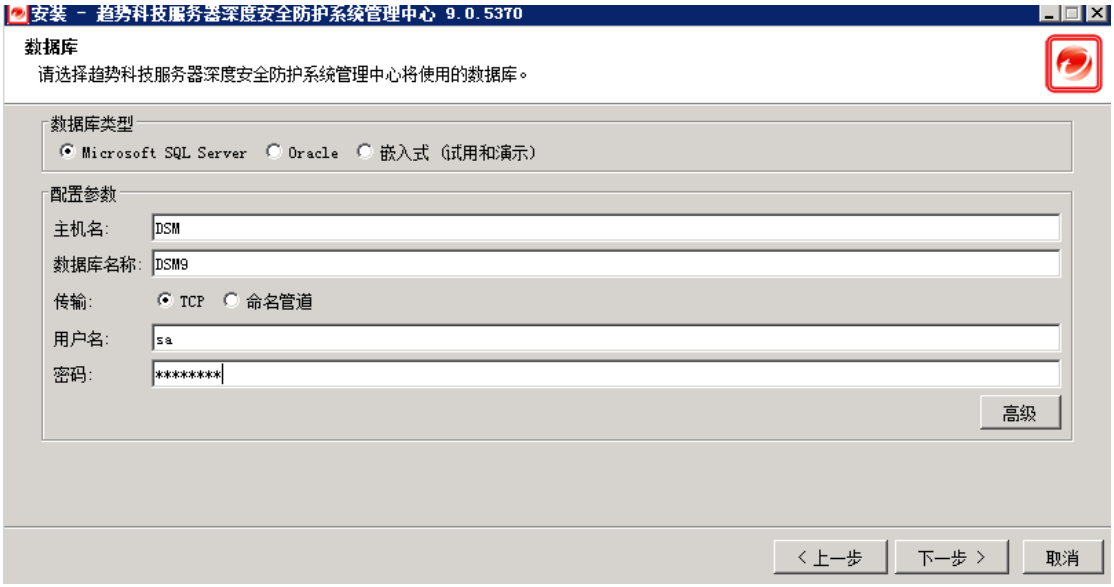
4) 如同意许可协议的条款，请选择我接受协议并单击下一步。



5) 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。

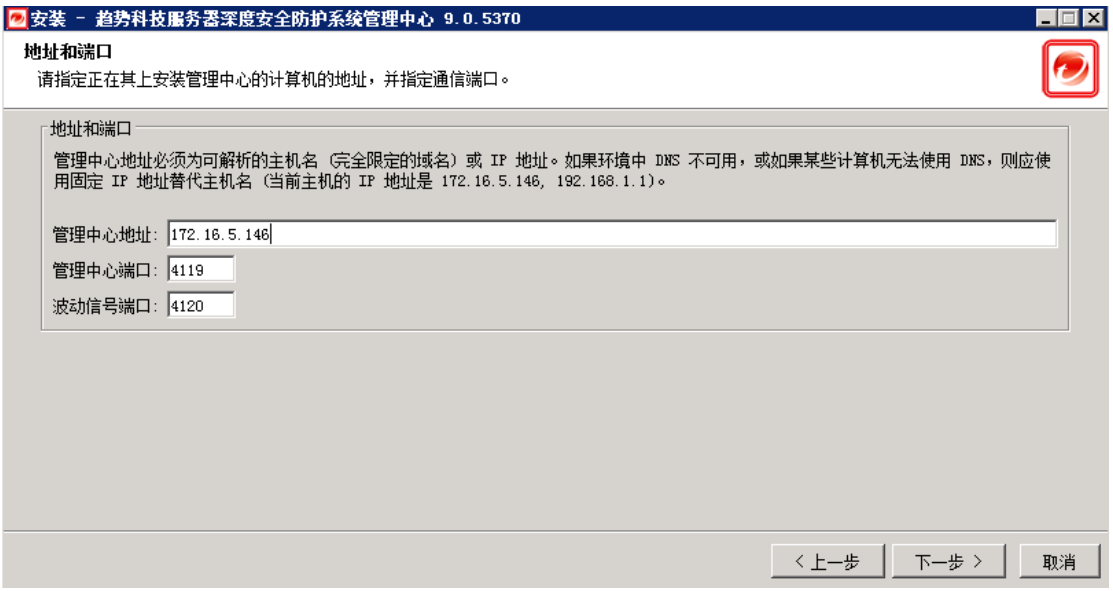


6) 指定要使用的数据库类型，如果使用 Oracle 或 SQL Server 数据库，则必须在安装趋势科技服务器深度安全防护系统管理中心之前创建数据库，输入帐户详细信息。

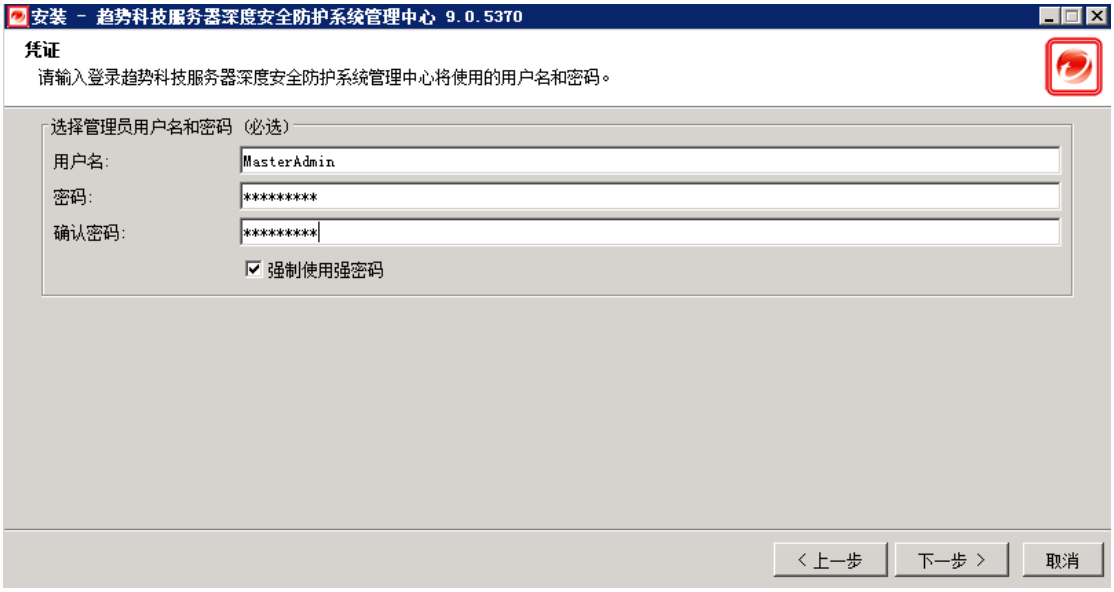


7) 输入激活码。请输入所有防护模块的激活码或分别输入已购买使用授权的各个模块的激活码。如果未输入任何激活码，您仍可以继续，但将无法使用任何防护模块。（您可以在安装趋势科技服务器深度安全防护系统管理中心后转至管理 > 使用授权输入首个激活码或添加激活码。

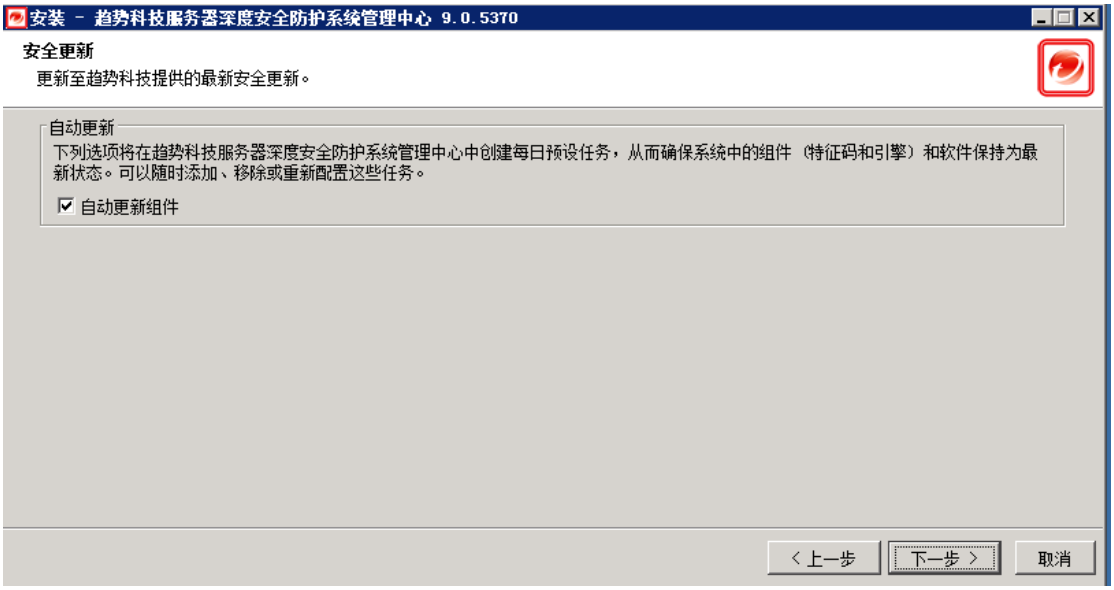
8) 键入此计算机的主机名、URL 或 IP 地址。管理中心地址必须为可解析的主机名(完全限定的域名) 或 IP 地址。如果环境中 DNS 不可用，或如果某些计算机无法使用 DNS，则应使用固定 IP 地址而不使用主机名。可以选择更改缺省通信端口：“管理中心端口”指可通过 HTTPS 访问管理中心的基于浏览器的 UI 的端口。“波动信号端口”指管理中心侦听来自客户端/设备的通信的端口。单击下一步。



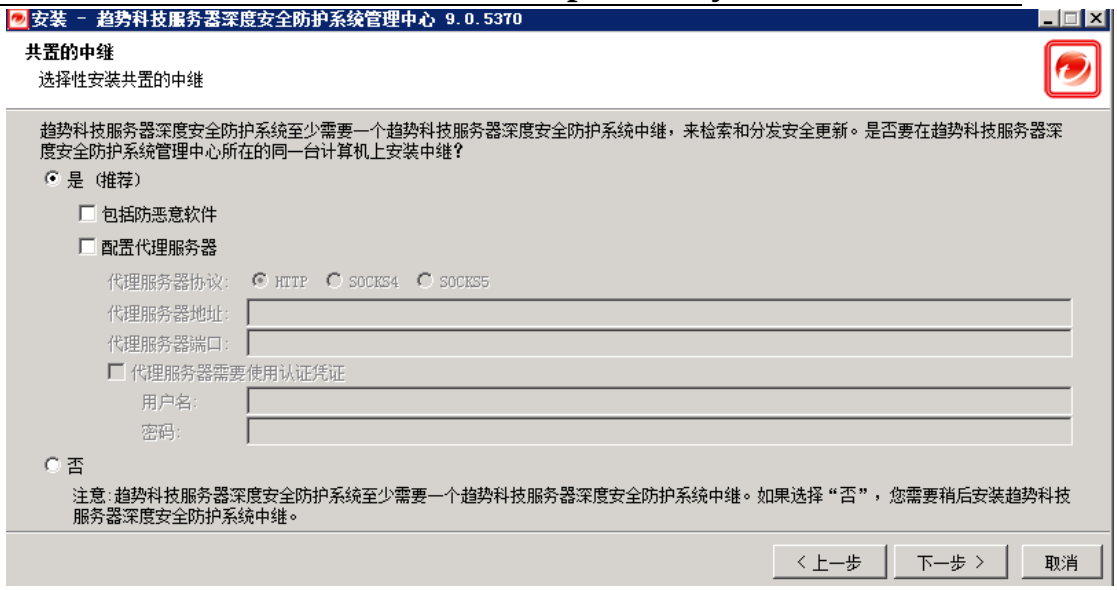
9) 输入主管理员帐户的用户名和密码。选中“强制使用强密码”（建议）会要求此管理员及以后创建的管理员的密码包括大写和小写字母、非字母数字字符以及数字，并且要求使用最小字符数。单击下一步。



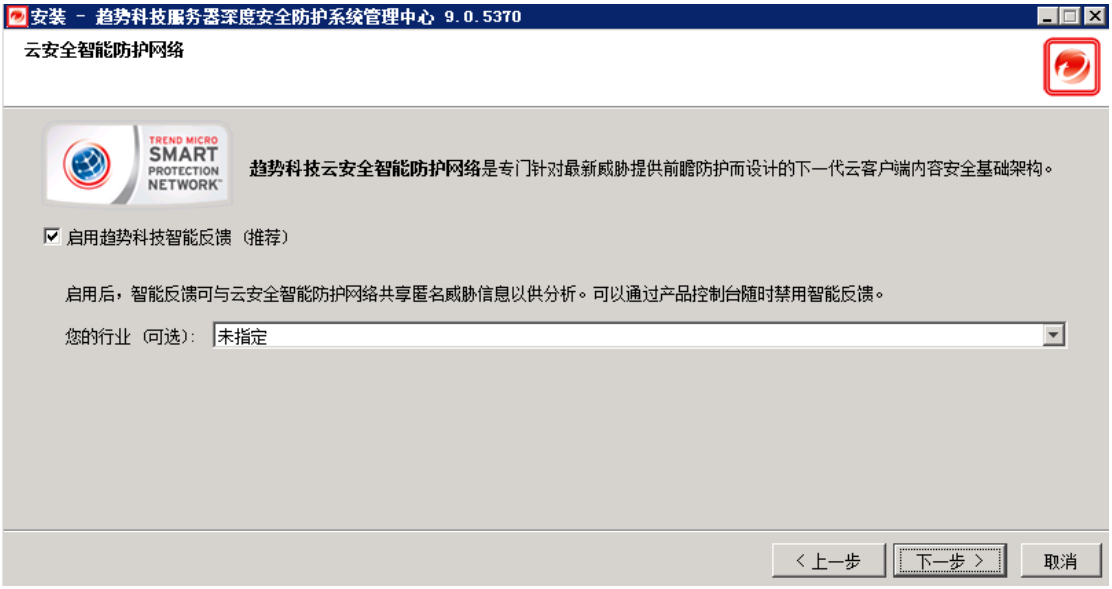
10) 选中“自动更新”（建议）。如果选中，趋势科技服务器深度安全防护系统管理中心将自动检索最新的组件或检查新软件。（以后可以使用趋势科技服务器深度安全防护系统管理中心配置更新。）单击下一步。



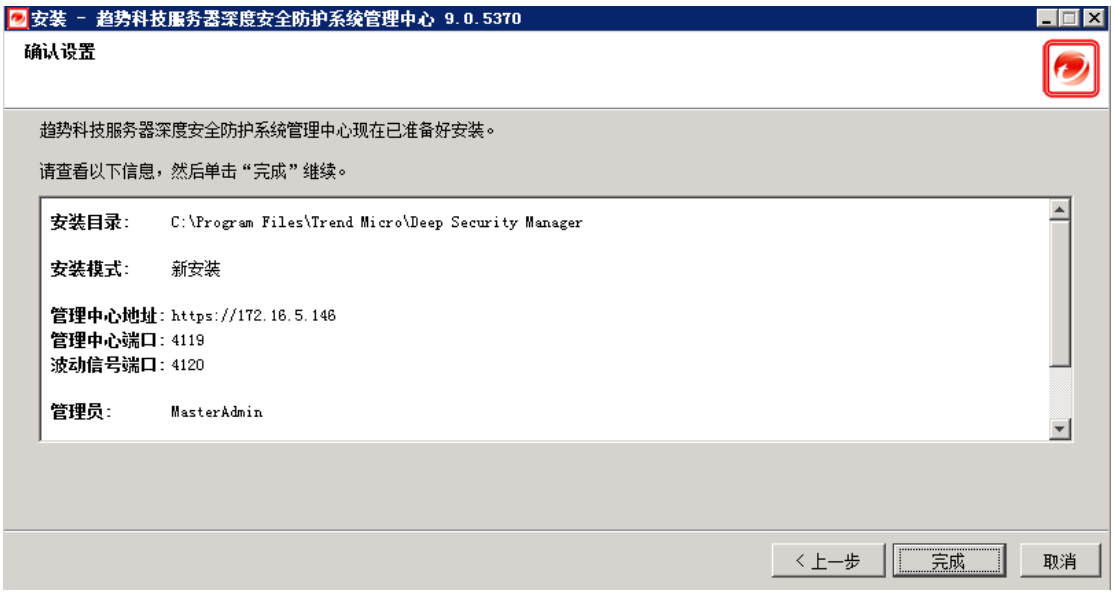
11) 选择是否安装共置趋势科技服务器深度安全防护系统中继。（如果在趋势科技服务器深度安全防护系统管理中心安装程序的位置没有趋势科技服务器深度安全防护系统中继安装包，将跳过此步骤。）单击下一步。



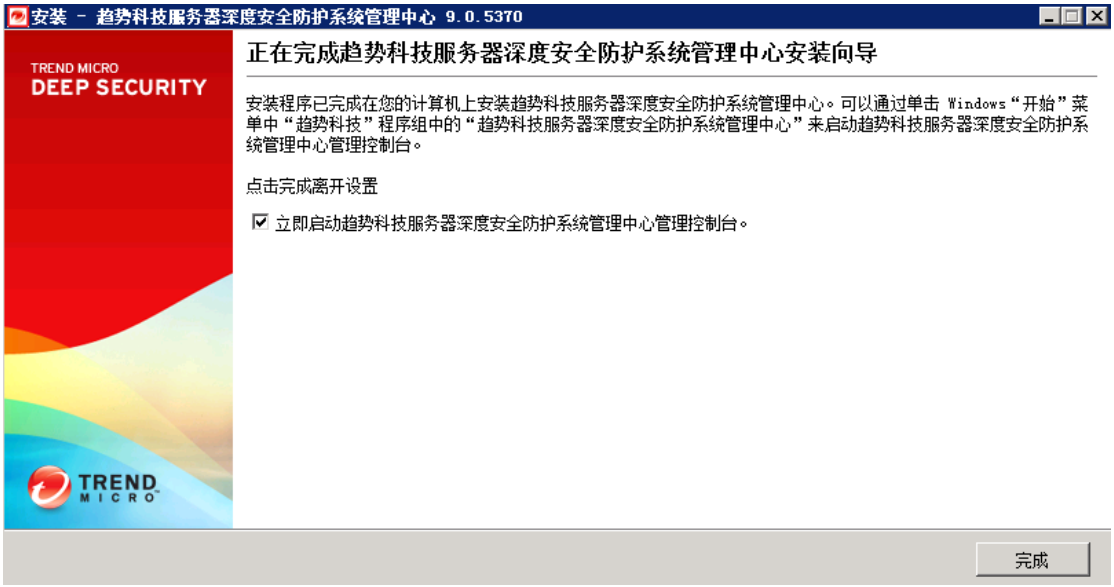
12) 选择是否要启用趋势科技智能反馈（建议）。（以后可以使用趋势科技服务器深度安全防护系统管理中心启用或配置智能反馈）。（可选）通过从下拉列表中进行选择来输入行业。单击下一步。



13) 确认设置。验证输入的信息，然后单击完成继续。



14) 单击完成关闭安装向导。

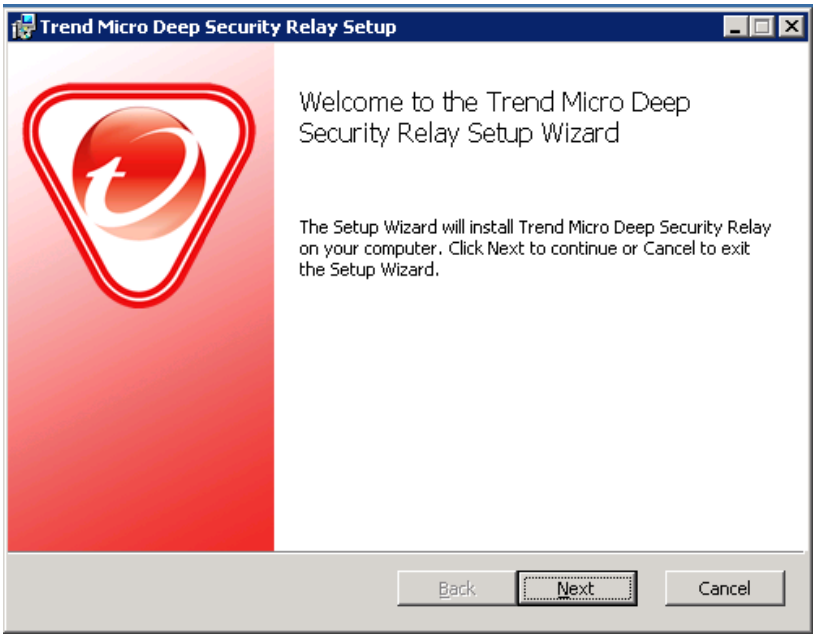


15) Deep Security Manager 服务会在安装完成时启动。如果在步骤 10 中选择了安装共置趋势科技服务器深度安全防护系统中继，现在将以静默方式运行中继安装。安装程序会在程序菜单中添加趋势科技服务器深度安全防护系统管理中心的快捷方式。如果要远程访问管理中心，应注意此 URL。

2. Deep Security Relay for Windows(DSR)安装（可选）

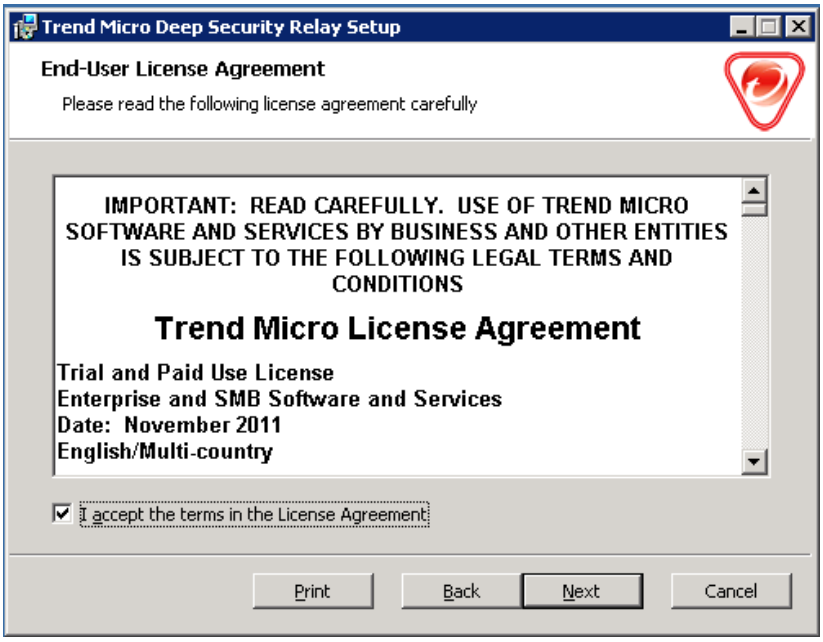
注意：Deep Security Relay 安装程序会同时安装 Relay Server 和 Deep Security Agent 在 windows 主机上的功能。

1) 双击安装文件来运行安装包，单击 Next 开始安装。



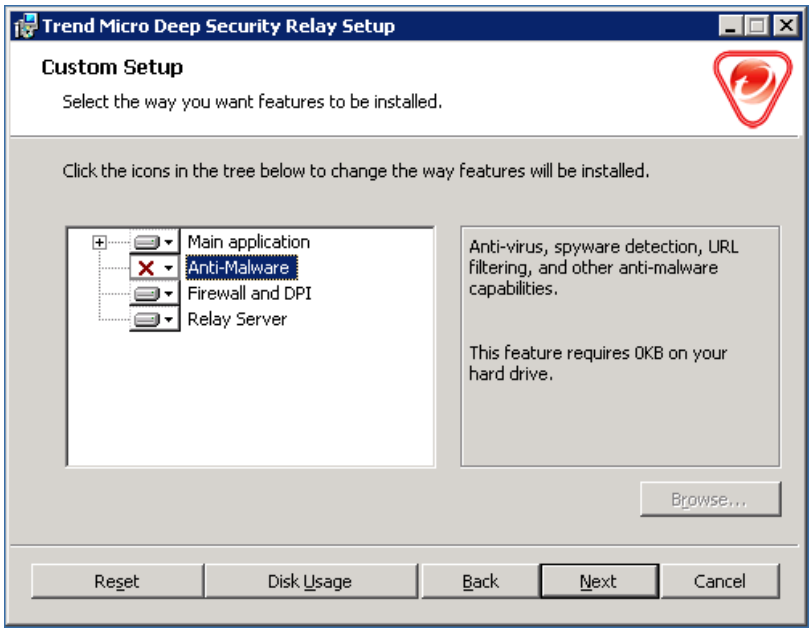
注意：安装时你必须在Windows主机上以管理员权限来安装和运行Deep Security Relay。

2) 接受许可协议，然后单击 Next 继续



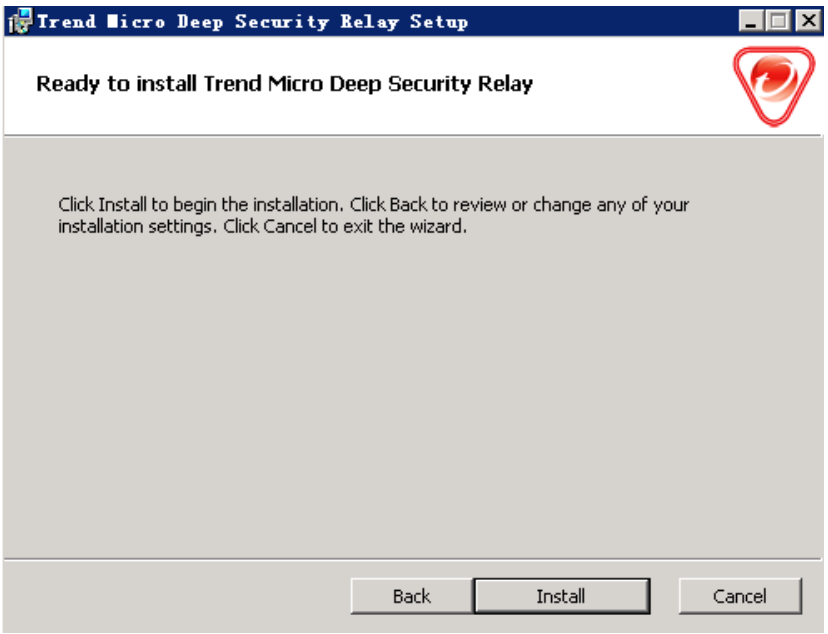
3) 选择要安装的功能（防恶意软件等一些功能是可选的）。单击 Browse 指定要安装趋

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 Reset 将选择重置为缺省设置。



注意：无法取消选择防火墙和入侵防御功能。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，即使不使用防火墙和入侵防御功能也会始终安装这些功能。单击“Disk Usage”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。

4) 点击 “Install”开始安装程序



5) 点击“Finish”完成安装

注意：

- *在执行安装过程中，网络接口会暂时中断几秒。如果您的主机使用DHCP方式分配IP地址，在连接恢复后产生的新的DHCP 地址分配请求可能会导致DSR被分配一个新的IP地址。*

- *不推荐通过远程桌面方式安装Deep Security Relay,如果需要通过远程桌面方式部署DSR ， 请在远程连接命令后面加上以下参数：*
  Windows Server 2008 ,Vista SP1 或 Windows XP SP3 更高版本请使用：
  mstsc.exe /admin
  更早的Windows 版本请使用以下命令：
  mstsc.exe /console

3. 配置 Vmware 整合

通过下列配置来准备 Deep Security / Vmware 环境

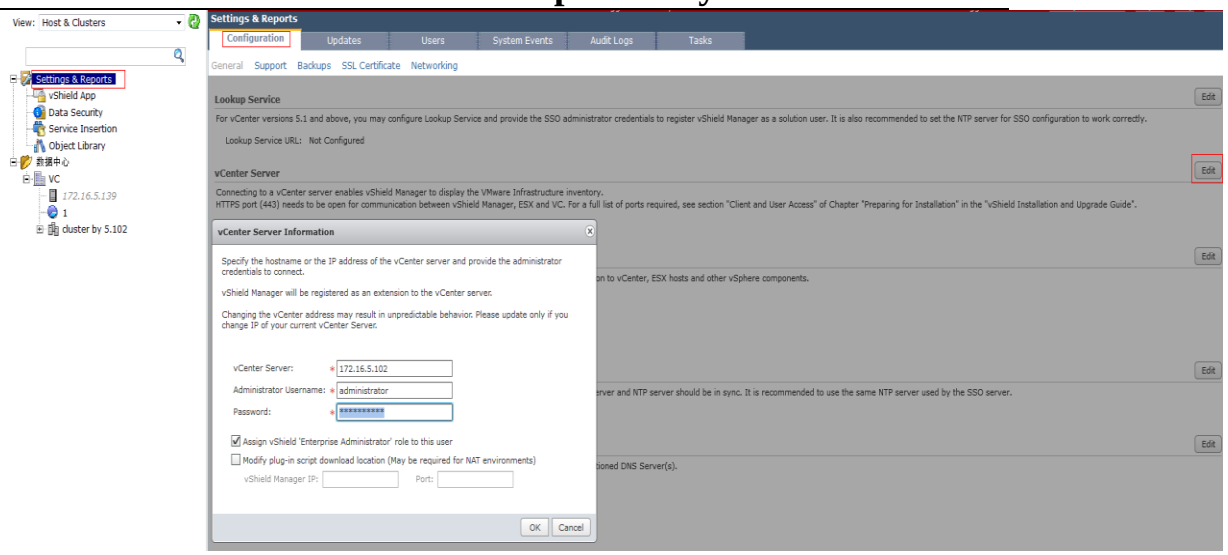
在进行配置前请确认：

- 已经根据虚拟化防护环境准备标准步骤完成 Vmware 基本环境搭建
- 已安装 Deep Security Manager （包括数据库）
- 已安装了 Deep Security Relay 并在 DSM 控制台进行基本配置

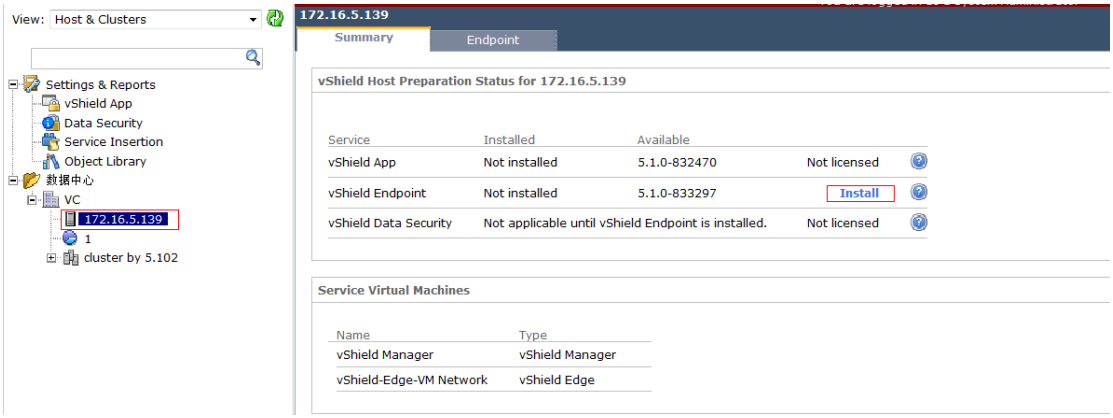
在 ESXi 主机上安装 Vmware vShield Endpoint(EPSec)

1) 登录 vShield Manager 管理控制台 https://<vSM-ip>
2) 输入默认用户名 admin,默认密码 default 登录。

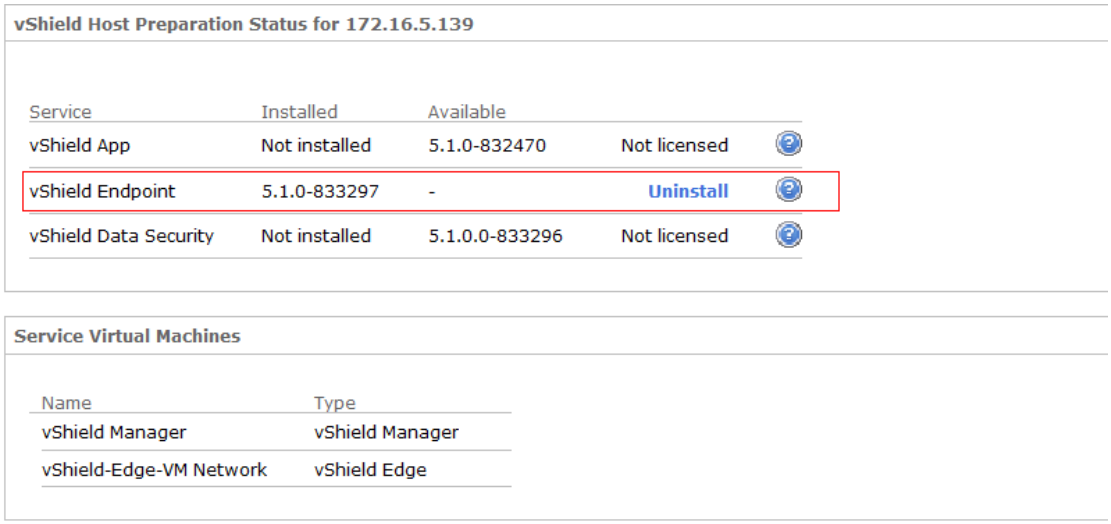
3) 按如下图设置 vCenter Server 信息。



4) 选择被 Deep Security 保护的 ESXi 主机，安装 vShield Endpoint 组件



5) 安装完毕后如图所示：

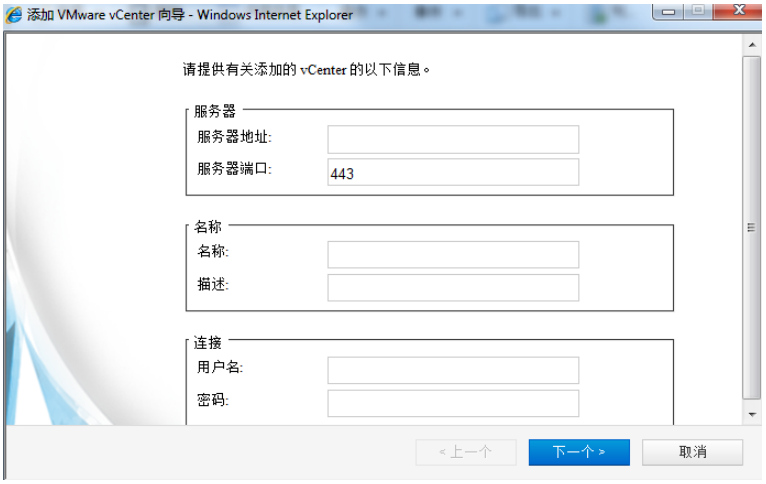


4. Deep Security Virtual Appliance(DSVA)安装部署

I. 添加 Vcenter

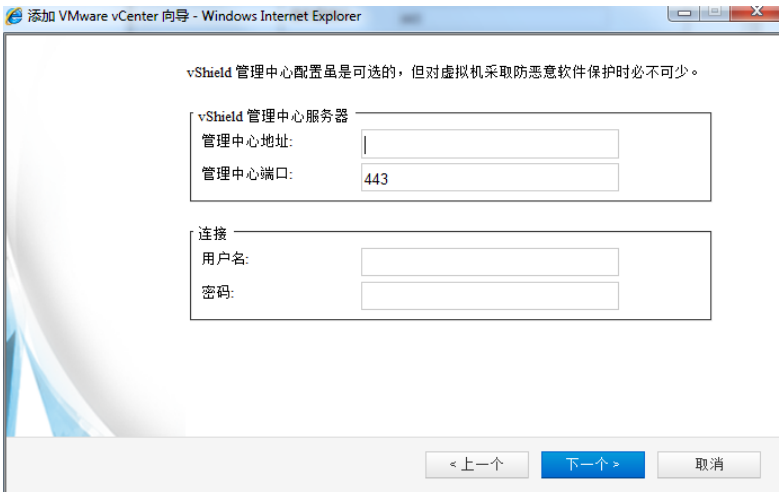
1) 在趋势科技服务器深度安全防护系统管理中心的计算机窗口中，单击新建 > 添加 VMware vCenter...

2) 输入 vCenter Server IP 地址（或主机名）、vCenter 的用户名和密码。单击下一个

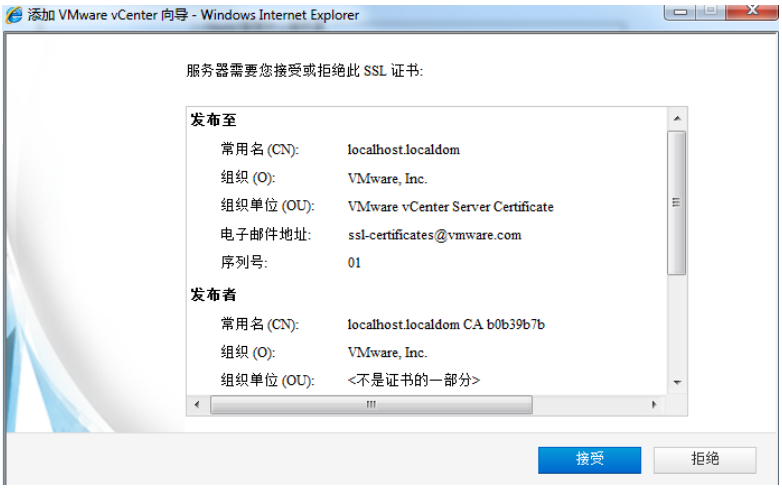


注意：确保 DNS 已配置且能够将 FQDN 解析为此环境中的所有计算机使用的 IP 地址，否则输入 IP 地址。

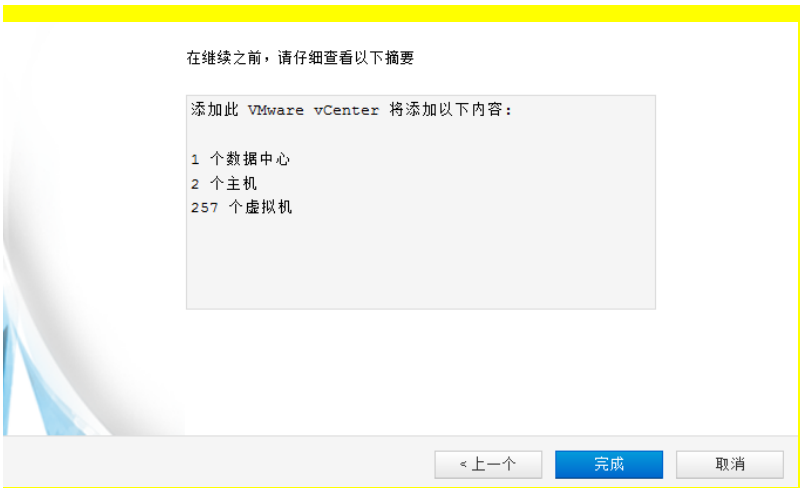
3) 输入 vShield Manager Server 地址。用户名和密码。（也可在以后从趋势科技服务器深度安全防护系统管理中心配置此信息。）单击下一个



4) 接受 vCente 证书。



5) 查看 vCenter 信息，单击完成。

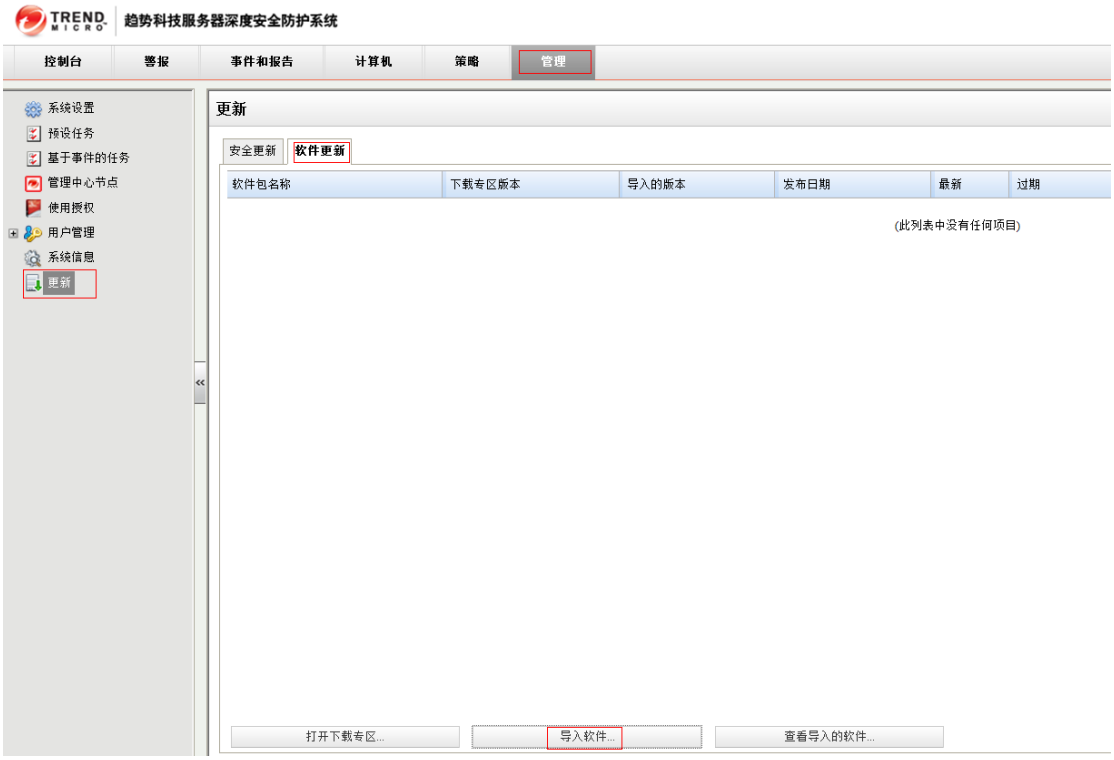


6) 此时将显示已成功添加 VMware vCenter 消息。单击关闭

注意：在具有 3000 台以上的计算机向 vCenter Server 报告的大型环境中，此过程可能要花费 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。

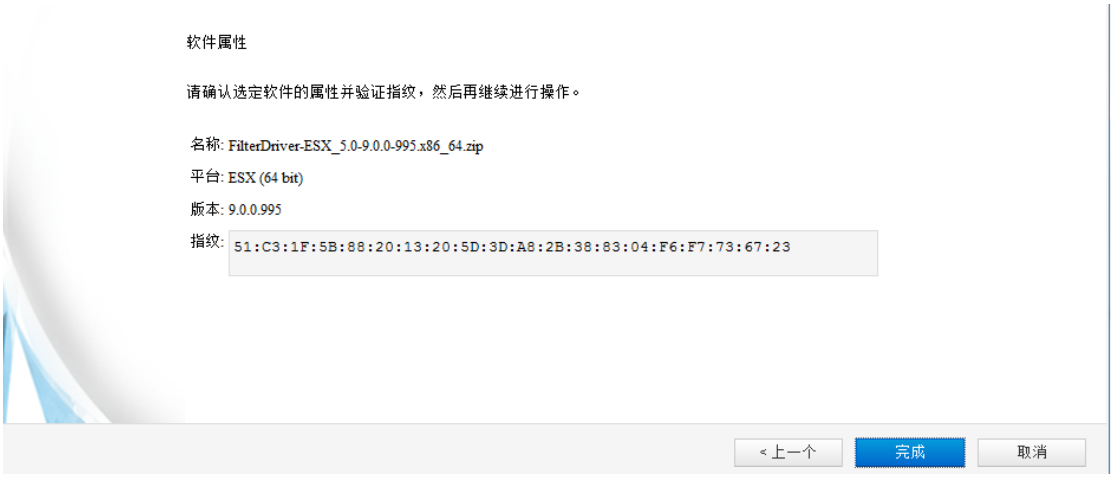
II. 对 ESXi 进行准备和驱动的安装

1）点击“管理”—“更新”—“软件更新”—“导入软件”



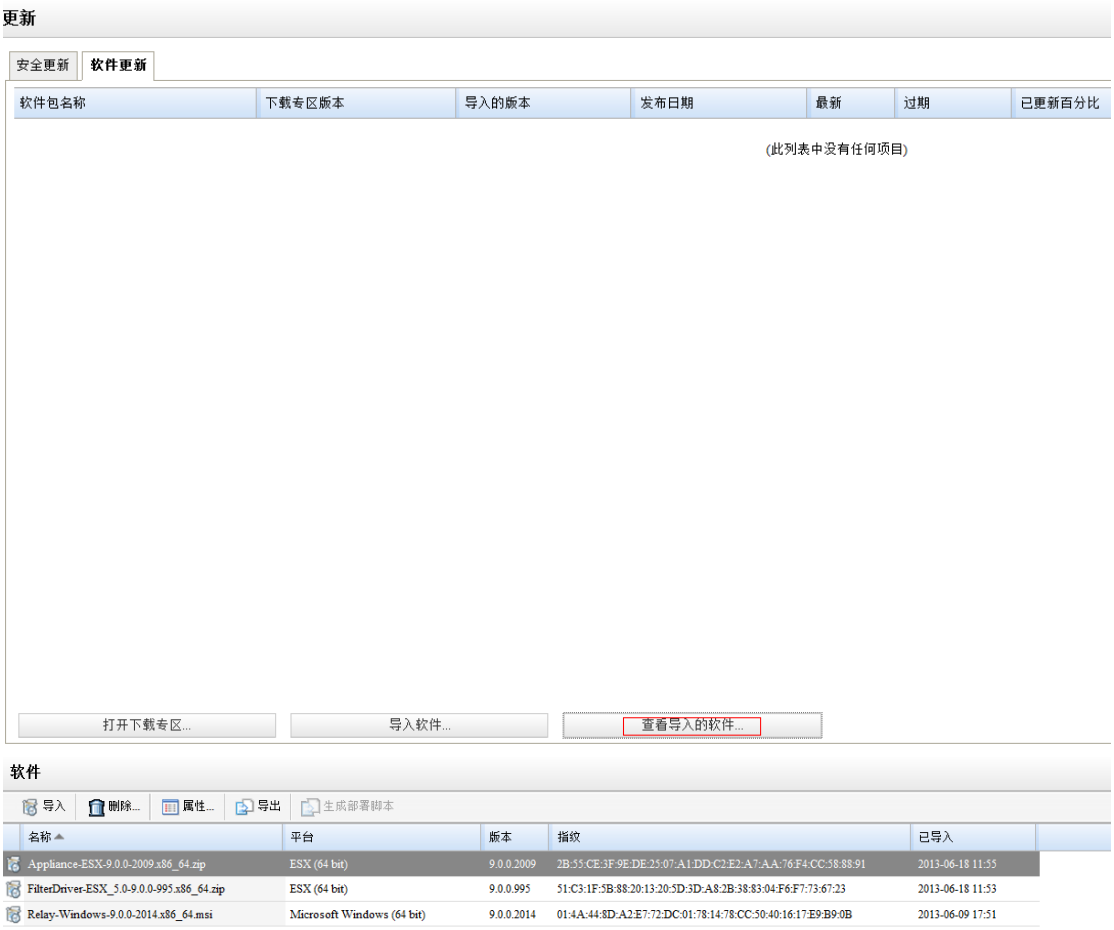
2）导入 Filter 驱动，点击“下一个”

3）点击完成

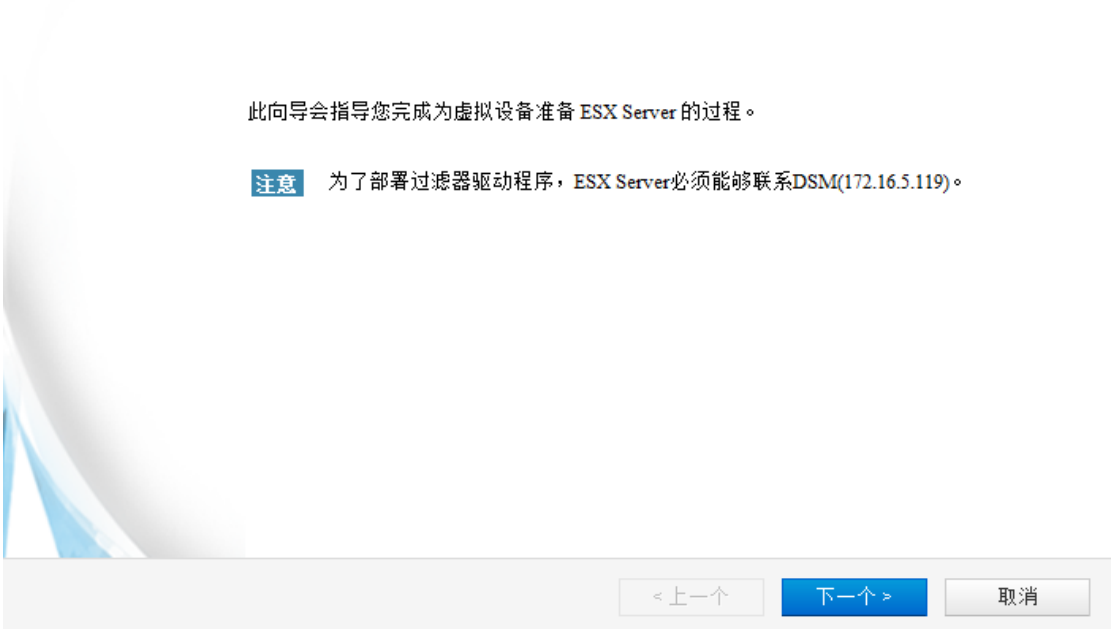


按照上述 1）至 3）步骤导入 Appliance

4）查看导入的软件

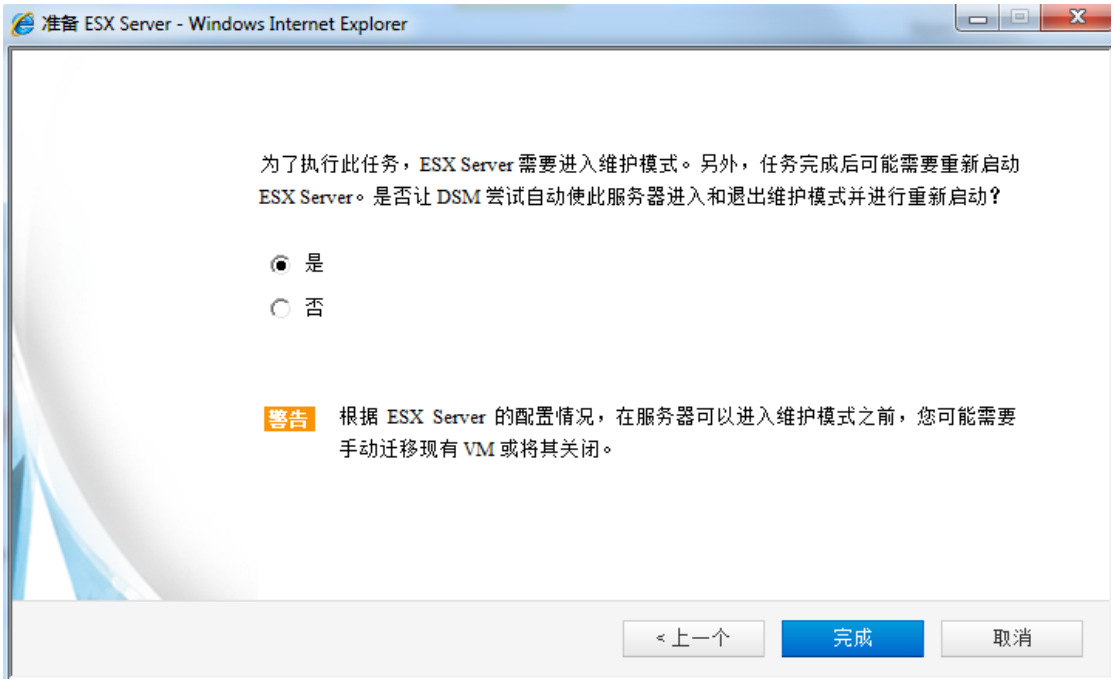


5）在“计算机”列表中找到 ESXi 主机（其状态列应显示为未准备），右键单击它，然后选择操作 > 准备 ESXi 以显示“准备 ESXi Server”向导。单击下一个



注意：ESX 主机会进入维护模式，因为需要安装 Filter 驱动，因此主机上的所有虚拟机都必须要关闭。

6）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 ESXi 进入和退出维护模式，单击完成。



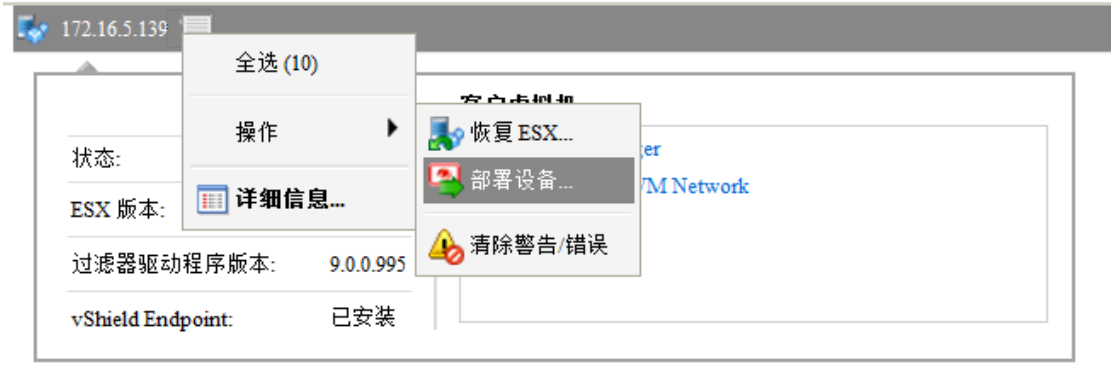
7）ESXi 准备过程将完成所有活动，而无需进一步的输入。(ESXi 将置于维护模式，将安装趋势科技服务器深度安全防护系统过滤器驱动程序，且将重新启动 ESXi。)

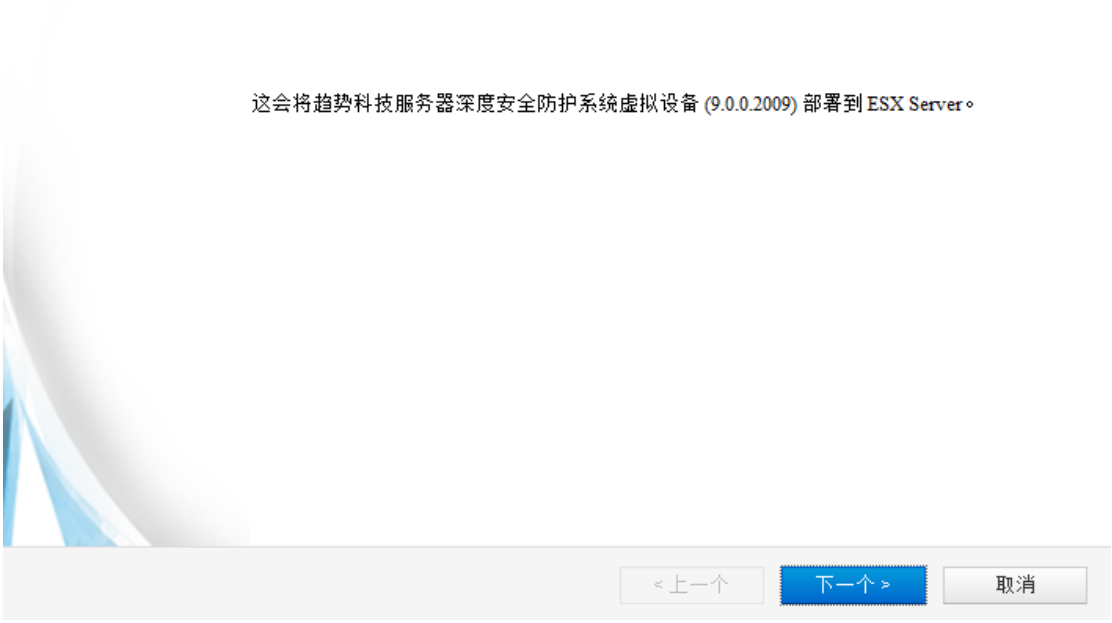
8）该过程完成后，可以选择继续进行下一步，即部署趋势科技服务器深度安全防护系统虚拟设备。选择“不”，稍后部署。单击关闭。

9）确保 ESXi 主机的状态设置为“已准备”

III. 部署 DSVA

1） 右键单击受保护的 ESXi 主机，然后选择操作 > 部署设备，单击下一个。



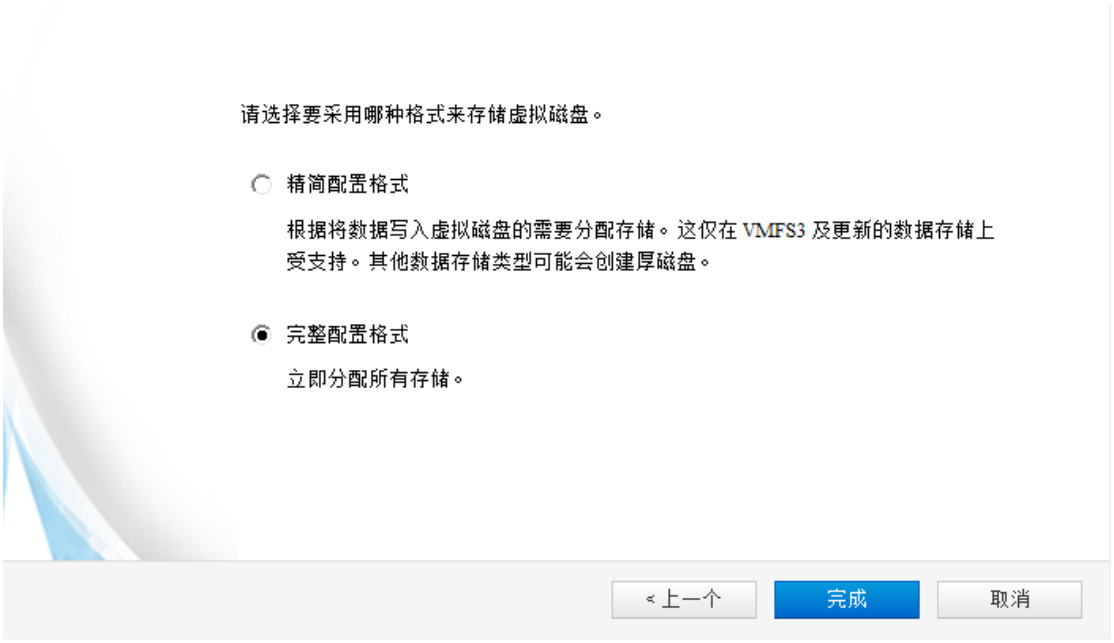


2) 输入设备的“设备名称”并为设备选择数据存储。选择数据中心的文件夹，然后选择设备的管理网络。单击下一个。

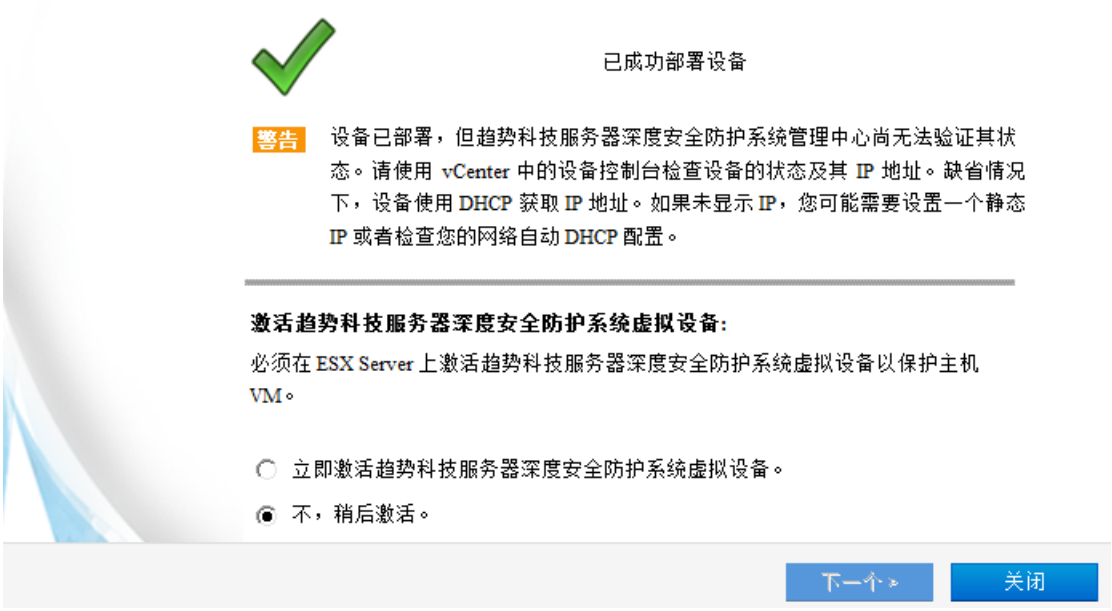
注意：管理网络的连接类型必须为虚拟机，而非 VMkernal

3) 定义设备主机名，输入设备的 IPv4 地址和/或 IPv6 地址。（缺省情况下启用 DHCP）。单击下一个。

4) 选择完整配置格式，单击完成，并等待 DSVA 上传完成。



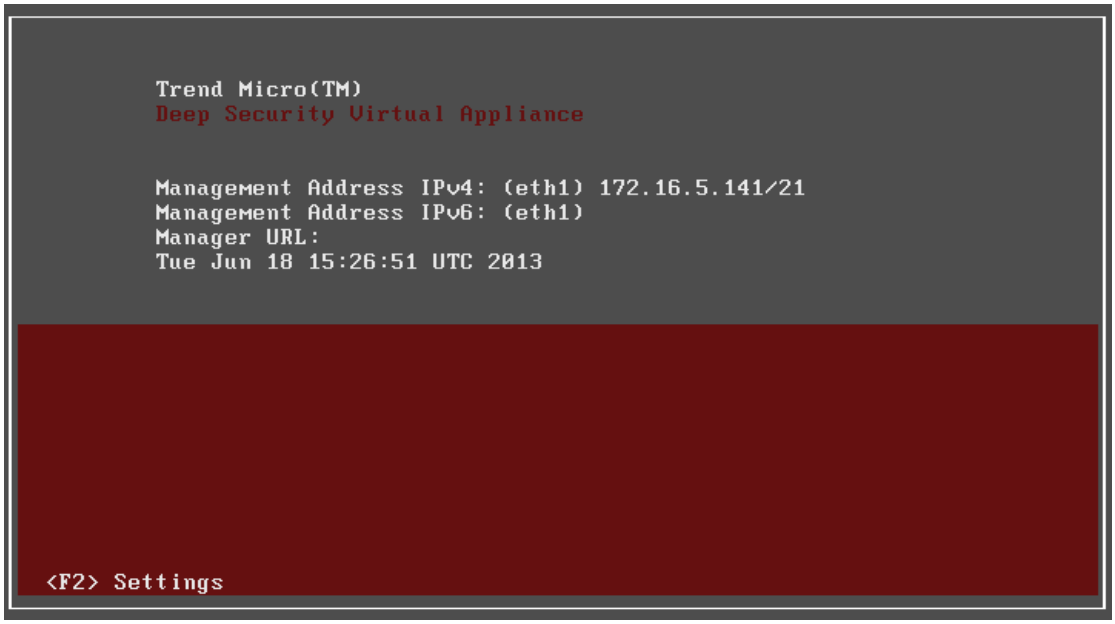
5) 在激活趋势科技服务器深度安全防护系统设备部分中，选择“不，稍后激活。”单击关闭。



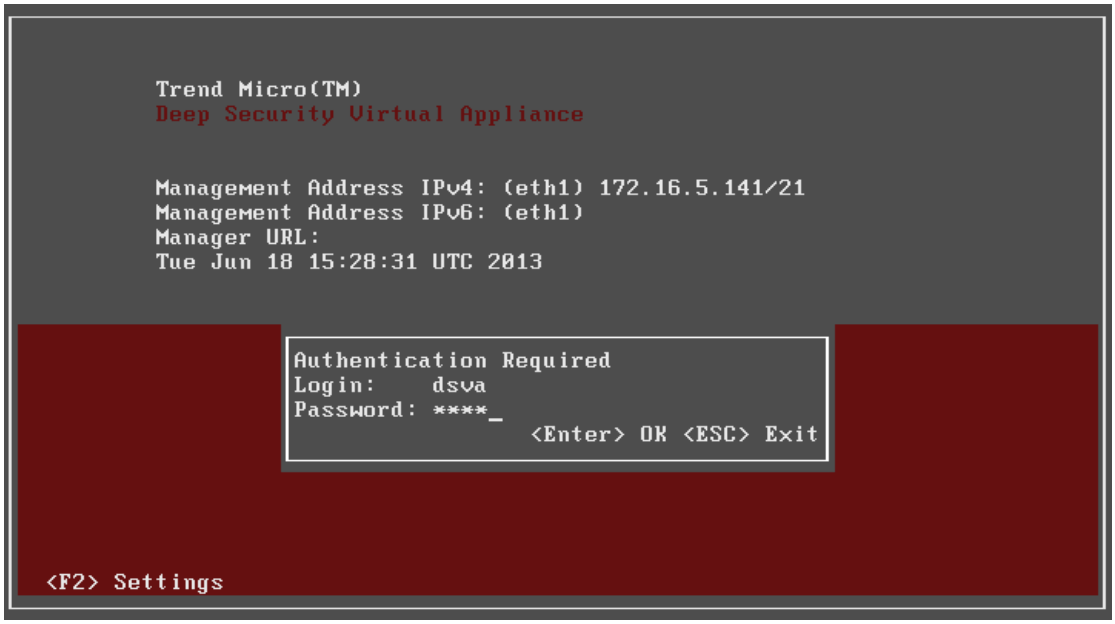
注意：在激活 DSVA 之前，要配置好 DSVA 的各项网络设置，包括 DNS 的解析。
所以请选择“不，稍后激活。”

IV. 设置 DSVA

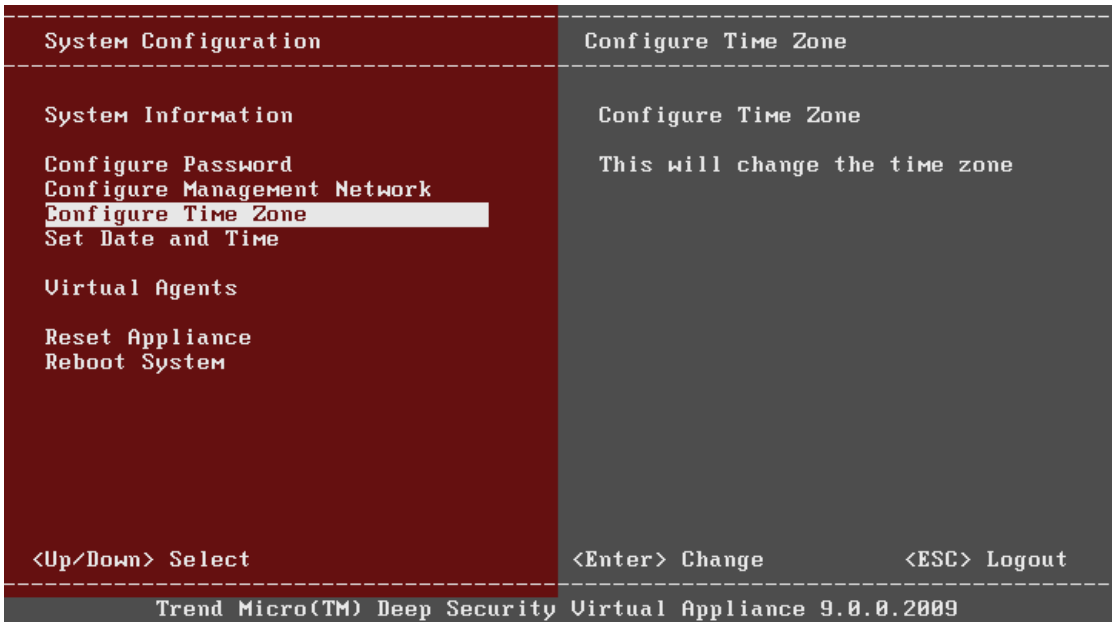
1) 通过 vCenter 的 client 端，登录到 DSVA 虚拟机上。



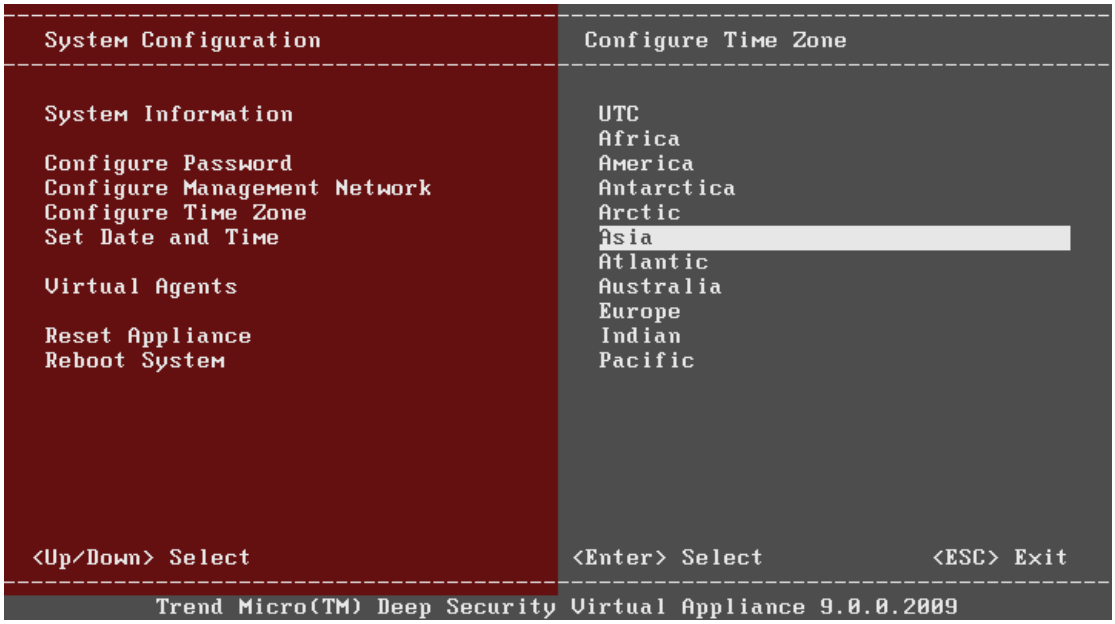
2) 按键盘 F2，进入设置，输入密码 dsva

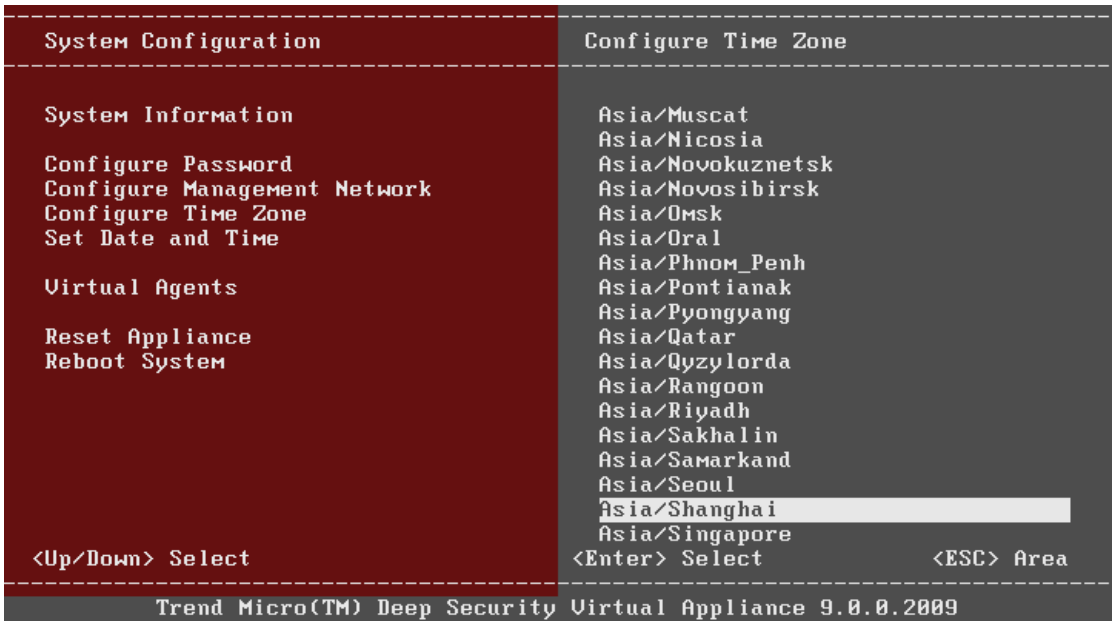


3) DSVA 时区与 DSM 不同步，所以需要配置“Time Zone”，选择“Configure Time Zone”，按回车



4) 首选选择“Asia”,按回车，然后选择“Asia/Shanghai”，再次按回车。

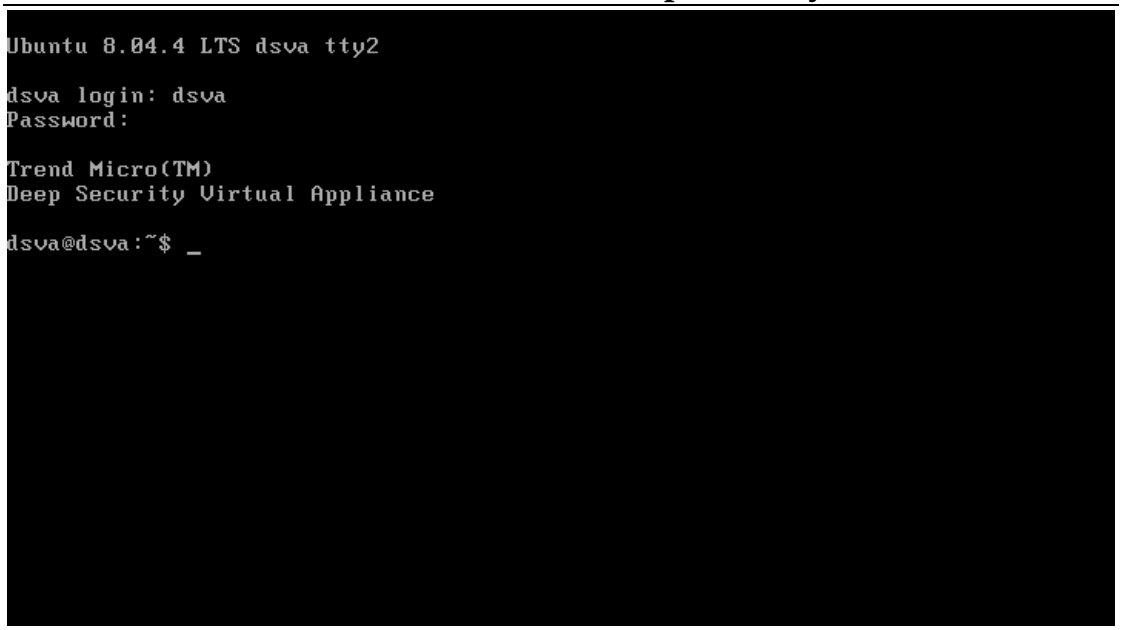




注意：DSVA 的时间必须与 DSM 同步，不然无法激活 DSVA。

5) 在激活前，要确保 DSM 和 DSVA 之前能够正常解析的。如果无法解析或者 DSVA 和 DSM 的时间不对，会造成无法激活。如果没有 DNS，暂时用/etc/hosts 来解析。按 alt+F2 进入命令行模式，按 Alt+F1 返回界面模式。

分别输入帐号和密码进入命令行模式（帐号和密码均为 dsva）



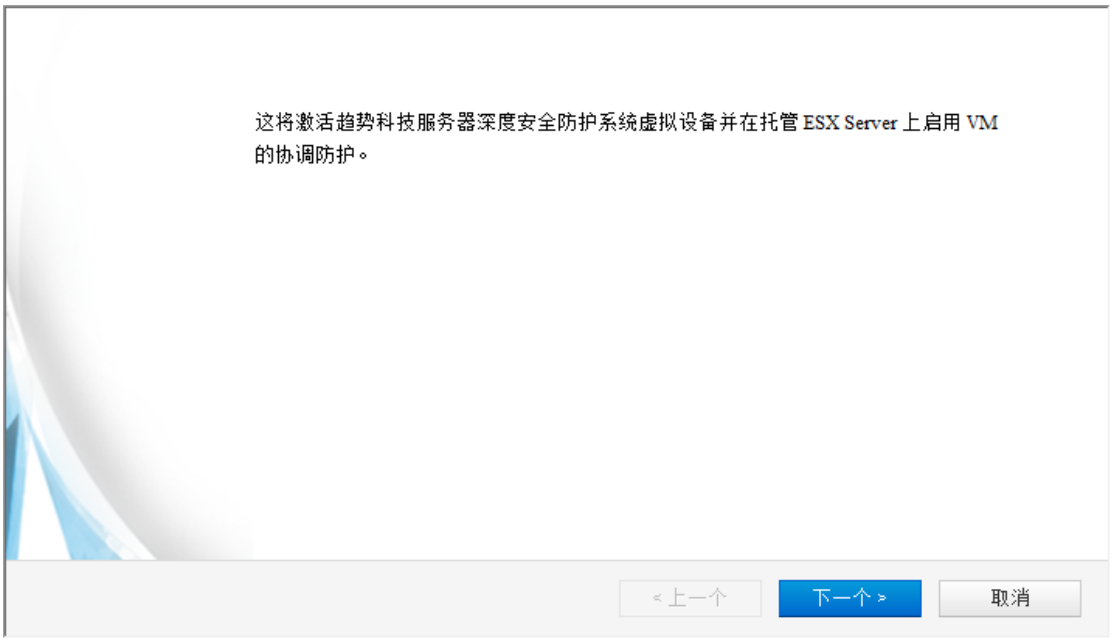
6) 用 root 账号来编辑文件,输入命令：sudo su -

7) 使用命令“vi /etc/hosts” 编辑 DSVA hosts 文件

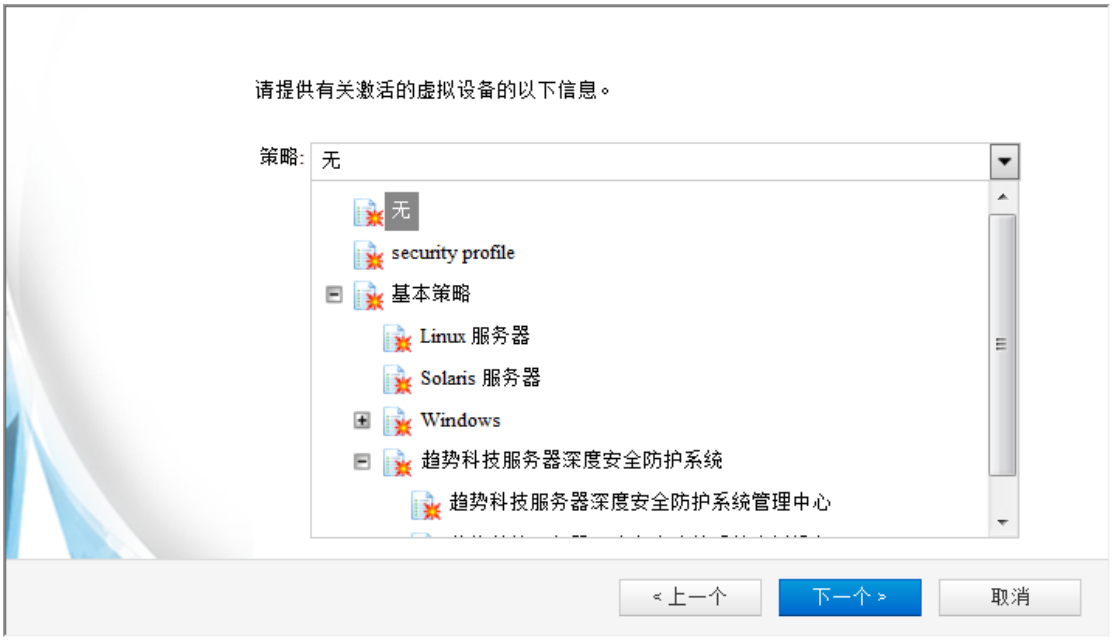
```
dsva@dsva:~$ sudo su -
root@dsva:~# vi /etc/host
host.conf  hostname   hosts
root@dsva:~# vi /etc/hosts_
```

V. 激活 DSVA

1) 右键单击 DSVA 计算机并选择操作 > 激活设备，单击下一个。

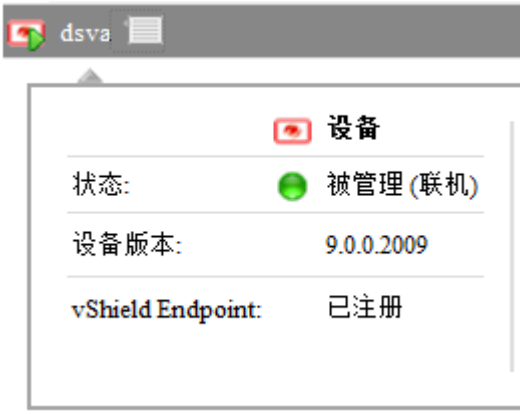


2) 对于策略，建议选“无”。单击下一个，将启动激活过程。



3) 选择是否要激活该 ESX 上的虚拟机。您也可以稍后激活，即使机器关机，也可以激活，单击“完成”完成激活。

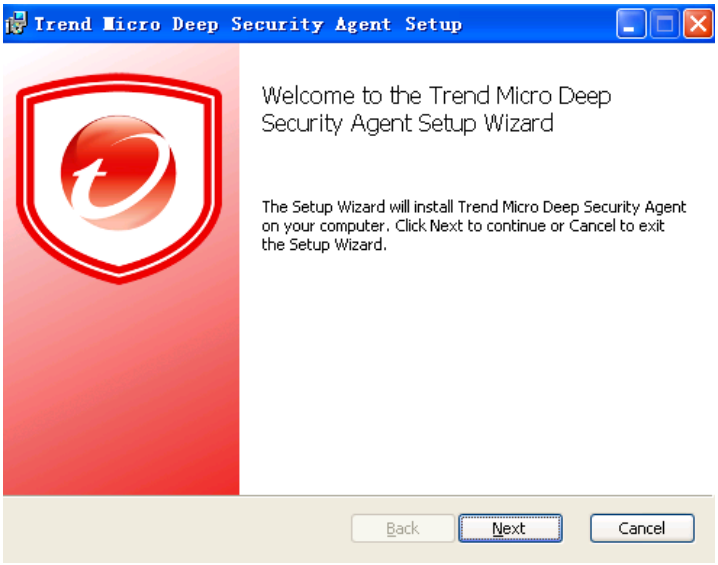
4) 激活后显示状态为“被管理”



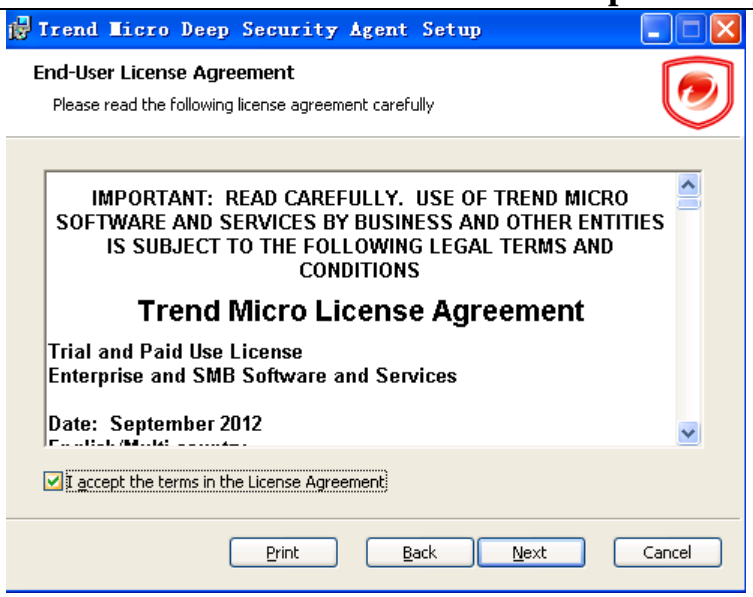
5. Deep Security Agent（DSA）安装

I. DSA For Windows

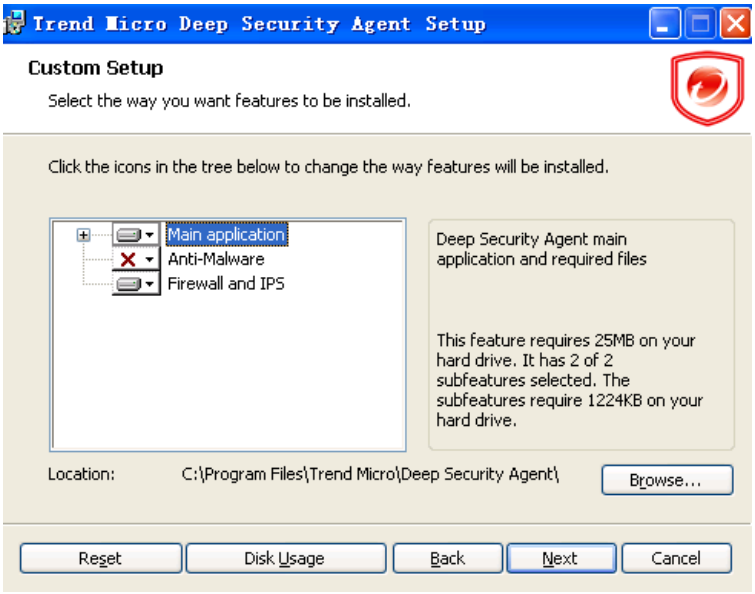
1) 将安装文件复制到目标计算机。
2) 双击安装文件来运行安装包，点击 Next 开始安装。



3) 阅读并接受许可协议并单击 Next。

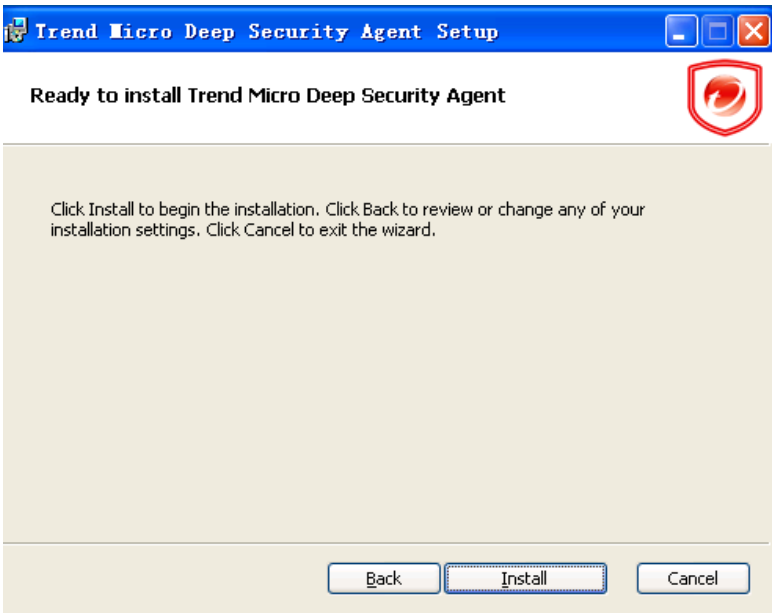


4) 选择要安装的功能（防恶意软件等一些功能是可选的）。单击 Browse 指定要安装趋势科技服务器深度安全防护系统中继的位置。（如果进行升级，则将无法更改安装目录。要安装到其他目录，必须首先卸载先前版本。）单击 Reset 将选择重置为缺省设置。

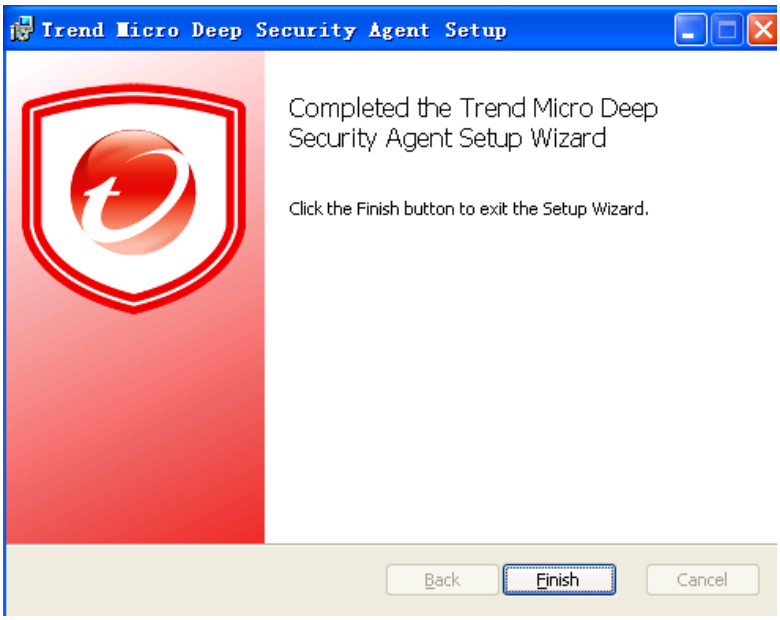


注意：无法取消选择防火墙和入侵防御功能。这些功能构成核心趋势科技服务器深度安全防护系统客户端体系结构的一部分，即使不使用防火墙和入侵防御功能也会始终安装这些功能。单击“Disk Usage”查看选定功能所需的总空间并与选定目位置上的可用空间进行比较。

5) 点击 “Install”开始安装程序



6) 点击“Finish”完成安装



注意：

在执行安装过程中，网络接口会暂时中断几秒。如果您的主机使用 DHCP 方式分配 IP 地址，在连接恢复后产生的新的 DHCP 地址分配请求可能会导致 DSR 被分配一个新的 IP 地址。

不推荐通过远程桌面方式安装 Deep Security Agent，如果需要通过远程桌面方式部署 DSR ，请在远程连接命令后面加上以下参数：

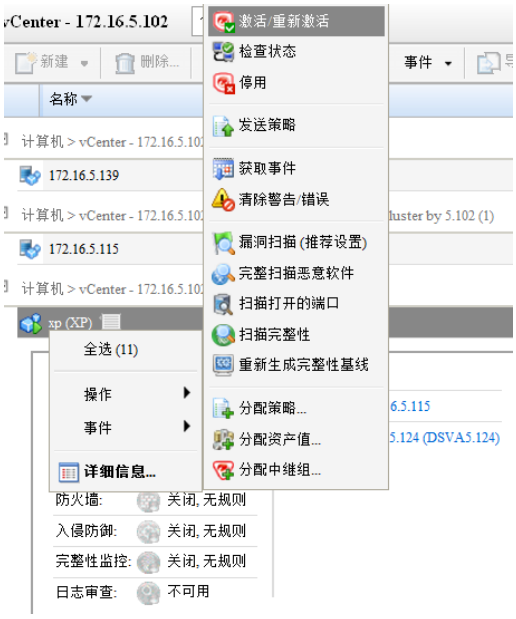
Windows Server 2008，Vista SP1 或 Windows XP SP3 更高版本请使用：

mstsc.exe /admin

更早的 Windows 版本请使用以下命令：

mstsc.exe /console

7） 选中 Agent，然后右键“操作”-“激活/重新激活 ”激活客户端。



8） 客户端被成功激活，在客户端的服务里面也可以看到启动正常

II. DSA For Linux

要求：

部署 Deep Security Agent Linux 版时必须先安装下列版本（更高）的库文件安装包 libstdc++-ssa-3.5ssa-0.20030801.48.i386.rpm，可以使用 yum 或 up2date 来安装这些版本。

安装步骤：

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。

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

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

III. DSA For Solaris

要求：

对于 Solaris Sparc/9：

- libiconv 1.11 或更高版本
- pfil_Solaris_x.pkg
- Agent-Solaris_5.9-9.0.0-xxxx.sparc.pkg.gz

对于 Solaris Sparc/10：

- SUNWgccruntime, GCC Runtime libraries
- pfil_Solaris_10sparc.pkg
- Agent-Solaris_5.10_U7-9.0.0-xxx.x86_64.pkg.gz
- Agent-Solaris_5.10_U5-9.0.0-xxx.x86_64.pkg.gz

对于 Solaris X86/11：

- SUNWgccruntime, GCC Runtime libraries
- pfil_Solaris_10x86.pkg
- Agent-Solaris_5.11-9.0.0-xxx.i386.p5p.gz

对于 Solaris SPARC/11：

- SUNWgccruntime, GCC Runtime libraries
- pfil_Solaris_10x86.pkg
- Agent-Solaris_5.11-9.0.0-xxx.sparc.p5p.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 11 客户端：

1. 获取所需的所有软件包
2. 将安装文件复制到目标计算机
3. 安装客户端：

gunzip Agent-Solaris_5.x_sparc-9.x.x-xxxx.sparc.p5p.gz
pkg install -g Agent*p5p ds-agent
svcadm enable ds_agent

安装 Solaris 10 客户端：

1. 获取所需的所有软件包（请参阅前述内容）
2. 将安装文件复制到目标计算机
3. 安装客户端：

gunzip Agent-Solaris_5.10_U7-9.0.0-xxx.x86_64.pkg.gz
pkgadd -d Agent-Solaris_5.10_U7-9.0.0-xxx.x86_64.pkg all

安装 Solaris Sparc 9 客户端：

1. 获取所需的所有软件包
2. 将安装文件复制到目标计算机
3. 安装 libiconv-1.8-solx-sparc.gz：

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

4. 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

5. 安装 pfil：

pkgadd -d pfil_Solaris_x.pkg all

6. 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。
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

7. 安装客户端：

gunzip Agent-Solaris_5.x_sparc-9.x.x-xxxx.sparc.pkg.gz
pkgadd -d Agent-Solaris_5.x_sparc-9.x.x-xxxx.sparc.pkg all

在 Solaris 10 和 11 上启动、停止和重置客户端：

- svcadm enable ds_agent - 启动客户端
- svcadm disable ds_agent - 停止客户端
- /opt/ds_agent/dsa_control -r - 重置客户端
- svcadm restart ds_agent - 重新启动客户端

- svcs -a | grep ds - 显示客户端状态

在 Solaris 9 上启动、停止和重置客户端：

- /etc/init.d/ds_agent start - 启动客户端
- /etc/init.d/ds_agent stop - 停止客户端
- /etc/init.d/ds_agent reset - 重置客户端
- /etc/init.d/ds_agent restart - 重新启动客户端

注意：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://downloadcenter.trendmicro.com/?regs=CH。

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)

IV. DSA For AIX

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：

1. 以 Root 身份登录
2. 将软件包复制到临时文件夹 ("/tmp")
3. 使用 gunzip 解压软件包：
   /tmp> gunzip Agent-AIX_x.x-x.x.x-x.powerpc.bff.gz
4. 安装客户端：
   /tmp> installp -a -d /tmp ds_agent

在 AIX 上启动客户端：
startsrc -s ds_agent
在 AIX 上停止客户端：
stopsrc -s ds_agent
在 AIX 上加载驱动程序：
/opt/ds_agent/ds_fctrl load
在 AIX 上退出驱动程序：
/opt/ds_agent/ds_fctrl unload +

V. DSA For HP-UX:

1. 以 Root 身份登录
2. 将安装文件复制到目标计算机
3. 将软件包复制到临时文件夹 ("/tmp")
4. 使用 gunzip 解压软件包：
   /tmp> gunzip Agent-HPUX_11.31-9.0.0-xxx.ia64.depot.gz
5. 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_11.31-9.0.0-xxx.ia64.depot

ds_agent

要在 HP-UX 上启动和停止客户端，请输入以下命令之一：

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

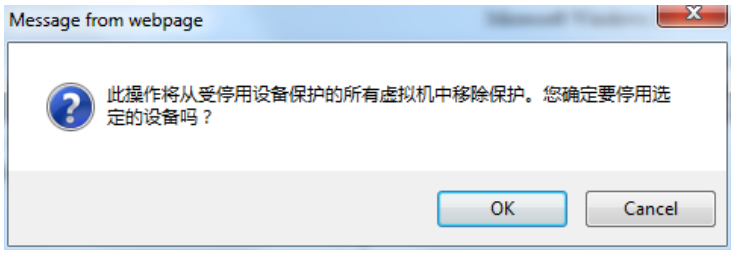
六、 卸载Deep Security

1. 移除Deep Security Virutal Appliance(DSVA)

1）登录Deep Security Manager控制台：

2）找到之前安装的DSVA的虚拟机，右键“操作”，选择“停用设备”选项以解除激活。

3）点击“OK”,停用设备。

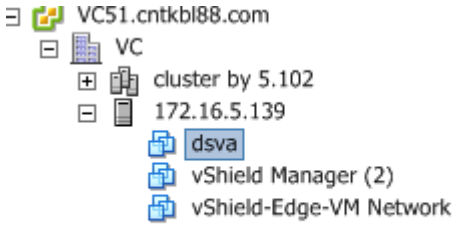


4）DSM会自动去解除DSVA的激活。

注意：如果之前有安装过vShield Manager模板，并让DSVA启用了vShieldManager，在取消激活DSVA之前，请保留vShield Manager，并让vShield Manager虚拟机启动着。否则，在解除激活的时候，会收到无法联机vShield Manager的报错。

5）如下状态表示解除成功。

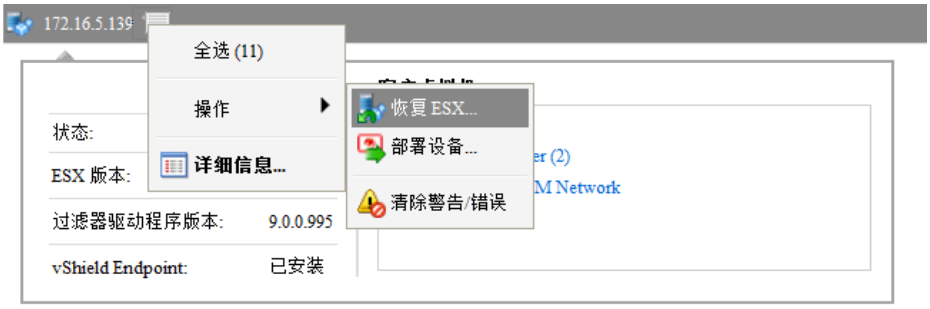
6） 登录vCenter Server，停止DSVA的运行。



7） 从磁盘删除DSVA。

2. 还原ESXi主机并卸载Deep Security Filter Driver

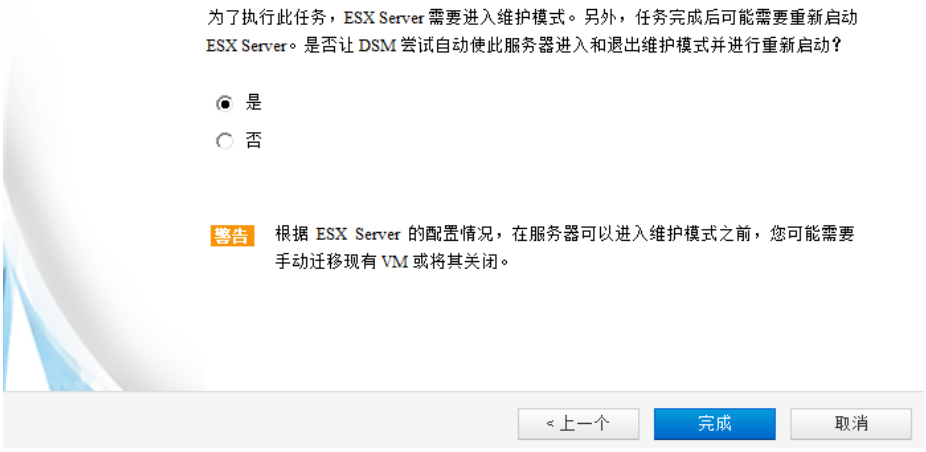
1） 选择需要还原的 Prepared ESX 主机，右键“操作”，选择“恢复 ESX”，然后点击“下一个”。



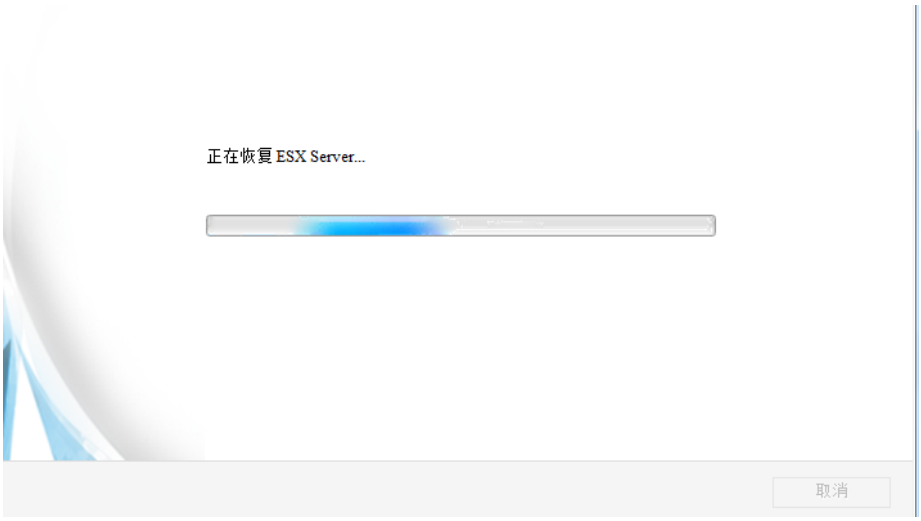
注意：再还原ESX的时候需要把把该主机上面的所有虚拟机都手动关机掉。因为在还原ESX的时候，会自动进入Maintenance模式。在恢复阶段的最后，ESX会自动重启并跳出Maintenance模式。

2） 点击“下一个”

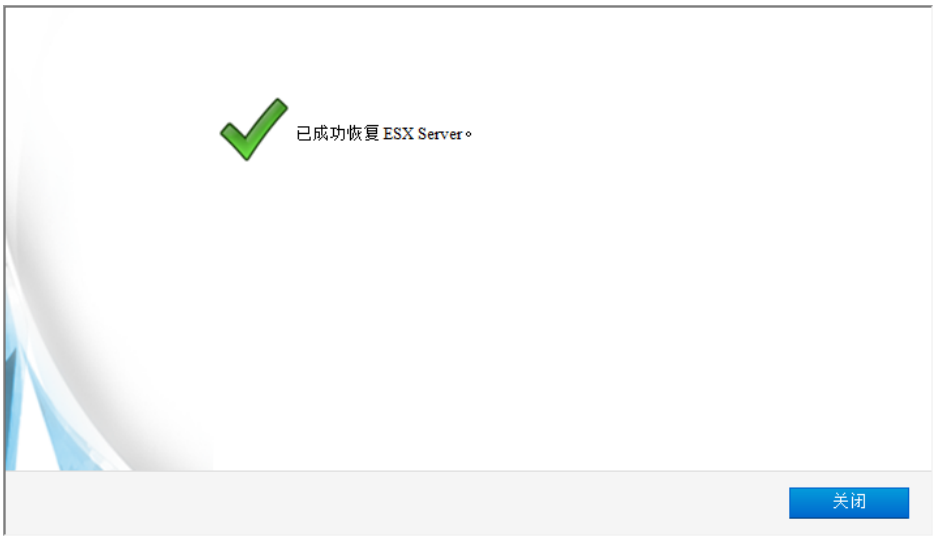
3) 提示自动进入维护模式，点击“完成”。



4) 开始恢复，并自动重启 ESX 主机。



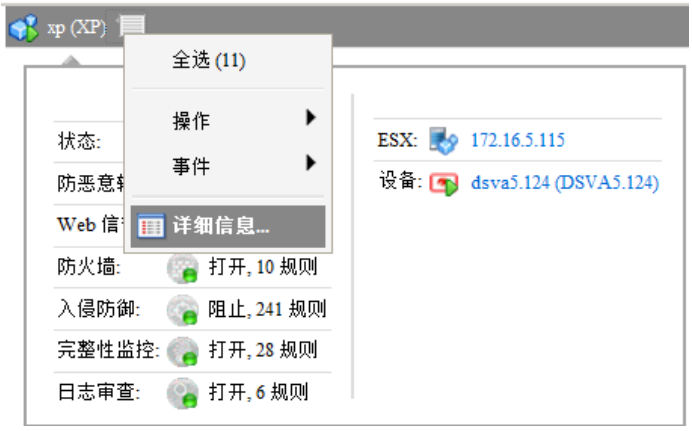
5） 如下图显示还原成功，点击“关闭”

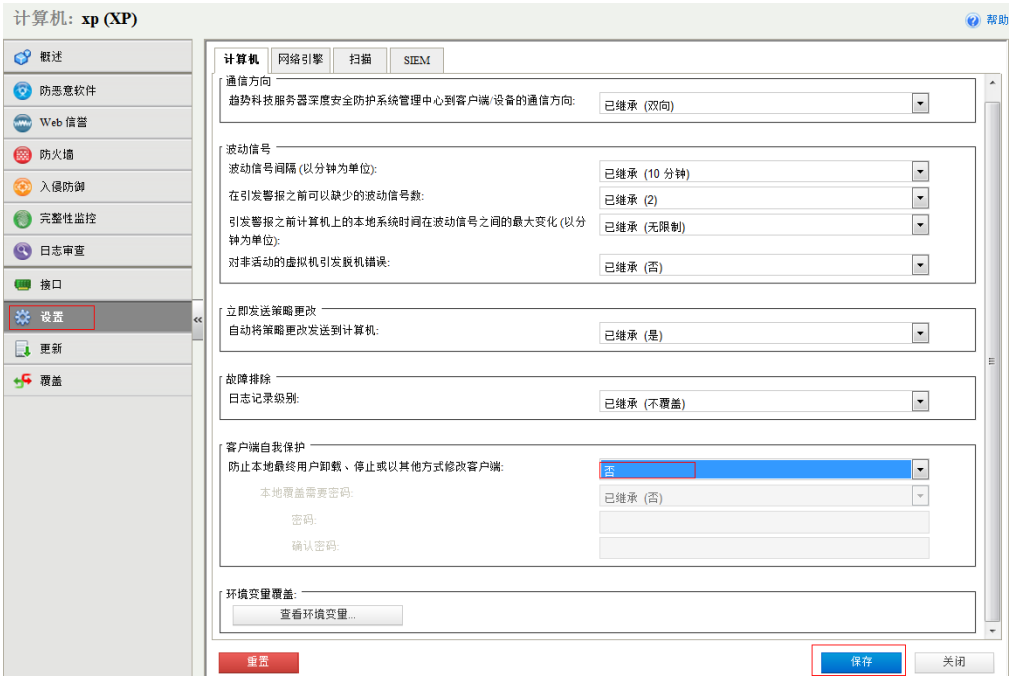


6） 再次在 DSM 上检查 ESX 主机，如果状态显示为“未准备”，表示 DSVA 的卸载完全成功。

3. 卸载DSA

注意：执行卸载DSA 操作以前请先进入进入目标主机的详细信息页面，取消自我保护设定





1） 卸载DSA for Windows，可以从添加/删除程序里面把Trend Micro Deep Security Agent给直接删除掉。

也可以在MS-DOS命令运行如下：

msiexec /x <package name including extension>

提醒：（对于静默卸载，请添加 "/quiet"）

2） 卸载DSA for Linux，可以使用如下命令：

```
# rpm -ev ds_agent
Stopping ds_agent: [ OK ]
```

```
Unloading dsa_filter module [ OK ]
```

注意：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。

3） 卸载DSA For Ubuntu，可以使用如下命令：

```
$ sudo dpkg -r ds-agent
Removing ds-agent...
Stopping ds_agent:.[OK]
```

4） 卸载DSA for Solaris，可以使用如下命令：

```
pkgrm ds-agent
```

注意：卸载可能需要重新启动。

5） 卸载DSA for AIX，可以用如下命令：

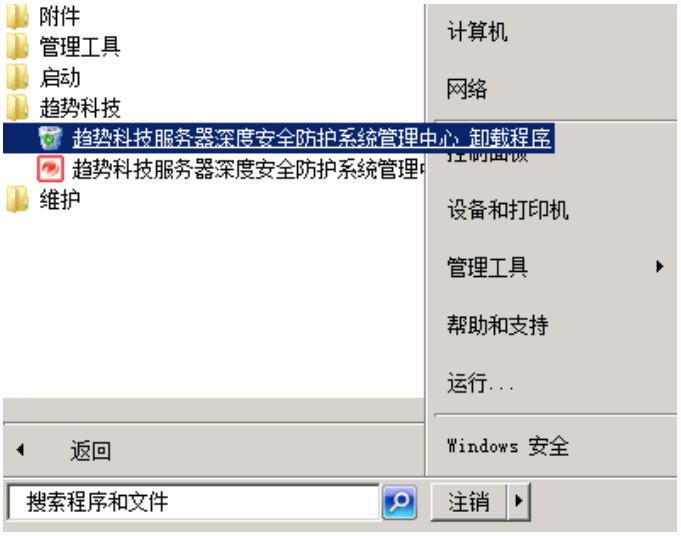
```
installp -u ds_agent
```

6） 卸载DSA for HP-UX，可以使用如下命令：

```
swremoveds_agent
```

4. 卸载DSM

卸载DSM，只需在快捷方式里面点击卸载程序即可

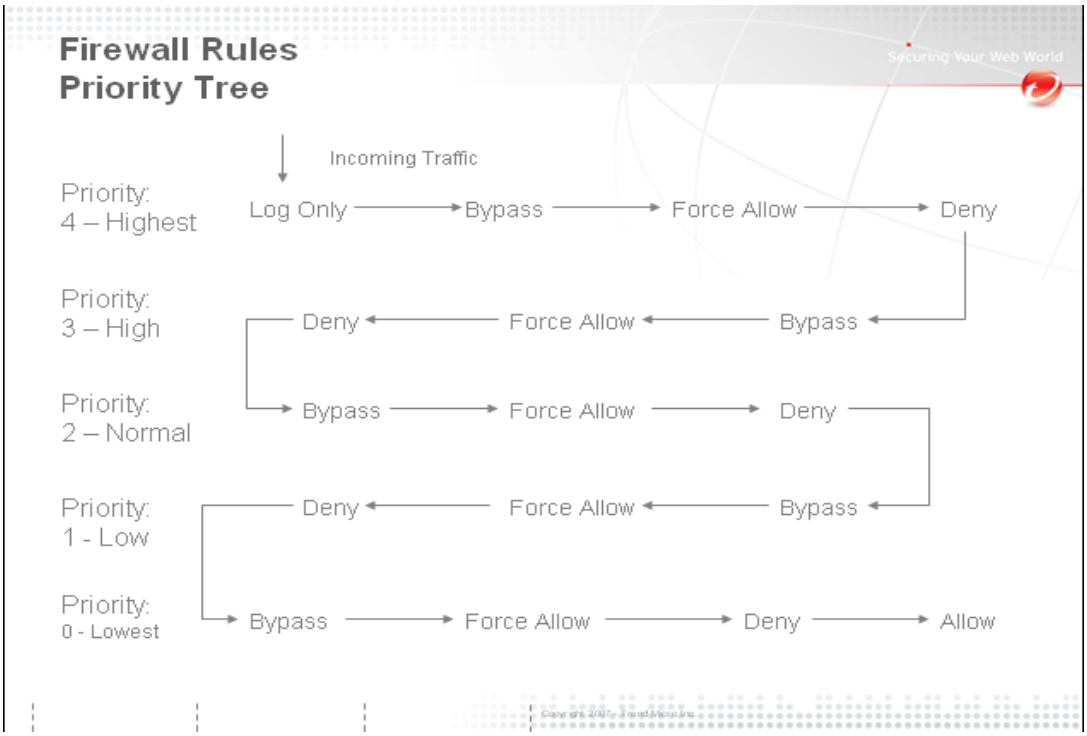


七、 Deep Security 的基本配置

1. 防火墙

主要作用：

针对不同的系统，设置不同的防火墙策略，阻挡不必要的网络流量，保证网络的安全。



当有数据包经过客户端时，数据包会按照“43210”的顺序通过防火墙策略，Priority相同的情况下，根据Action的优先级不同决定策略的执行先后顺序。

策略原则：

A.每个Priority都有Bypass，Force Allow，Deny三个Action，顺序也相同

B.Log Only只有在Priority Highest的时候才有，Allow只有在Priority Lowest的时候才有

C.什么策略都不部署的时候，其实是Allow All

D.Bypass和Force Allow的区别是Bypass除了放行该流量，还会使得该流量通过DPI的检测

E.Force Allow和Allow的区别，Allow=Allow+Deny All，Force Allow只是让该策略的流量通过防火墙检测

F.如果选择了Priority Lowest的Allow Action，意味着除了这条策略的的行为Allow外，其他的通信都Deny，可以注意到Allow已经在整个数据流的最后一个

测试注意事项：

1) 不要轻易部署 Priority Lowest 里面 Action 为 Allow 的策略，因为这样意味着除了之前 Bypass 和 Force Allow 和本策略 Allow 的流量外，其他的流量均被 Deny，会造成断网的情况
2) 防火墙策略有方向性，建议部署 incoming 策略的时候，Source Port 设置为 ANY，Destination Port 设置特定的端口，Outgoing 策略的时候 Source Port 设置为特定的端口，Destination Port 设置为 ANY
3) 不建议用 ICMP 进行测试，因为 ICMP 包有回包，例如在 172.16.4.66 这台客户端上设置了 incoming 的 ICMP 包为 Deny，其实其他客户端 ping 不通 172.16.4.66 的同时，172.16.4.66 也无法 ping 通其他的客户端

测试建议：

1) 建议选择 Action 为 Deny 的策略进行测试，这样能看到效果
2) 建议在 Priority Highest 的 level 里面设置一条 outgoing http bypass 的策略，因为如果设置的防火墙和 DPI 策略比较多的话，会导致上网等一些正常的应用变得比较缓慢

2. 入侵防御

主要作用：

该功能对一些恶意攻击进行特征码的匹配，利用策略的部署对受保护的客户端能起到虚拟补丁的保护作用

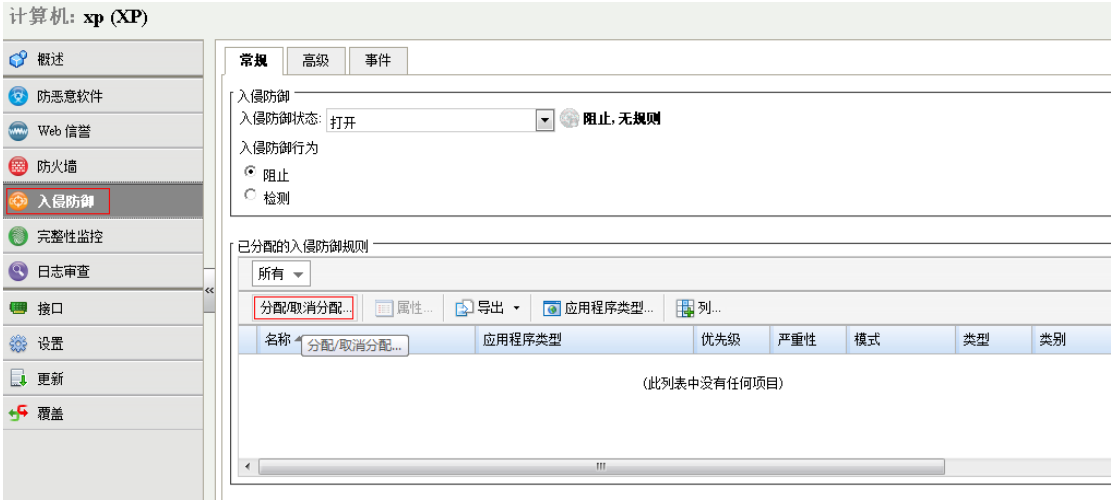
如何筛选rule

在入侵防御设置页面，点击“分配/取消分配”，在弹出的规则页面中，选择“高级搜索页面”，然后选择Microsoft，在后面输入漏洞编号，如08-067，便可以筛选出和这个补丁相关的入侵防御策略。

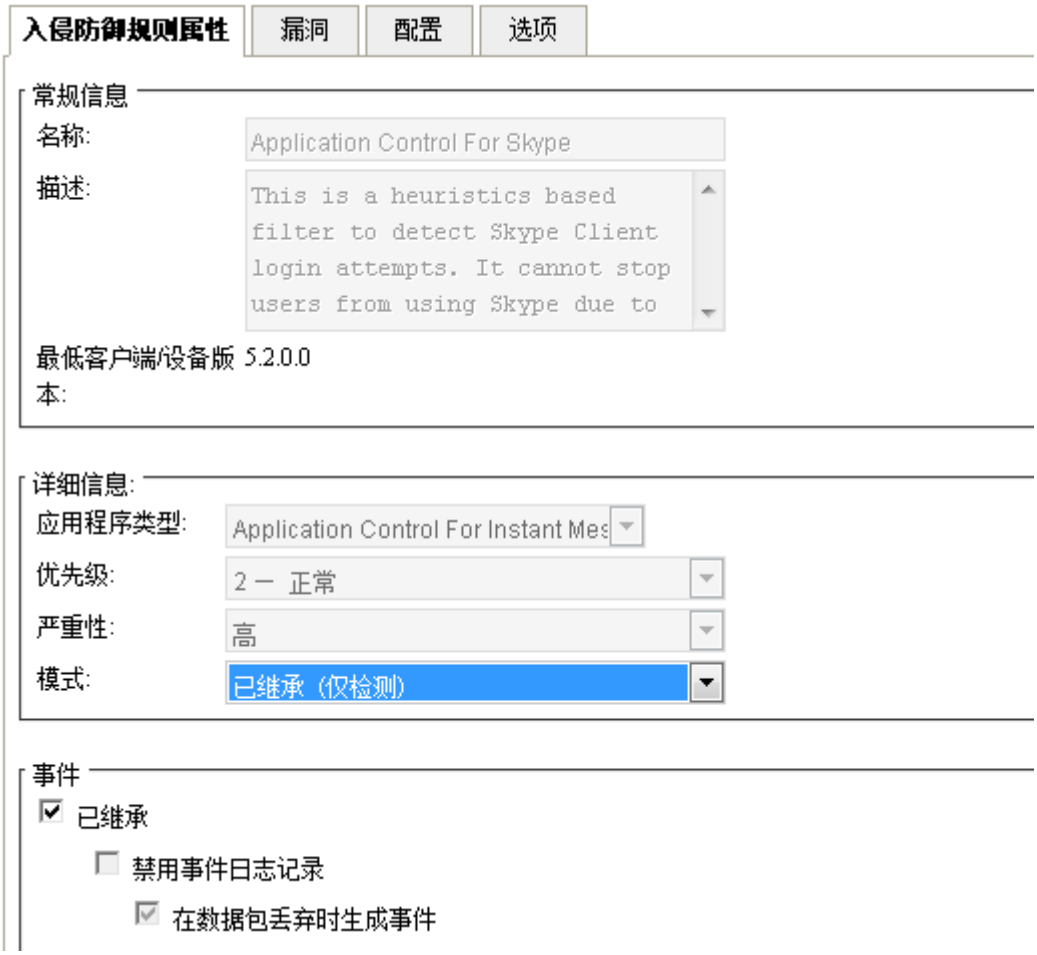
使用方法：

1）进入目标主机的详细信息页面

2）在“入侵防御”页面，点击“分配/取消分配”



3）例如选择“1002159”，在前面打钩，然后双击该策略



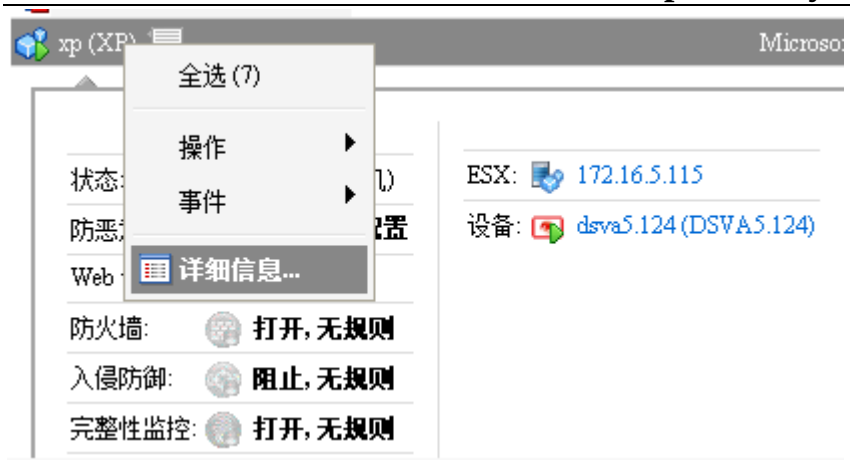
4）默认情况该策略是无法调整优先级和严重性。我们可以设置事件的记录规则和操作。例如不选择“仅检测”，那么当发现 skype 有漏洞的时候，会阻止网络数据包。如果选择“仅检测”，那么只是做记录，不会阻止 skype。

3. 完整性监控

功能描述：任何恶意事件的发生都会伴随着文件或注册表、服务进程的改变，Deep Security 完整性监控模块可监控关键的操作系统和应用程序文件（如目录、注册表项键值）以及服务进程的变化，用以检测可疑行为。

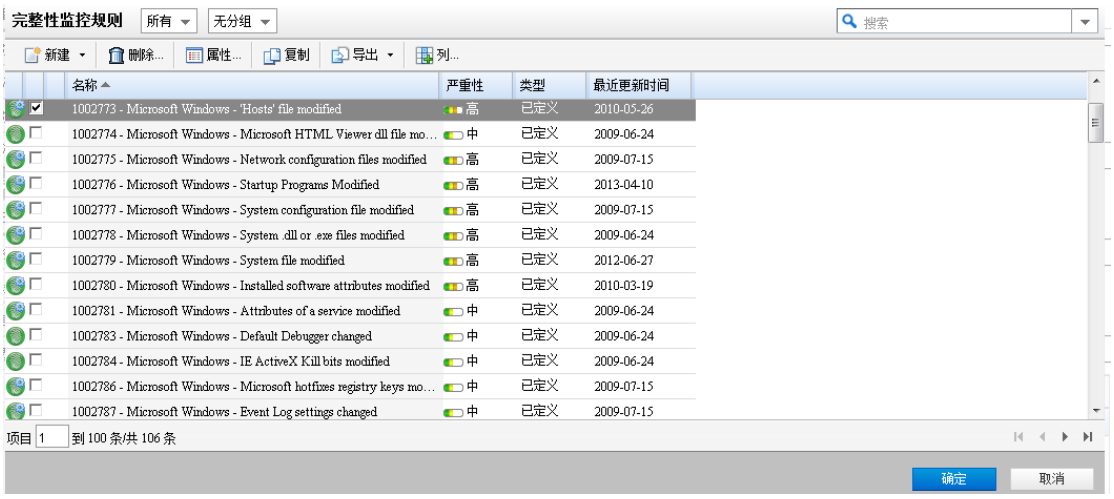
使用预设的完整性检查规则可对文件和目录针对多方面的更改进行监控，包括：内容、属性（如所有者、权限和大小）以及日期与时间戳。还可监控对 Windows 注册表键值、访问控制列表以及日志文件进行的添加、修改或删除操作，并提供警报。此功能适用于 PCI DSS 10.5.5 要求。

1）进入目标主机的详细信息页面

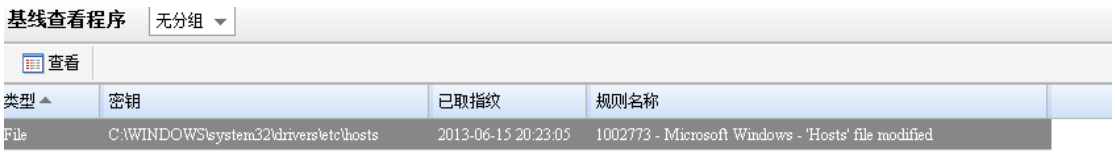


2）在“完整监控性”页面，点击“分配/取消分配”

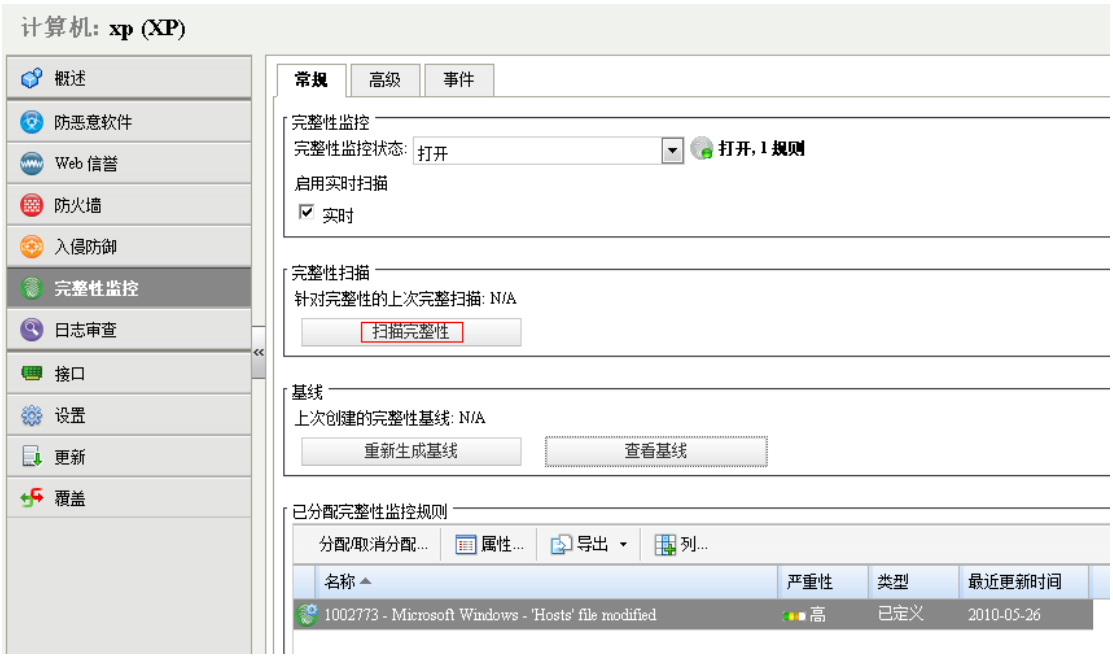
3）选中”1002773-Microsoft Windows –“Hosts”file modified”，点击“确定”



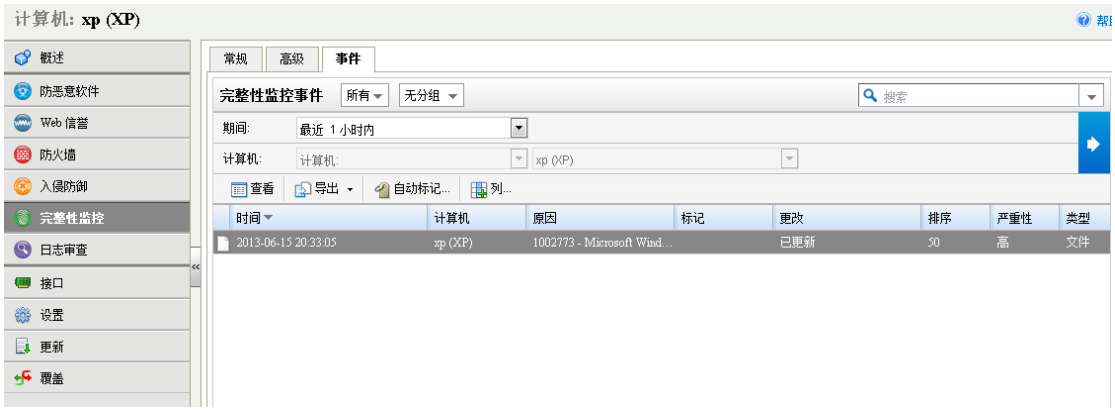
4）返回“完整监控性”页面，点击“查看基线”检查基线是否存在，如果不存在执行“重新生成基线”



5）进入目标计算机修改 hosts 文件，然后运行“扫描完整性”命令



6）在“事件页面”检查事件情况

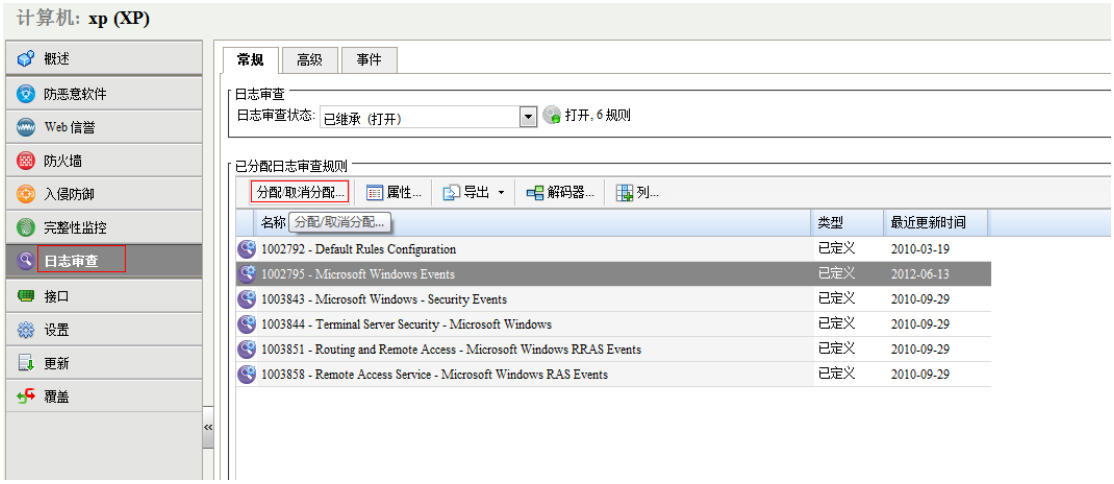


4. 日志审核（Log Inspection）

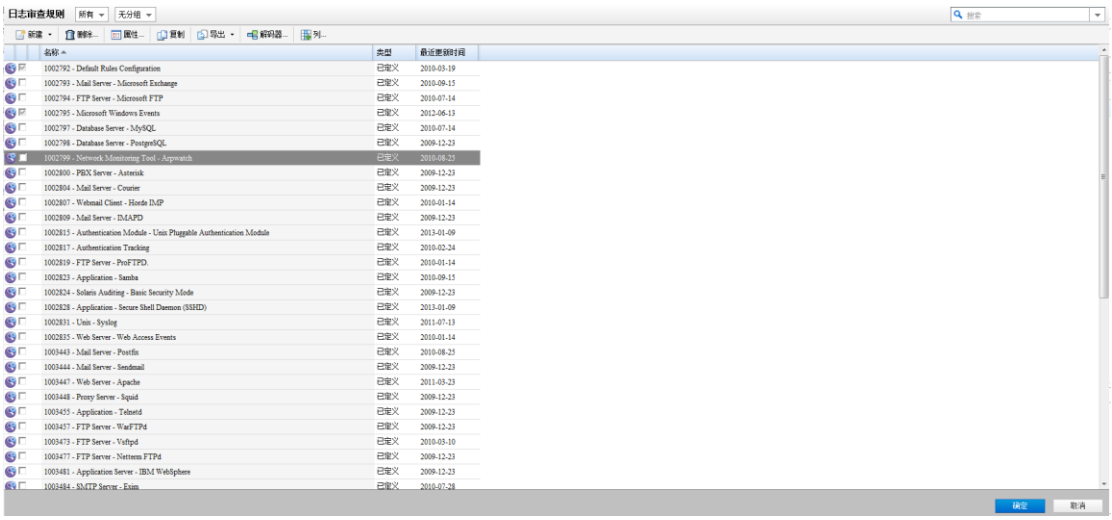
功能描述：对于管理大量服务器的管理员来讲，如何在海量的日志信息中发现威胁，是个费时费力的事情；使用 Deep Security 日志审计模块可收集并分析操作系统和应用程序日志，以查找安全事件。日志审计规则优化了对多个日志条目中隐藏的重要安全事件进行识别的能力。

1）进入目标主机的详细信息页面

2）在“日志审查”页面，点击“分配/取消分配”



3）勾选需要部署的规则，点击“确定”



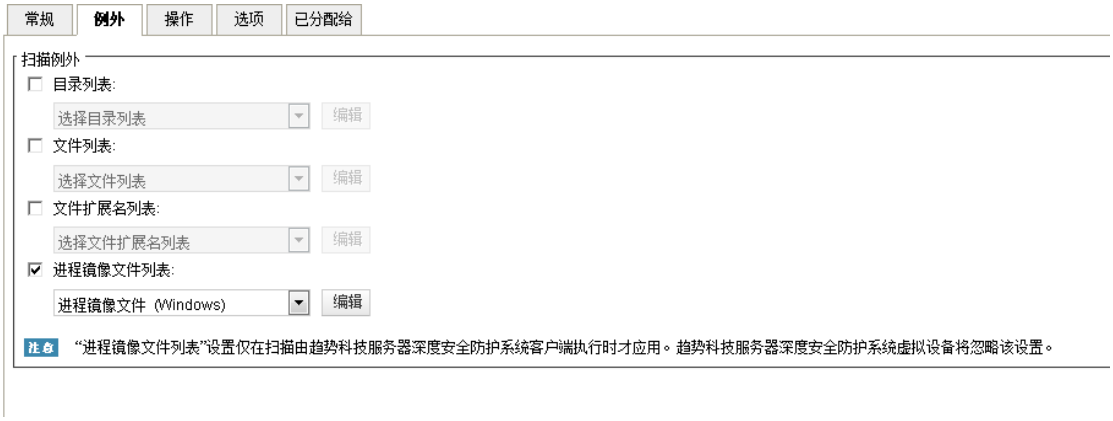
5. 启用病毒保护功能

1） 进入目标主机的详细信息页面

2） 选择“缺省的实时扫描配置”，点击“编辑”

A. 设置扫描的名称、扫描的文件和目录

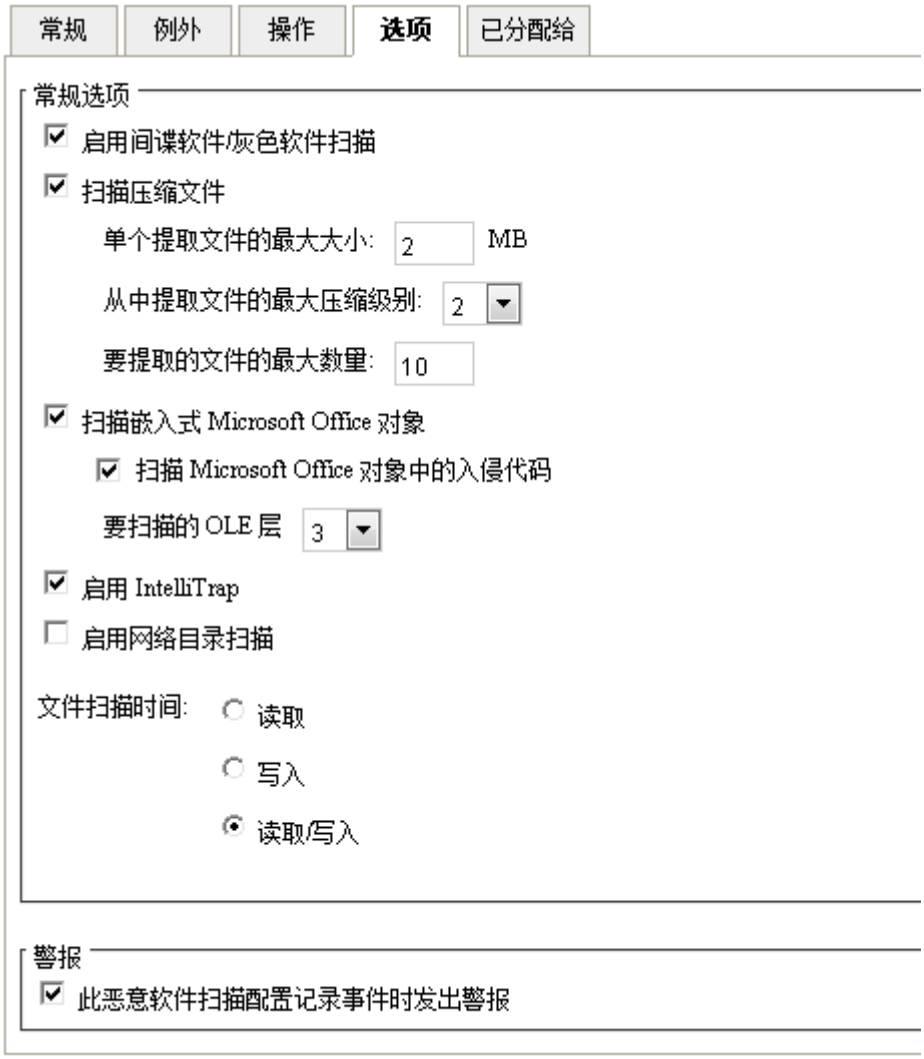
B. 设置例外的文件和目录



C. 设置操作


常规
例外
操作
选项
已分配给
可识别的恶意软件
检测时:
使用 ActiveAction 确定的处理措施
定制处理措施:
对于病毒:
清除
对于特洛伊木马:
隔离
对于加壳软件:
隔离
对于间谍软件:
隔离
对于其他威胁:
清除
可能的恶意软件
检测时:
缺省

D. 选项的修改



3） 预设扫描、手动扫描的配置和实时扫描配置类似

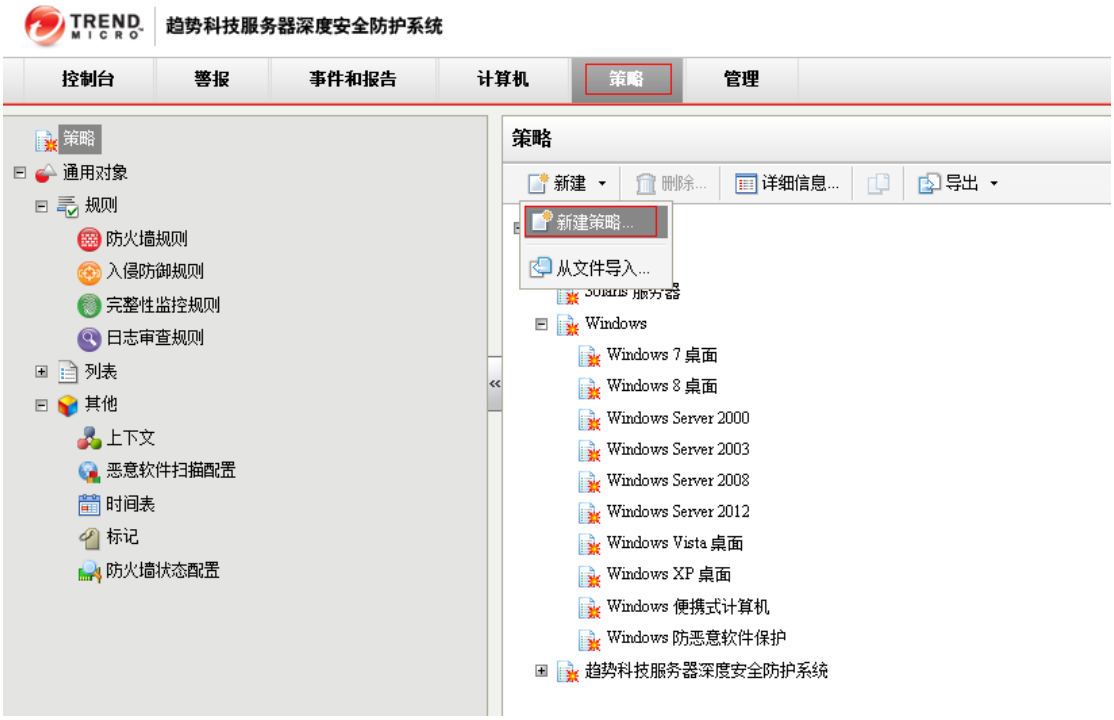
6. 策略的设置和分配

本节将重点介绍策略的配置和分配给具体的计算机。

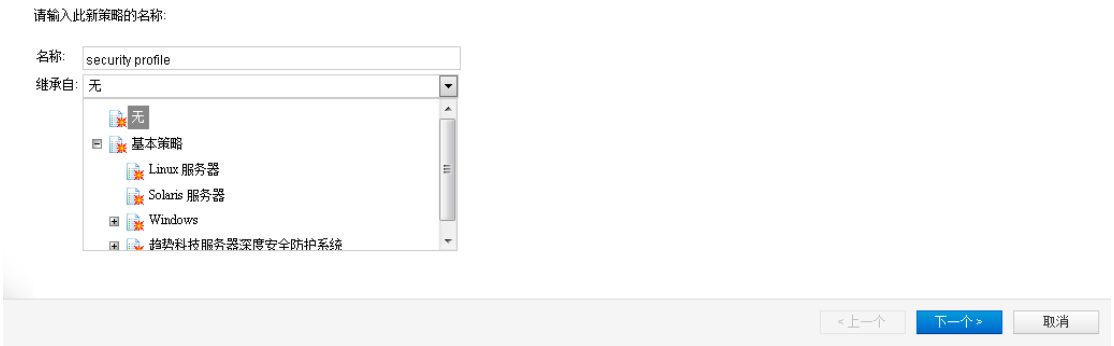
要有效使用Deep Security，建议设置策略，策略把各个模块的策略涵盖和统一。方便统一部署到虚拟机上。

创建一个全新的策略：

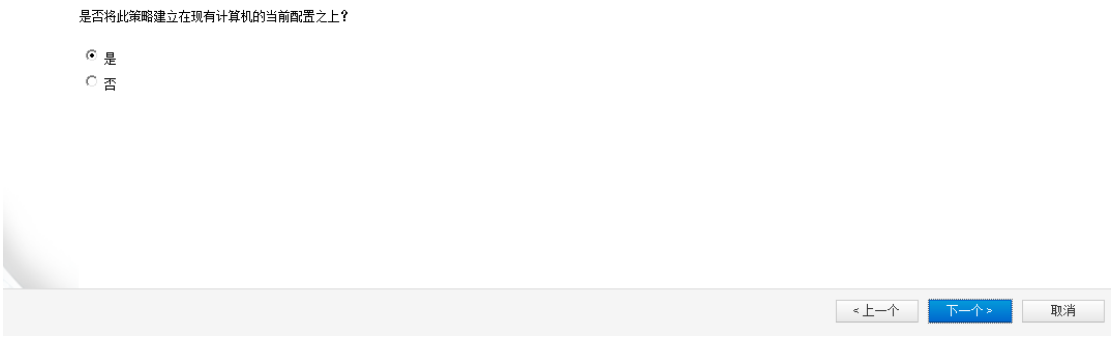
1） 点击“策略”选项开，在策略页面点击“新建—新建策略”



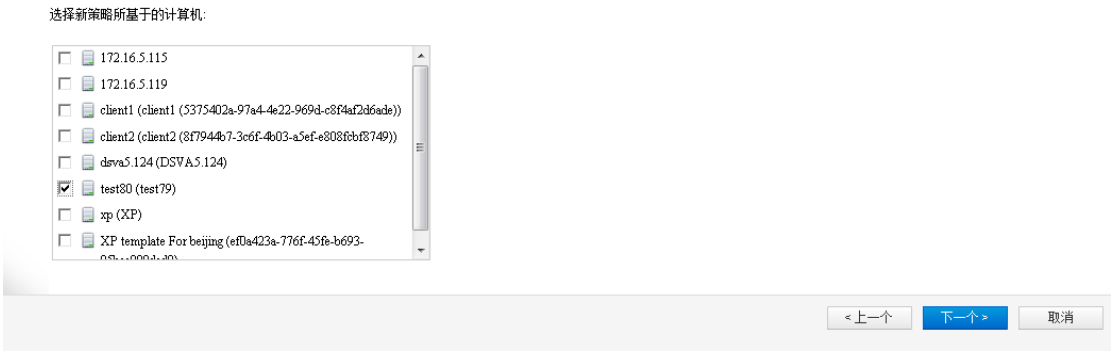
2） 输入策略名，例如securirty profile,同时选择是否继承已有的策略



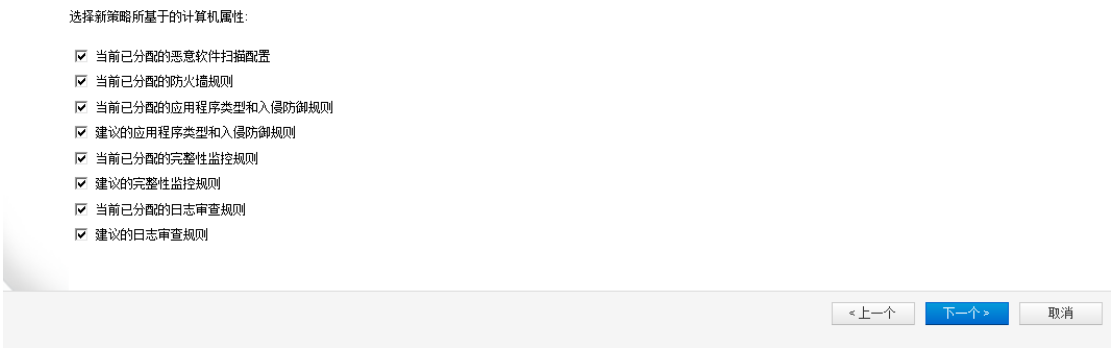
3） 选择是否要分配到现有的计算机



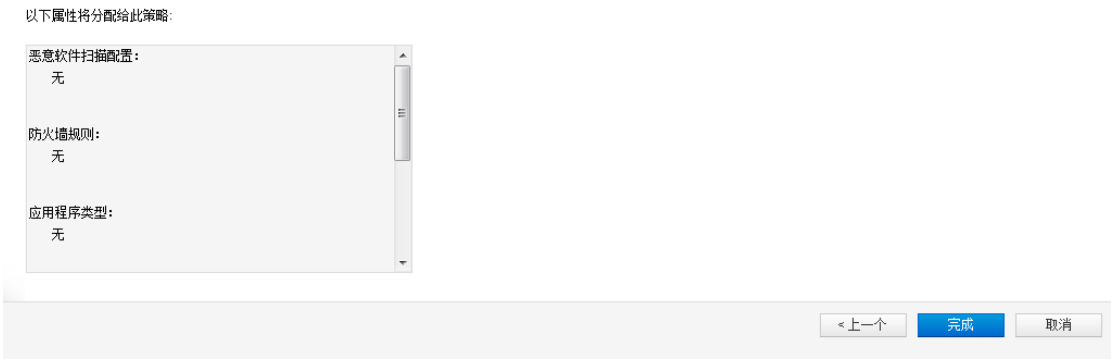
4） 如点击“是”，如图选择计算机



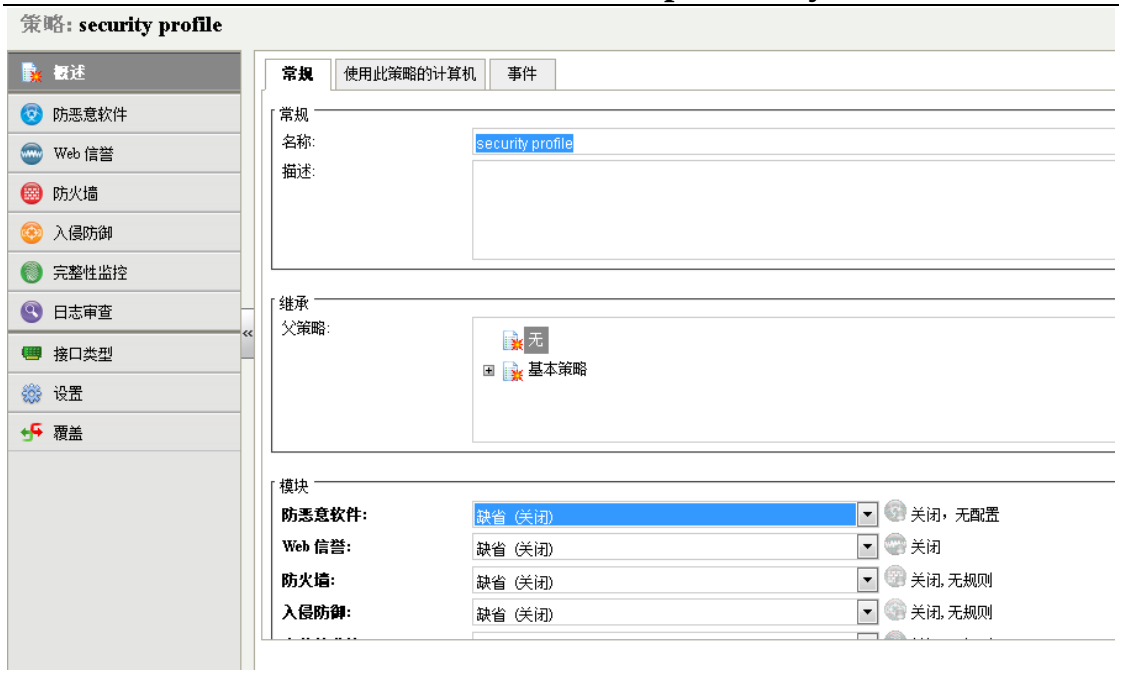
5） 选择策略所基于的计算机属性



6） 策略创建完毕



7） 根据之前设置各个模块策略和规则的方法，设置这个策略文件里面的各模块。其中包括：防恶意软件、Web信誉、防火墙、入侵防御、完整性监控、日志审查等。



分配策略：

1） 选择一台计算机，如图

2） 右键，选择“操作”-“分配策略”

3） 点击“确定”，如下图，此虚拟机运用了这个概要文件

7. 列表配置

点击“列表”。如图：

列表的定义： IP列表、MAC列表、文件列表、文件扩展名列表、目录列表、端口列表。

1） IP列表

把不同的IP段划分到一个列表中。

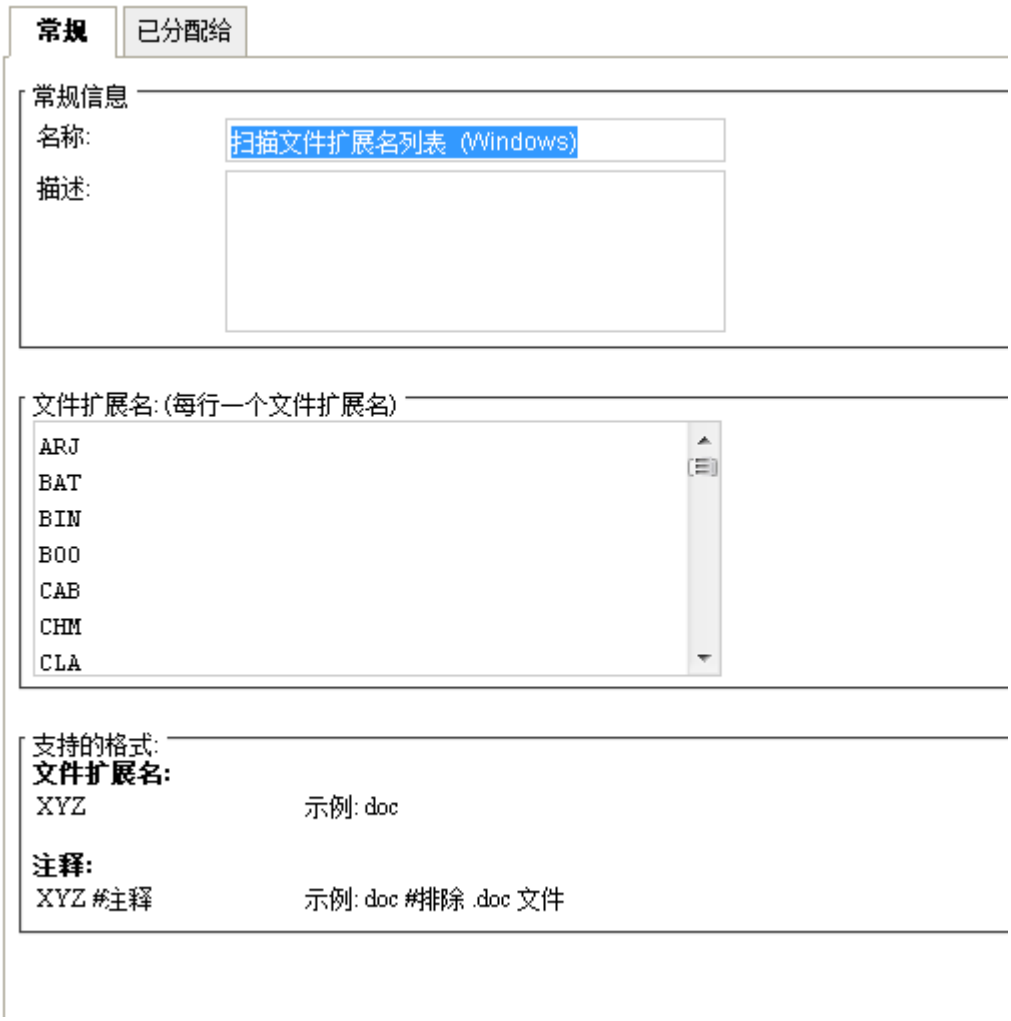
2） mac地址列表

3） 文件列表

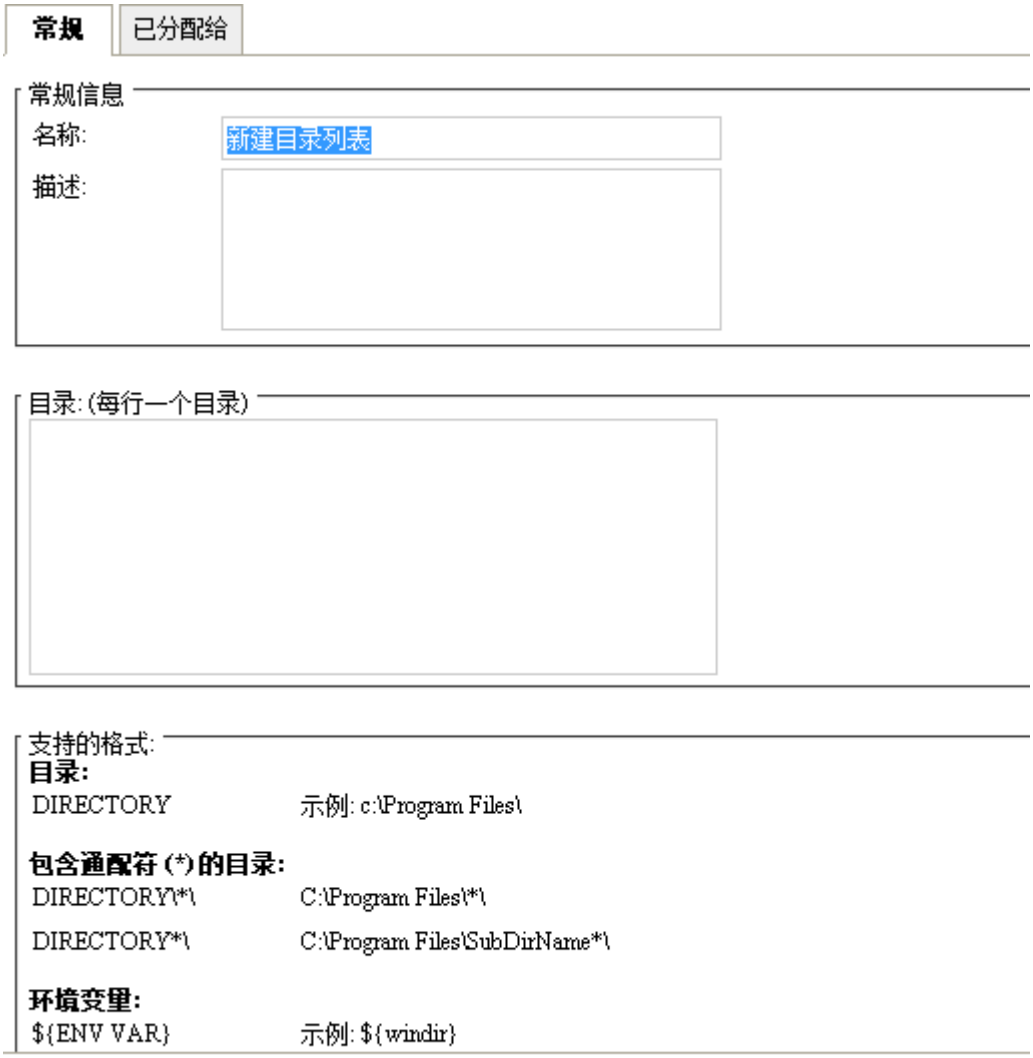
将文件定义在一个列表之中


常规
已分配给
常规信息
名称:
新建文件列表
描述:
文件:(每行一个文件)
支持的格式:
文件:
FILE
示例: testfile.doc
FILEPATH
示例: C:\Documents\testfile.doc
包含通配符(*)的文件:
FILE*
示例: MyApp*.vApp
FILE.EXT*
示例: MyApp.v*
环境变量:

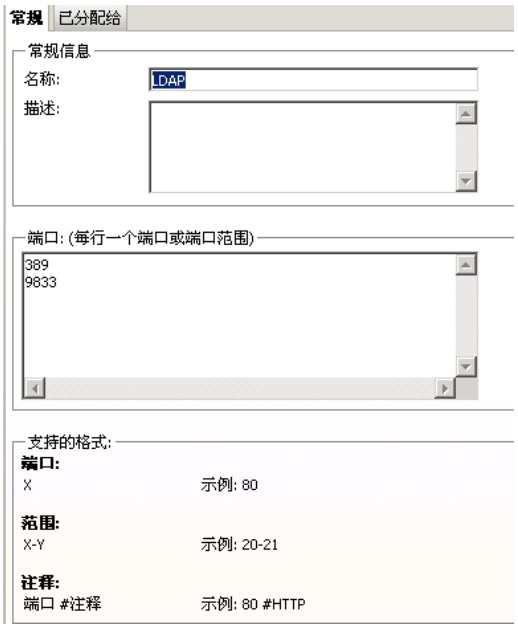
4） 文件扩展名列表



5） 目录列表（将目录设置在列表定义中）


常规
已分配给
常规信息
名称:
新建目录列表
描述:
目录: (每行一个目录)
支持的格式:
目录:
DIRECTORY
示例: c:\Program Files\
包含通配符 (*) 的目录:
DIRECTORY*\
C:\Program Files*\
DIRECTORY*\
C:\Program Files\SubDirName*\
环境变里:
${ENV VAR}
示例: ${windir}

6） 端口列表


常规
已分配给
常规信息
名称:
LDAP
描述:
端口: (每行一个端口或端口范围)
389
9833
支持的格式:
端口:
X
示例: 80
范围:
X-Y
示例: 20-21
注释:
端口 #注释
示例: 80 #HTTP

7） 列表的使用

在设置策略和规则的时候，可以使用组件列表，而不用屡次来定义。

例如在设置防火墙规则时，我们就可以使用IP列表和端口列表，而不用去每次在设置策略的时候去指定。

8. 多租户

该功能为DS9.0的新功能，通过多租户可以在企业内独立安装趋势科技服务器深度安全防护系统。可以针对组织内各个部门或业务领域创建趋势科技服务器深度安全防护系统租户。每个租户均可以访问趋势科技服务器深度安全防护系统除核心系统设置之外的所有功能。租户可以独立于其他租户负责创建和管理其自己的资产、用户、策略和规则。租户的资产或安全组件对任何其他租户均不可见。每一租户都是独立的，并与其他各个租户隔离开来。

趋势科技服务器深度安全防护系统多租户的要求如下：

- 趋势科技服务器深度安全防护系统管理中心 9

- Oracle Database 或 Microsoft SQL Server

启用多租户：

1) 在趋势科技服务器深度安全防护系统管理中心中，转至管理 > 系统设置 > 高级，然后在多租户选项区域中单击启用多租户，以显示多租户配置向导。

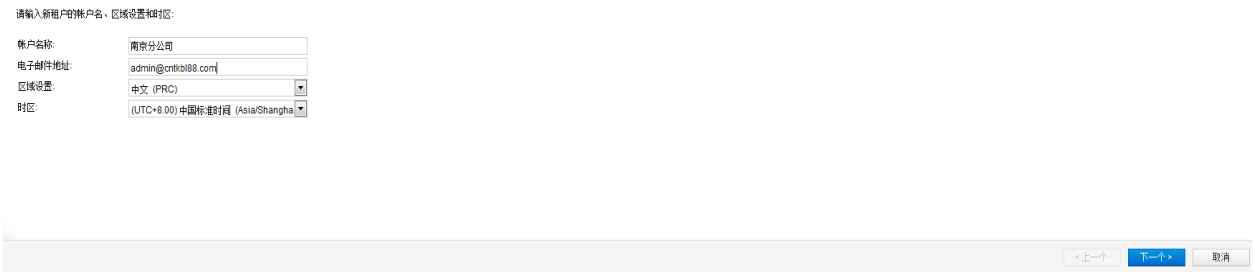
2) 输入激活码，然后单击下一步
3) 选择要实施的使用授权模式：
- 从主租户继承使用授权：为所有租户授予主租户具有的相同使用授权。
- 每租户使用授权：在此模式下，租户自己在首次登录时输入使用授权。

4) 单击下一步完成在趋势科技服务器深度安全防护系统管理中心中启用多租户。

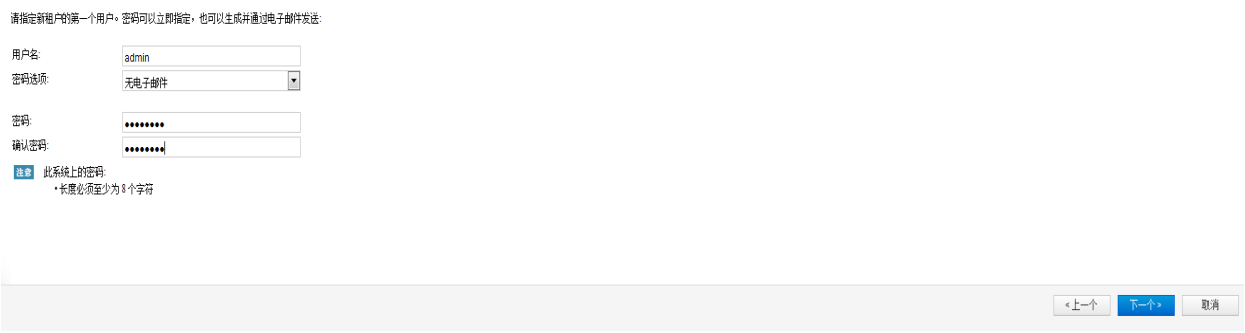
创建新租户：

1) 转至管理 > 租户页面，然后单击“新建”显示新建租户向导。

2) 输入租户帐户名称、电子邮件地址、区域设置、时区等信息，点击“下一个”。帐户名称可以是“Primary”之外的任意名称，“Primary”用于主租户。



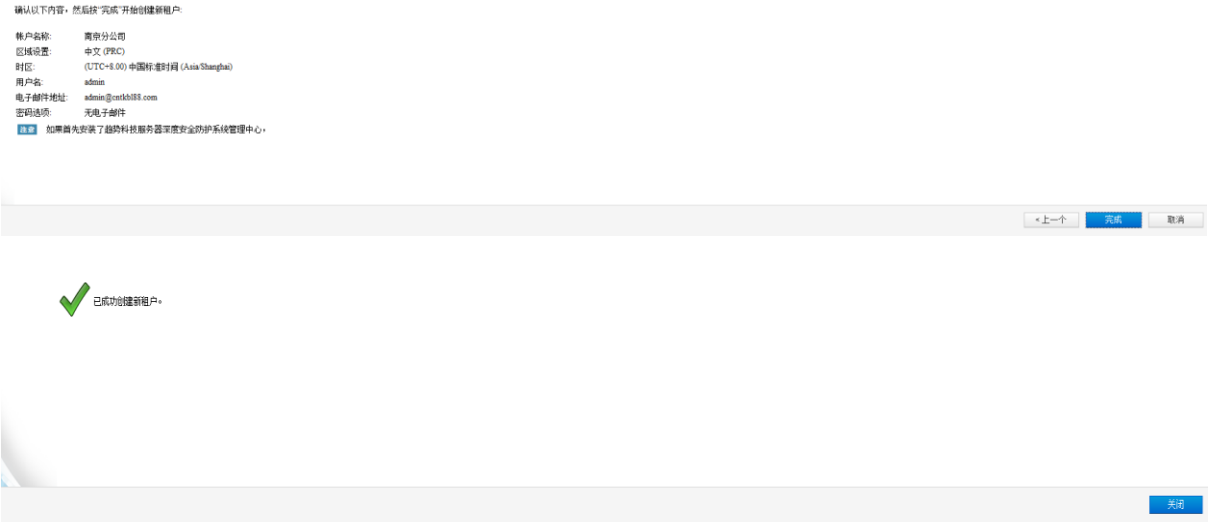
3) 输入新租户帐户首个用户的用户名，并设置对应的密码，点击下一个



注意：可以通过如下三个密码选项之一设置用户密码：

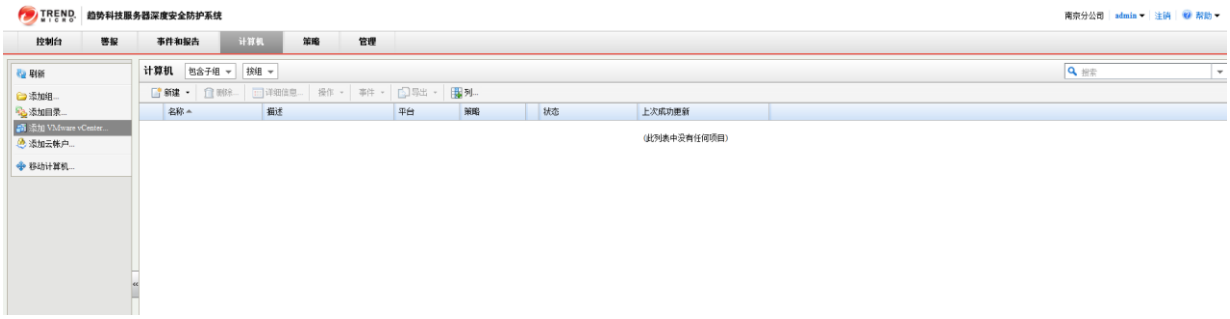
- *无电子邮件：在此处定义租户首个用户的用户名和密码，不发送电子邮件。*
- *电子邮件确认链接：您设置租户首个用户的密码。但是，直到用户单击将通过电子邮件收到的确认链接后，帐户才会被激活。*
- *电子邮件生成的密码：这允许租户创建者在未指定密码的情况下生成租户。手动创建创建者不需要访问权限的用户帐户时，此选项最适用。*

4) 单击完成向导并创建租户。（创建新租户数据库并填充数据和示例策略可能需要 30 秒到 4 分钟。）



5) 启用多租户后，登录页面将显示另一个“帐户名称文本框”，输入租户的账号名称、用户名、密码信息进行登陆。

6) 登陆后，可以添加vCenter、计算机等并对该些信息进行独立管理。


趋势科技服务器深度安全防护系统
南京分公司 | admin | 注销 | 帮助
控制台
警报
事件和报告
计算机
策略
管理
刷新
添加组...
添加目录...
添加 VMware vCenter...
添加云帐户...
移动计算机...
计算机
包含子组
按组
新建
删除...
详细信息...
操作
事件
导出
列...
名称
描述
平台
策略
状态
上次成功更新
(此列表中没有任何项目)

八、Deep Security 9.0的升级

要升级到趋势科技服务器深度安全防护系统 9.0，必须运行趋势科技服务器深度安全防护系统 8.0 SP2或更高版本。如果运行的是较早版本的趋势科技服务器深度安全防护系统，则必须首先升级到趋势科技服务器深度安全防护系统 8.0 SP2（或更高版本），然后才可升级到版本 9.0。有关如何升级到趋势科技服务器深度安全防护系统 8.0 SP2 的说明，请参考可从趋势科技下载专区获得的《趋势科技服务器深度安全防护系统 8.0 SP2 安装指南》。

趋势科技服务器深度安全防护系统 9.0 不支持 ESX/ESXi 版本 4.1。要部署趋势科技服务器深度安全防护系统 9.0，必须将 VMware 基础架构（vCenter、vShield Manager、vShield Endpoint 和 vShieldEndpoint 驱动程序）升级到版本 5.x。

一）从具有无客户端防恶意软件防护的 DS 8.0 SP2 升级（包括将 ESX/ESXi 4.1 升级到 5.x）

趋势科技服务器深度安全防护系统 9.0 不支持 ESX/ESXi 版本 4.1。要部署趋势科技服务器深度安全防护系统 9.0，必须将 VMware 基础架构（vCenter、vShield Manager、vShield Endpoint 和 vShieldEndpoint 驱动程序）升级到版本 5.x。

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。

第一个阶段，升级 VMware 组件将包括以下步骤：

1. 停用 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 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. 从 ESXi 卸载 vShield Endpoint
4. 从 ESXi 上的 VM 卸载 vShield Endpoint 客户虚拟机驱动程序
5. 升级 vCenter
6. 将 ESXi 升级到 ESXi 5.x（如果已升级到 ESXi 5.0，则应用 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 ESXi 上安装 vShield Endpoint

10. 在 VM 上安装 vShield Endpoint 驱动程序（位于随 ESXi 5.x 提供的 VMware Tools 中）

11. 重新启动 ESXi

第二个阶段，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. 升级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 9.0 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 ESXi（此操作将在 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 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 ESXi 上的客户 VM

9. 升级趋势科技服务器深度安全防护系统通知程序（如果需要）

10. 部署趋势科技服务器深度安全防护系统客户端（如果需要）

注意：

- *卸载 vShield Endpoint 模块（步骤 3）会将 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 ESXi 主机，以避免在重新启动期间关闭这些虚拟机。*
- *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。

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

二）从仅具有无客户端 FW 和 IPS 的趋势科技服务器深度安全防护系统 8.0 SP2 进行升级（从 ESX/ESXi 4.1 升级到5.x）

趋势科技服务器深度安全防护系统 9.0 不支持 ESX/ESXi 版本 4.1。要部署趋势科技服务器深度安全防护系统 9.0，必须将 VMware 基础架构（vCenter、vShield Manager、vShield Endpoint 和 vShieldEndpoint 驱动程序）升级到版本 5.x。

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 IPS 防护的VMware 环境。

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。

第一个阶段，升级 VMware 组件将包括以下步骤：

1. 停用 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 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. 将 ESXi 升级到 5.x。（如果要升级到 5.0，则应用 Patch“ESXi 5.0 (Build 474610)”或更高版本。）

第二个阶段，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 9 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 ESXi（此操作将在 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）

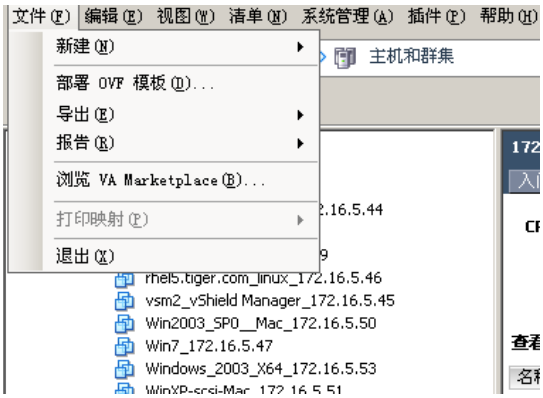
5. 在为升级做准备时重新激活趋势科技服务器深度安全防护系统虚拟设备
6. 升级 ESXi 上的趋势科技服务器深度安全防护系统虚拟设备
7. 部署和配置趋势科技服务器深度安全防护系统中继
8. 激活 ESXi 上的客户 VM
9. 部署趋势科技服务器深度安全防护系统客户端（如果需要）

九、附录

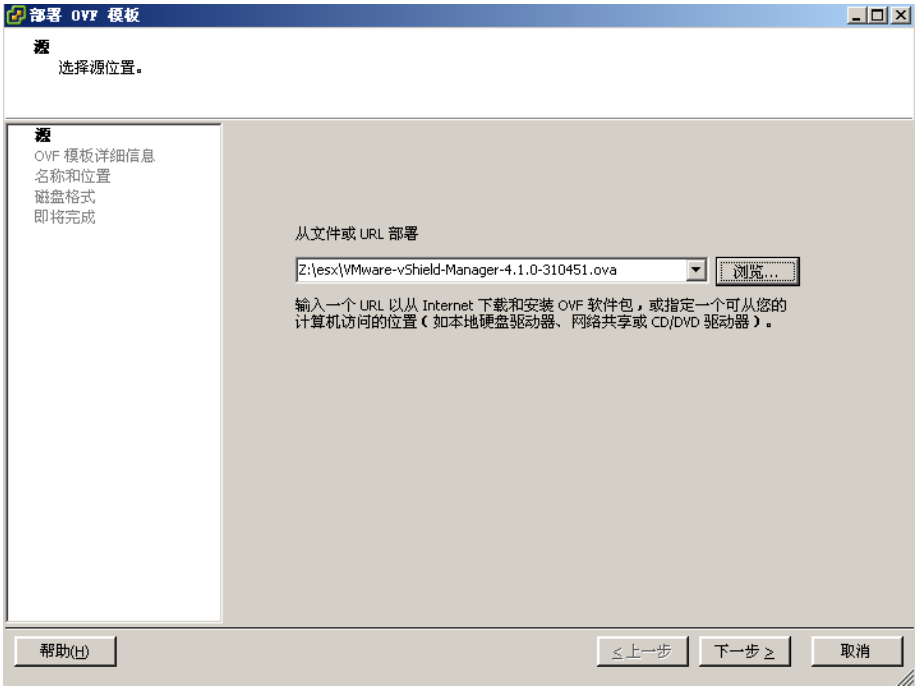
附录一：如何部署 vShield Manager

如何部署 vShield Manager

1) 点击部署 OVF 模板

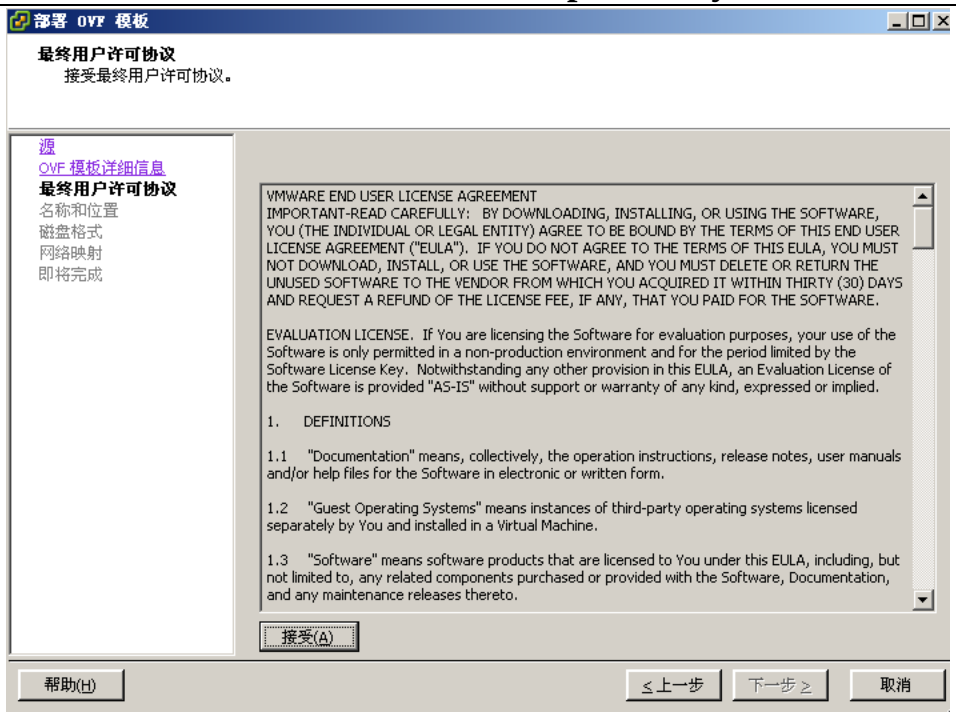


2) 选择好 shield manager 的模板，点击“下一步”

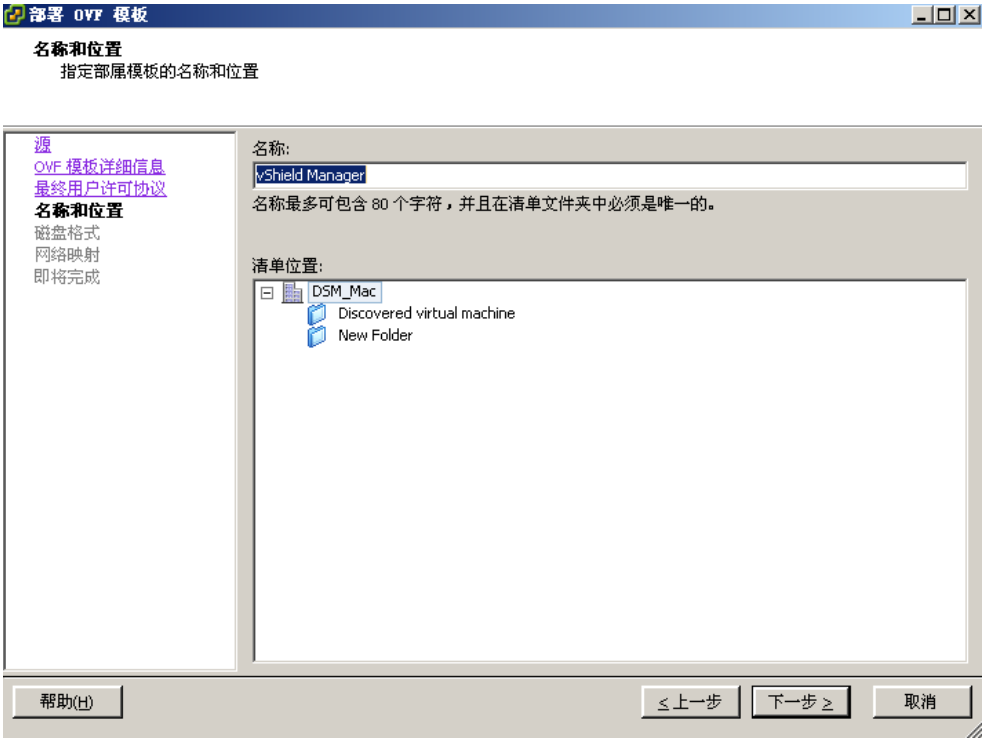

部署 OVF 模板
源
选择源位置。
源
OVF 模板详细信息
名称和位置
磁盘格式
即将完成
从文件或 URL 部署
Z:\esx\VMware-vShield-Manager-4.1.0-310451.ova
浏览...
输入一个 URL 以从 Internet 下载和安装 OVF 软件包，或指定一个可从您的计算机访问的位置（如本地硬盘驱动器、网络共享或 CD/DVD 驱动器）。
帮助(H)
≤ 上一步
下一步 ≥
取消


部署 OVF 模板
OVF 模板详细信息
验证 OVF 模板详细信息。
源
OVF 模板详细信息
最终用户许可协议
名称和位置
磁盘格式
网络映射
即将完成
产品:
vShield Manager
版本:
4.1.0-310451
供应商:
VMware, Inc.
发布者:
证书不存在
下载大小:
536.6 MB
占用空间:
876.7 MB (精简置备)
8.0 GB (厚置备)
描述:
vShield Manager is the centralized management appliance that is used to configure, monitor and update vShield Zones, vShield App, vShield Edge and vShield Endpoint products.
帮助(H)
≤ 上一步
下一步 ≥
取消

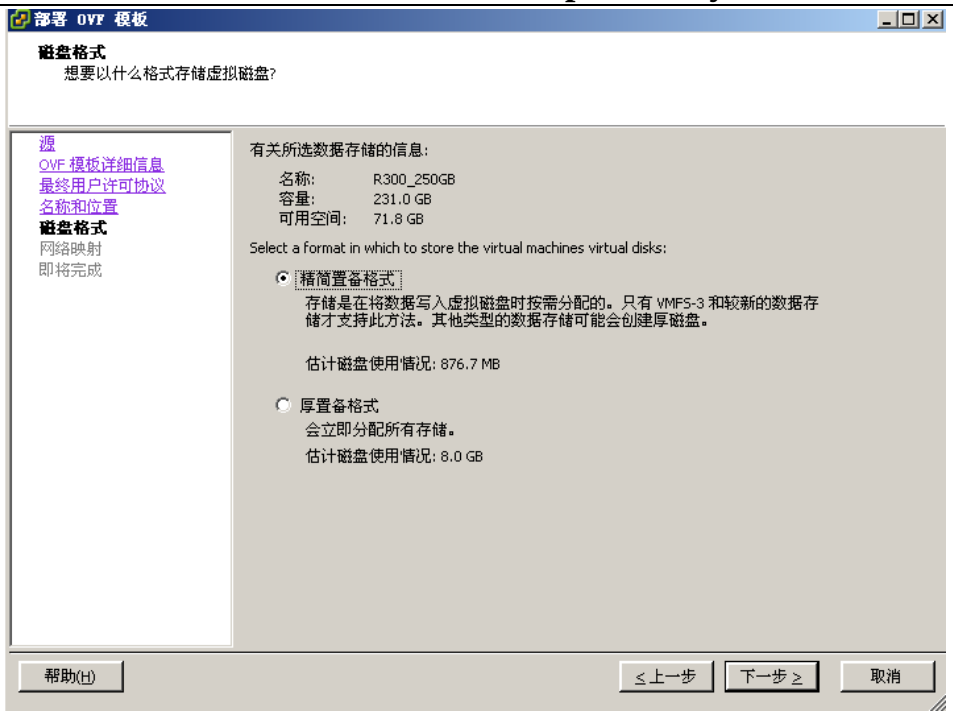
3) 接受协议



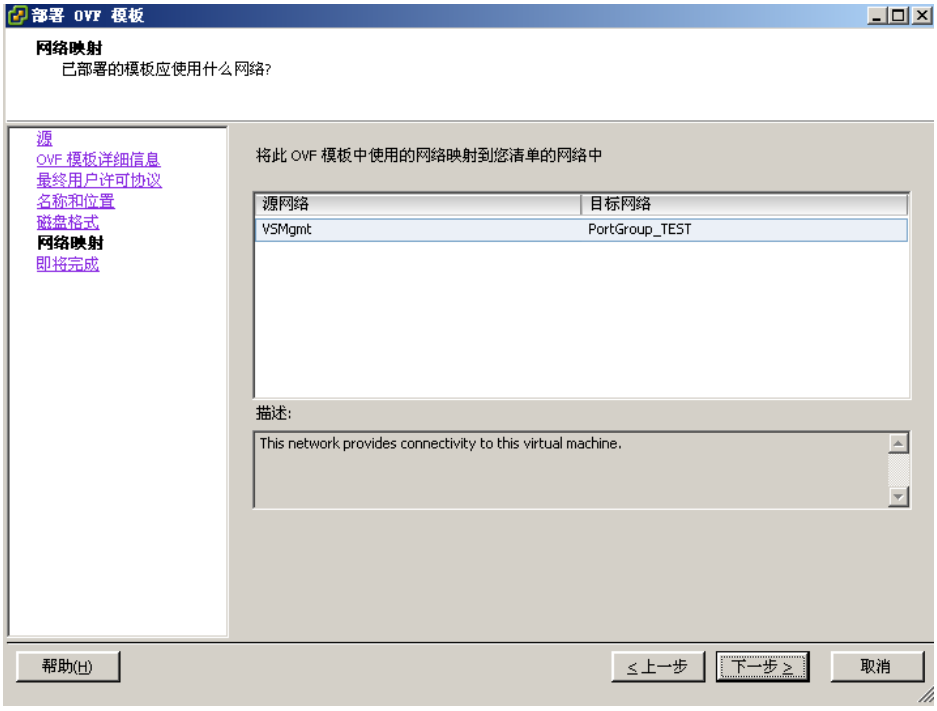
4) 选择位置后，点击“下一步”



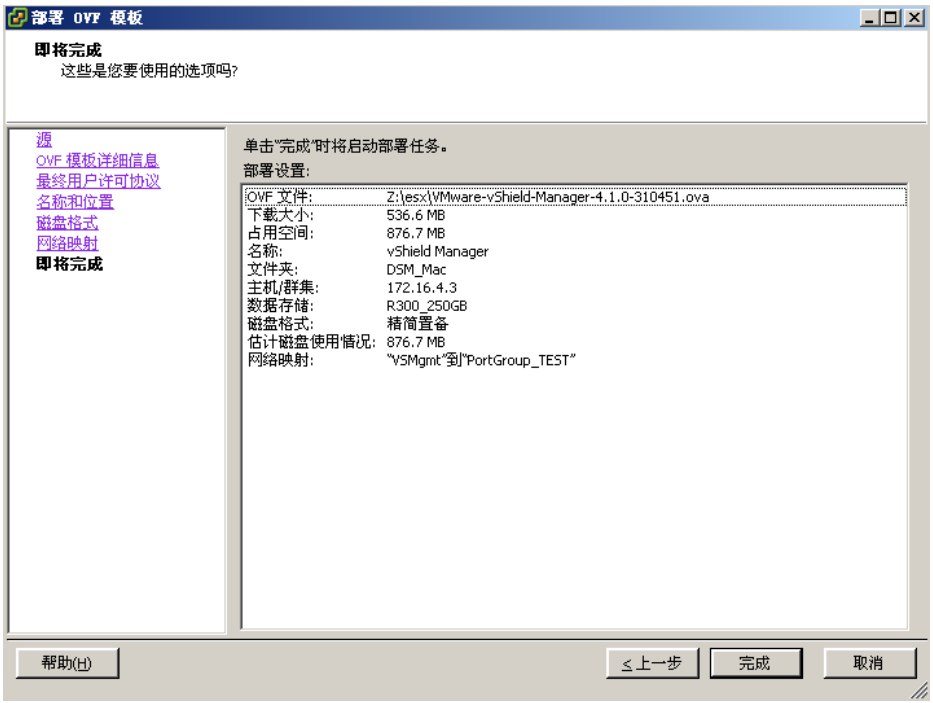
5) 选择模式后，点击“下一步”



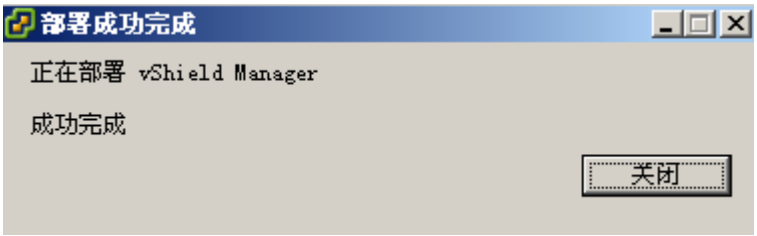
6) 映射到网络，点击“下一步”



7) 点击“完成”



8) 创建虚拟机，点击“关闭”完成部署



9) 开启 vShield Manager 虚拟机，进入 vShield 命令行模式，默认账号为 admin，密码为 default，输入 enable 进入特权模式，密码为 default，输入命令 setup，如图配置 IP 等网络设置：

```
localhost login: admin
Password:
manager> enable
Password:
manager# setup

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

IP Address (A.B.C.D): 172.16.4.198
Subnet Mask (A.B.C.D): 255.255.255.0
Default gateway (A.B.C.D): 172.16.4.1
Primary DNS IP (A.B.C.D): 10.28.128.8
Secondary DNS IP (A.B.C.D):
Warning: Secondary DNS not set.
DNS domain search list (space separated):
Warning: Search list not set. Only fully qualified hostnames will be resolved.
Old configuration will be lost
Do you want to save new configuration (y/[n]): y_
```

10) 登录 Manager 的 web 控制台，打开 IE，输入 https://vshield 的 IP，控制台的账号为 admin，密码为 default

附录二：调整虚拟机 filterdriver 性能

注意：默认情况下，每台 ESXi 上的 DSVA 可以保护 25 台虚拟机，如果一台 ESXi 上的虚拟机数量超过 25 台需要增大 FilterDriver 的 heap memory 以确保 DSVA 工作正常。

进入ESXi 维护模式

步骤1.打开vCenter 控制台

步骤2. 右键单击ESXi主机并选择进入维护模式

在fast path driver 中增加Heap Memory

步骤1. 性能调节公式：

<虚拟机数量> * <10485760 Bytes (10MB) >

例如. 30 * 1MB +108MB = 375390208 Bytes

步骤 2. 通过SSH客户端登录到ESXi Console 并执行以下命令:

%esxcfg-module –s DSAFILTER_HEAP_MAX_SIZE=375390208 dvfilter-dsa

步骤 3.输入以下命令检查heap memory 设置是否生效:

%esxcfg-module –g dvfilter-dsa

步骤 4. 执行以下命令时配置生效（或重启 ESXi 主机）

%esxcfg-module –u dvfilter-dsa

%esxcfg-module dvfilter-dsa

退出ESXi 维护模式

附录三：Deep Security 9.0 离线更新方案

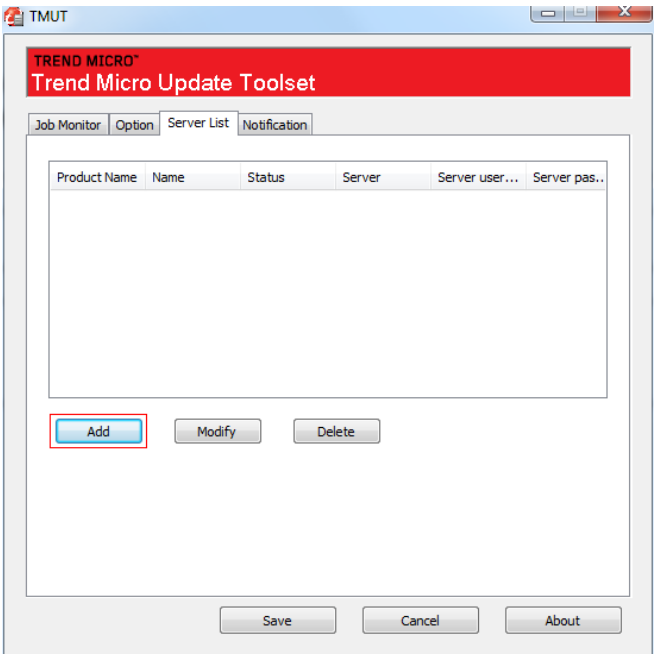
1) 下载 TMUT 工具

http://support.trendmicro.com.cn/TM-Product/Product/TMUT/1047/TMUT1.0_1047.zip

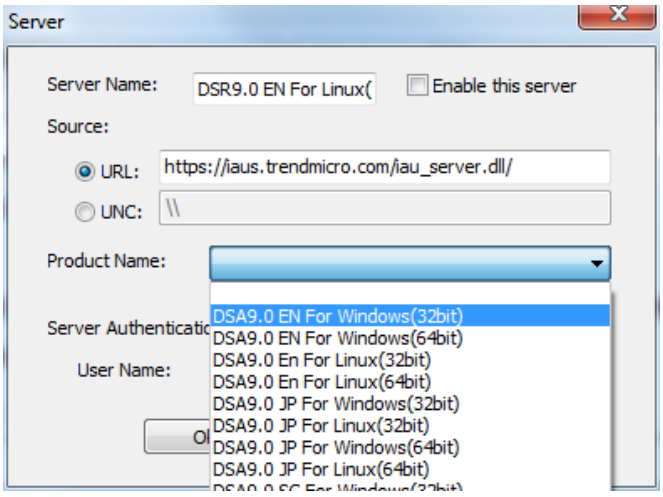
2) 解压缩以后编辑 TMUT 安装目录中的 ProductInfo.ini 配置文件，加入以下参数：

DSA9.0 EN For Windows(32bit):c22t2200v8.0.0l1p1r1o1
DSA9.0 EN For Windows(64bit):c22t2200v8.0.0l1p5889r1o1
DSA9.0 En For Linux(32bit):c22t2200v8.0.0l1p257r1o1
DSA9.0 En For Linux(64bit):c22t2200v8.0.0l1p9217r1o1
DSA9.0 JP For Windows(32bit):c22t2200v8.0.0l4p1r3o1
DSA9.0 JP For Linux(32bit):c22t2200v8.0.0l4p257r3o1
DSA9.0 JP For Windows(64bit):c22t2200v8.0.0l4p5889r3o1
DSA9.0 JP For Linux(64bit):c22t2200v8.0.0l4p9217r3o1
DSA9.0 SC For Windows(32bit):c22t2200v8.0.0l8p1r5o1
DSA9.0 SC For Linux(32bit):c22t2200v8.0.0l8p257r5o1
DSA9.0 SC For Windows(64bit):c22t2200v8.0.0l8p5889r5o1
DSA9.0 SC For Linux(64bit):c22t2200v8.0.0l8p9217r5o1
DSVA9.0 EN For Linux(64bit):c22t2201v8.0.0l1p9217r1o1
DSR9.0 EN For Windows(32bit):c22t2202v8.0.0l1p1r1o1
DSR9.0 EN For Windows(64bit):c22t2202v8.0.0l1p5889r1o1
DSR9.0 EN For Linux(64bit):c22t2202v8.0.0l1p9217r1o1

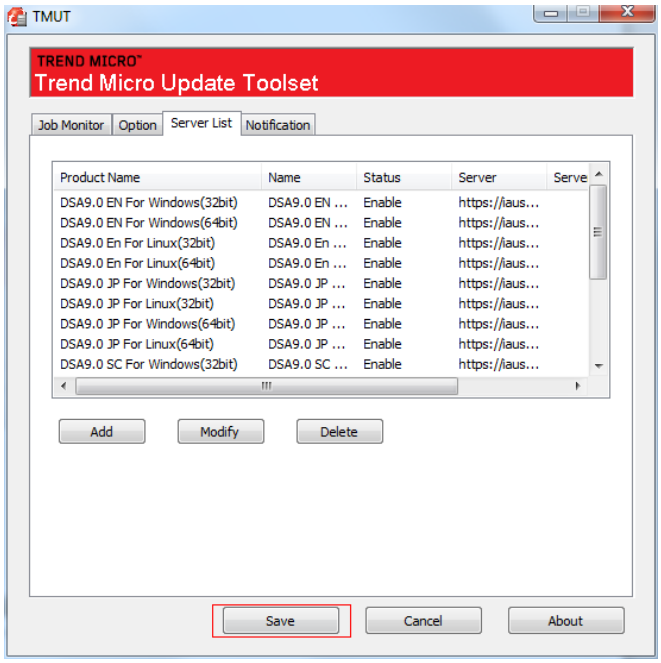
3) 设置 TMUT 工具，如下图所示,添加服务器：



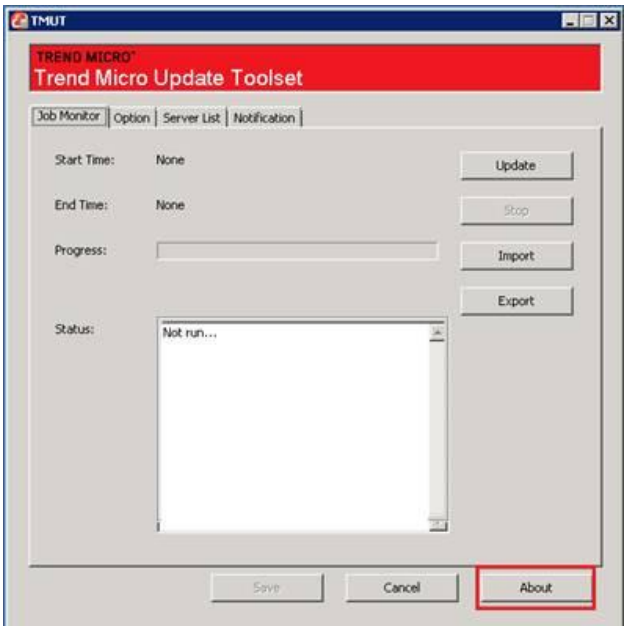
4) 依次把 Deep Security 9 所有组件添加到服务器列表

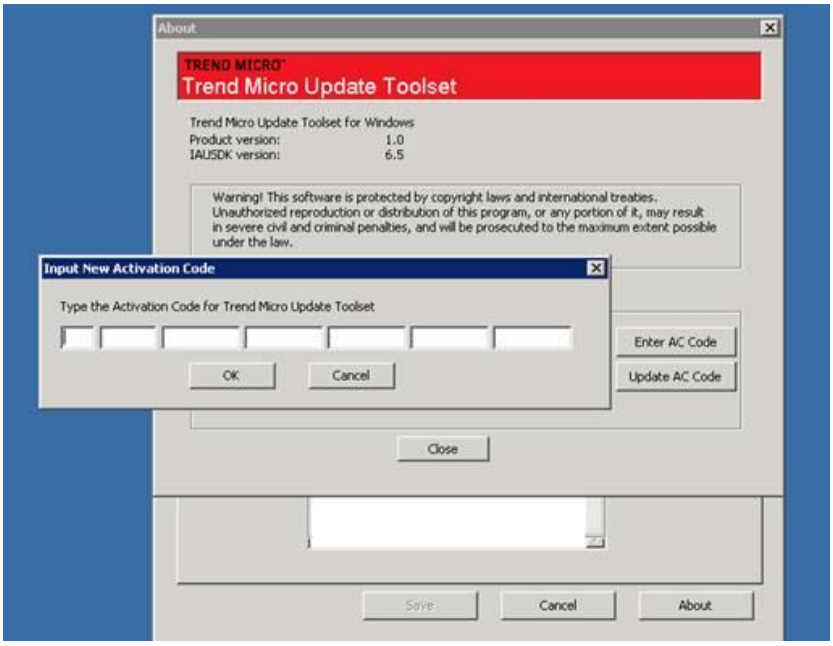


5) 保存设置

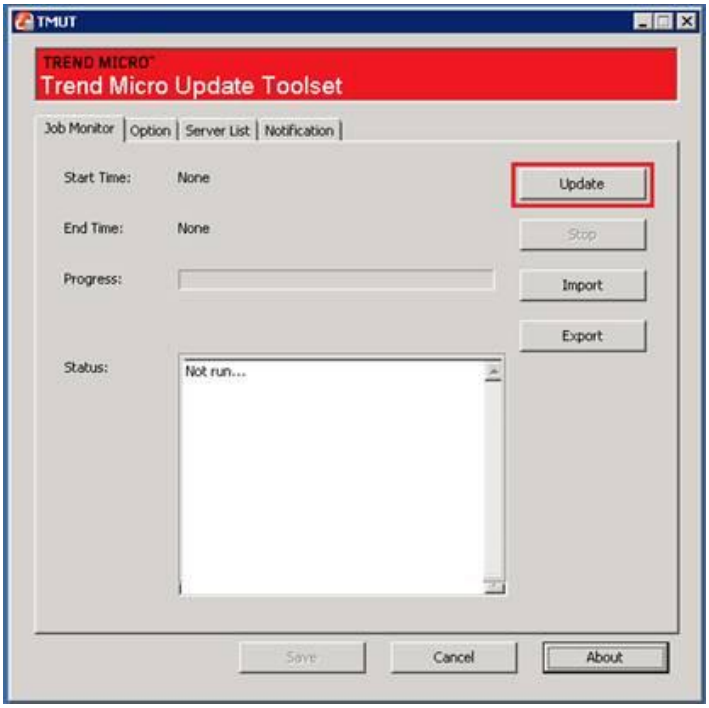


6) 输入激活号（支持各种产品激活号，包括 AP 测试号）

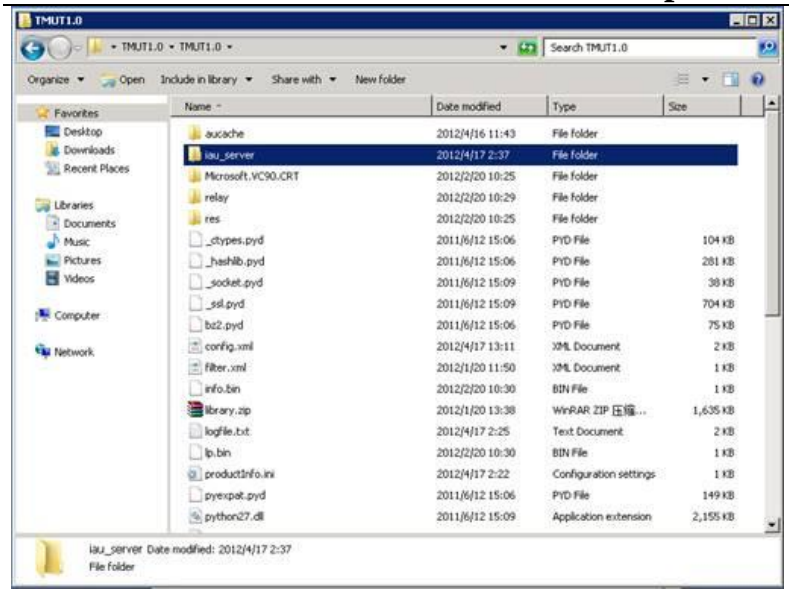




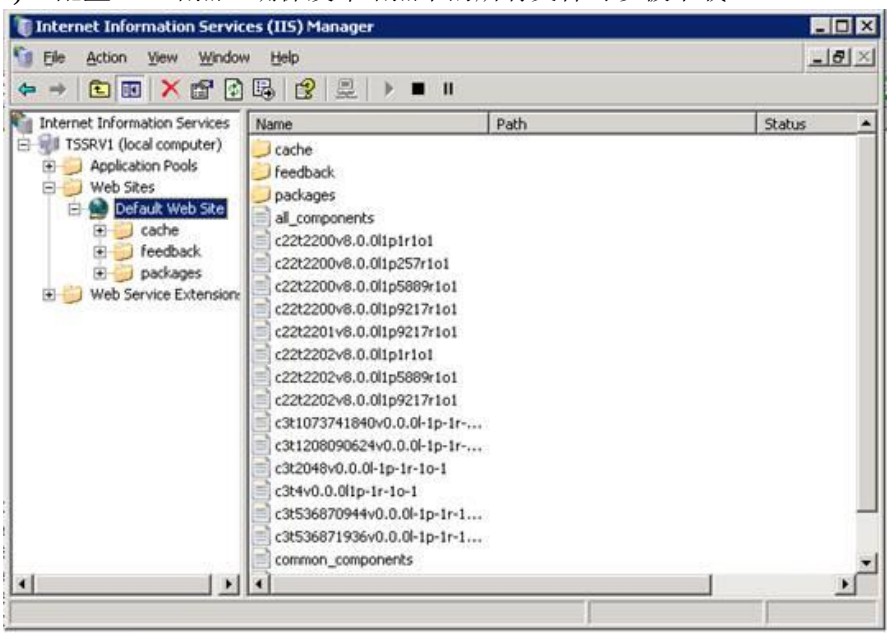
7) 点击更新按钮



8) 完成更新通过 IIS 发布 TMUT 目录下的

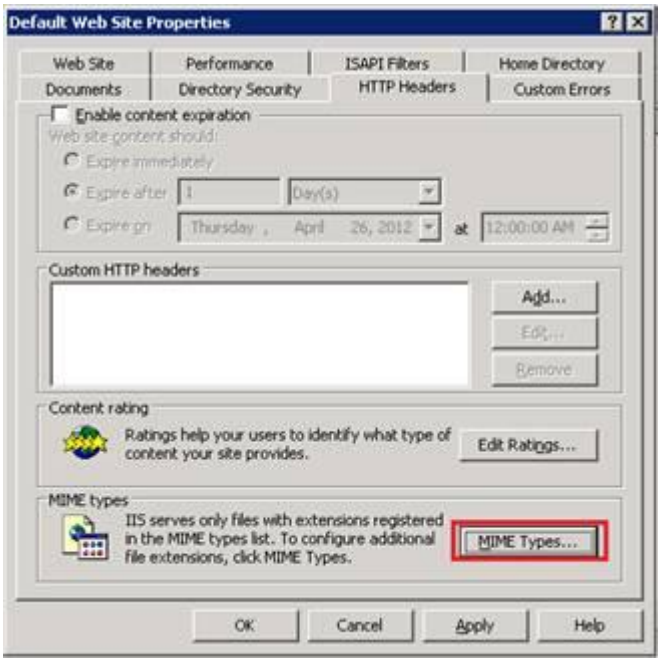


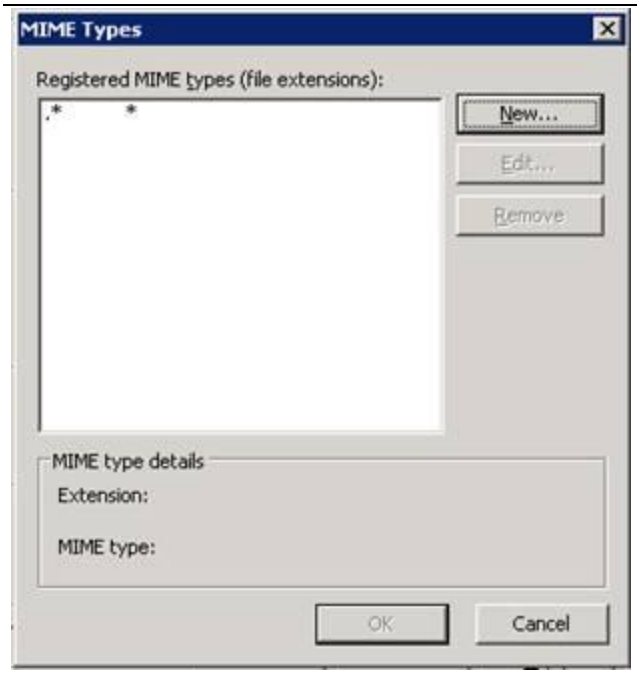
9) 配置 IIS 站点，确保发布站点下的所有文件可以被下载：

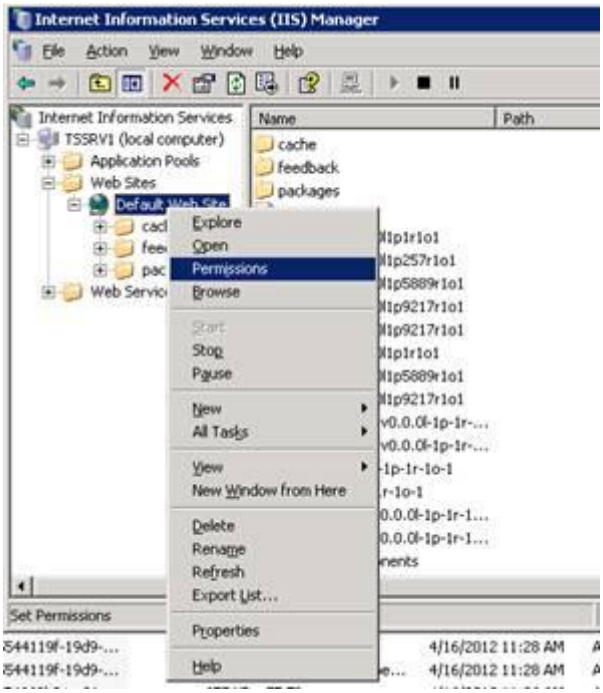


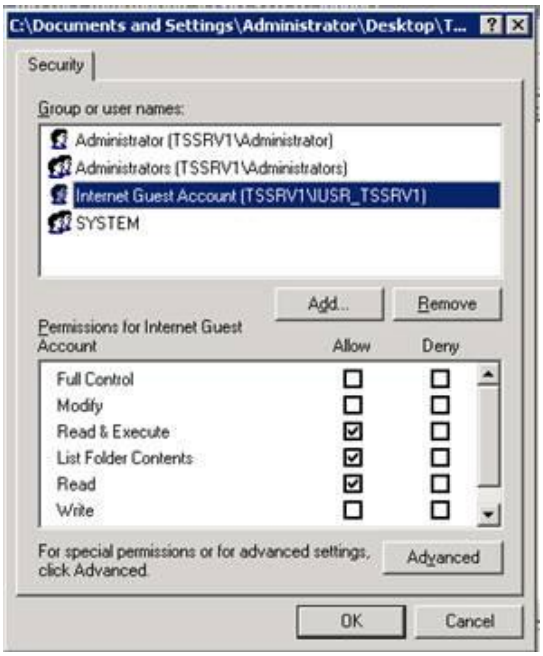
IIS 站点设置细节：


Default Web Site Properties
Documents
Directory Security
HTTP Headers
Custom Errors
Web Site
Performance
ISAPI Filters
Home Directory
The content for this resource should come from:
A directory located on this computer
A share located on another computer
A redirection to a URL
Local path:
Desktop\TMUT1.0\TMUT1.0\jau_server
Browse...
Script source access
Log visits
Read
Index this resource
Write
Directory browsing
Application settings
Application name:
Default Application
Remove
Starting point:
<Default Web Site>
Configuration...
Execute permissions:
None
Application pool:
DefaultAppPool
Unload
OK
Cancel
Apply
Help

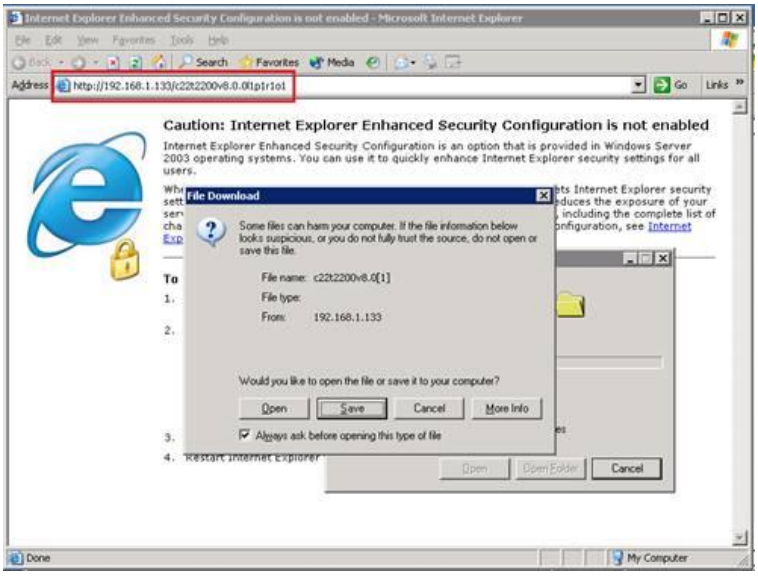

Default Web Site Properties
Web Site
Performance
ISAPI Filters
Home Directory
Documents
Directory Security
HTTP Headers
Custom Errors
Enable content expiration
Web site content should:
Expire immediately
Expire after
Day(s)
Expire on
Thursday , April 26, 2012
at
12:00:00 AM
Custom HTTP headers
Add...
Edit...
Remove
Content rating
Ratings help your users to identify what type of content your site provides.
Edit Ratings...
MIME types
IIS serves only files with extensions registered in the MIME types list. To configure additional file extensions, click MIME Types.
MIME Types...
OK
Cancel
Apply
Help


MIME Types
Registered MIME types (file extensions):
.*
*
New...
Edit...
Remove
MIME type details
Extension:
MIME type:
OK
Cancel

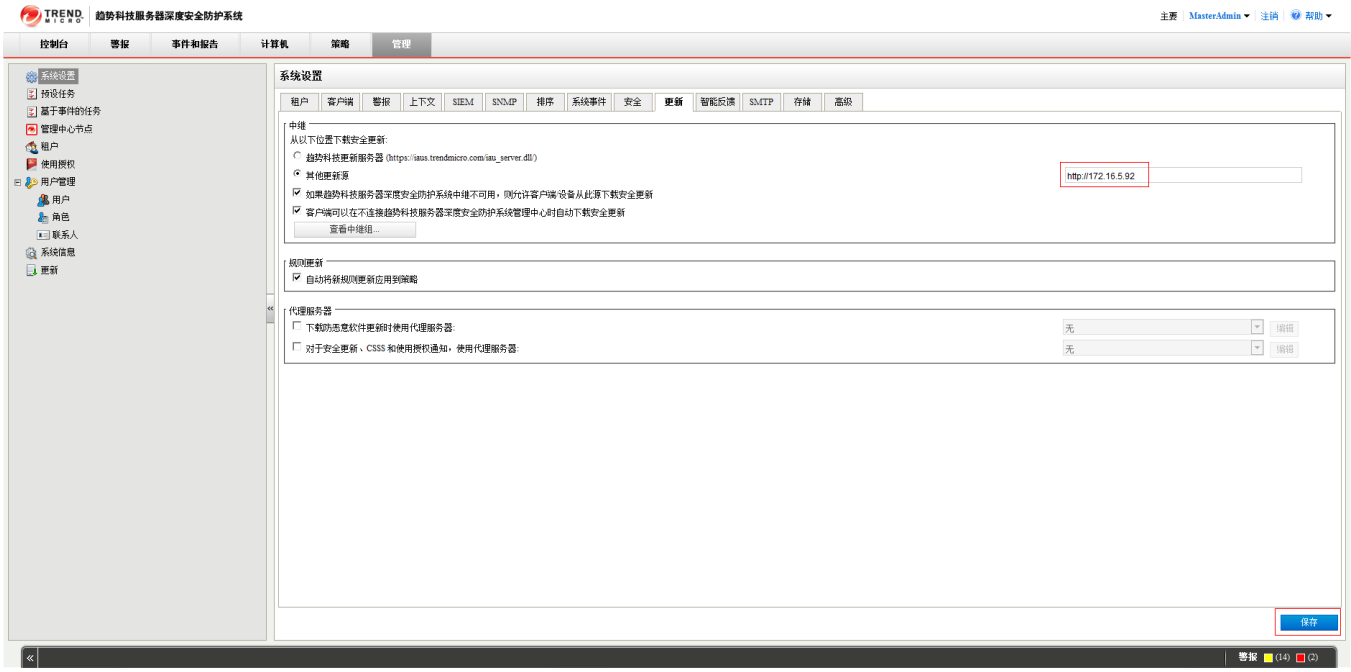

Internet Information Services (IIS) Manager
File Action View Window Help
Internet Information Services
TSSRV1 (local computer)
Application Pools
Web Sites
Default Web Site
Name
Path
cache
feedback
packages
Explore
Open
Permissions
Browse
Start
Stop
Pause
New
All Tasks
View
New Window from Here
Delete
Rename
Refresh
Export List...
Properties
Help
Set Permissions
4/16/2012 11:28 AM
4/16/2012 11:28 AM



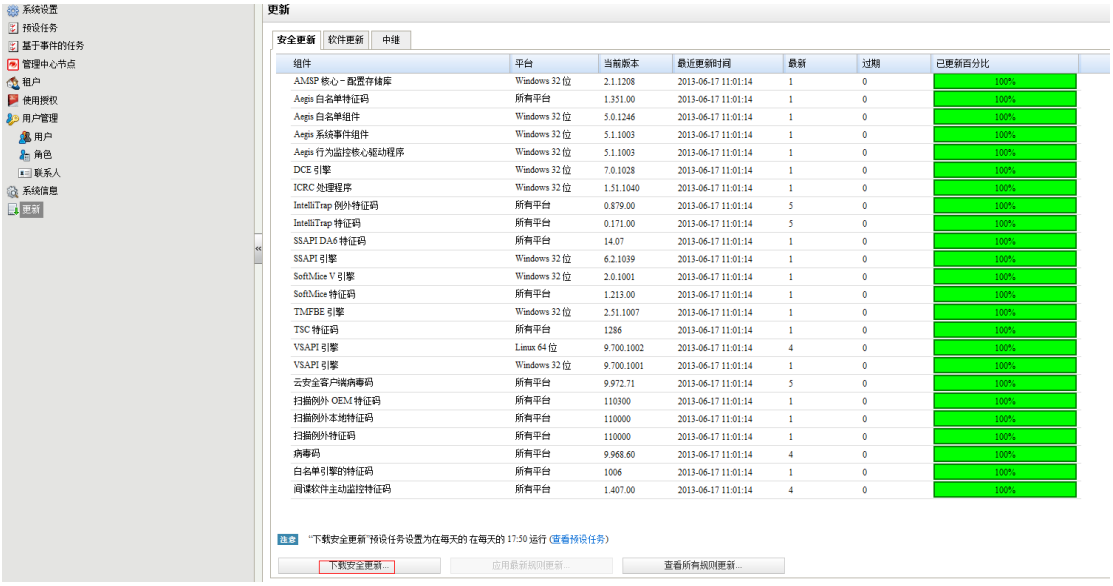
10) 测试更新源有效性：



11) 修改 DSM 更新源：



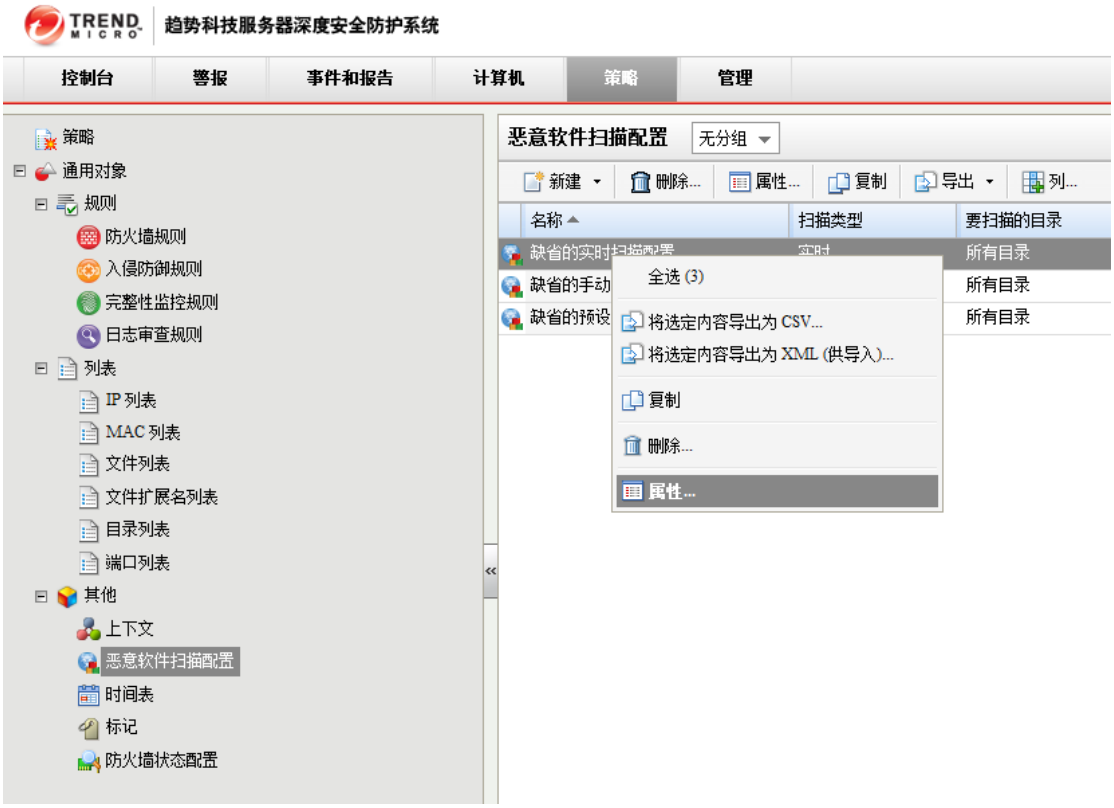
12) 更新 DSM



附录四：Deep Security Anti-malware 模块扫描优化配置

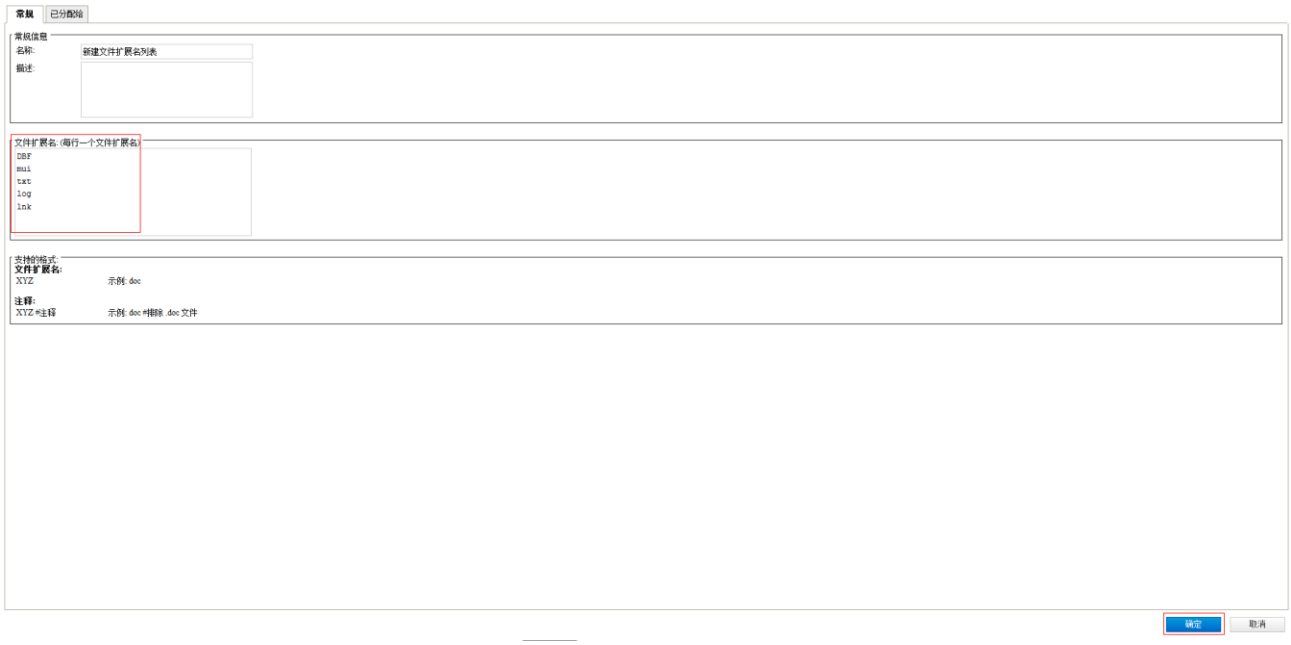
对于 DS 的防病毒模块，建议参考如下配置来优化扫描性能：

1) 登录 DSM 控制台
2) 点击“策略 > 其他 > 防恶意软件配置”，然后右击“缺省的实时扫描配置”，点击“属性”



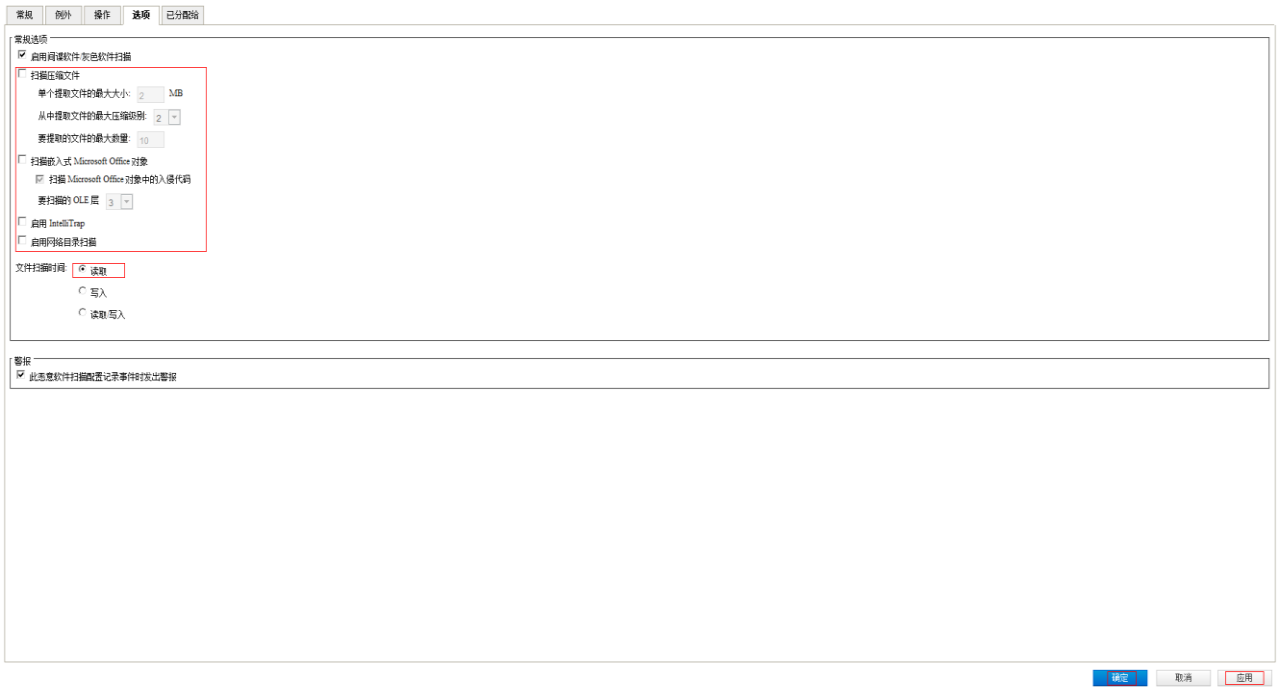
3) 在“常规”选项卡中，勾选“扫描文件扩展名列表（windows）”

4) 单击“例外”选项卡，将 DBF、mui、txt、 log、 lnk 等扩展名类型设置为例外，设置完成后点击“确定”

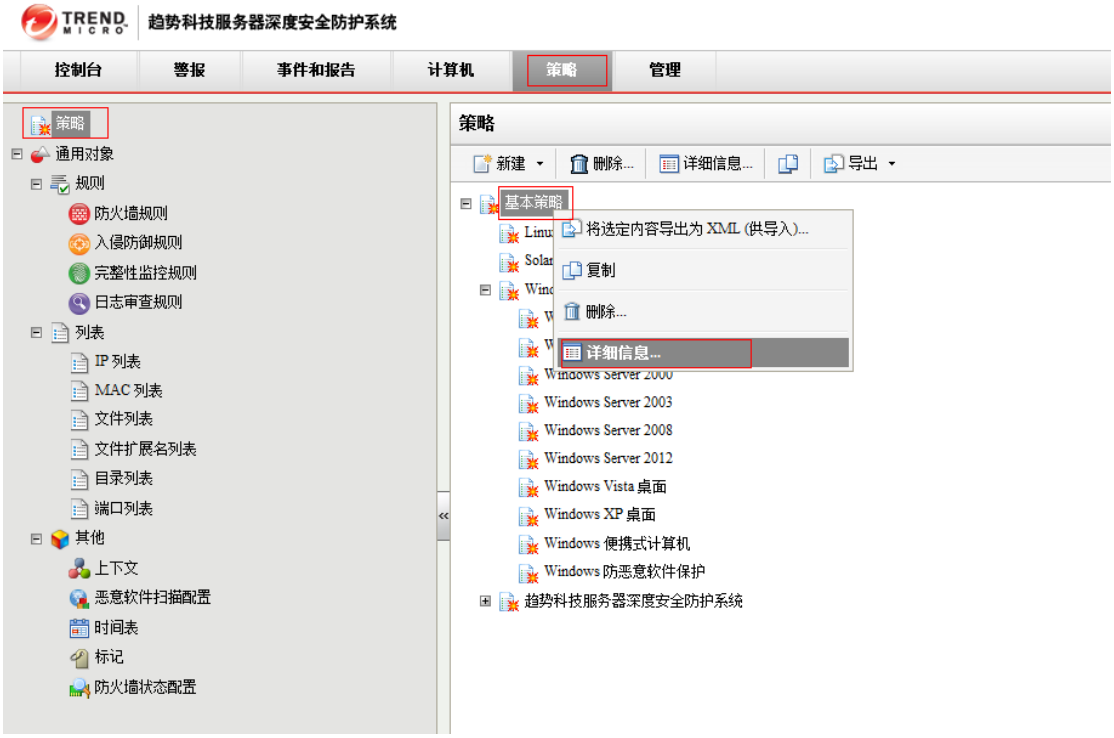


5) 勾选“进程镜像文件列表”，选择“进程镜像文件 (Windows)”

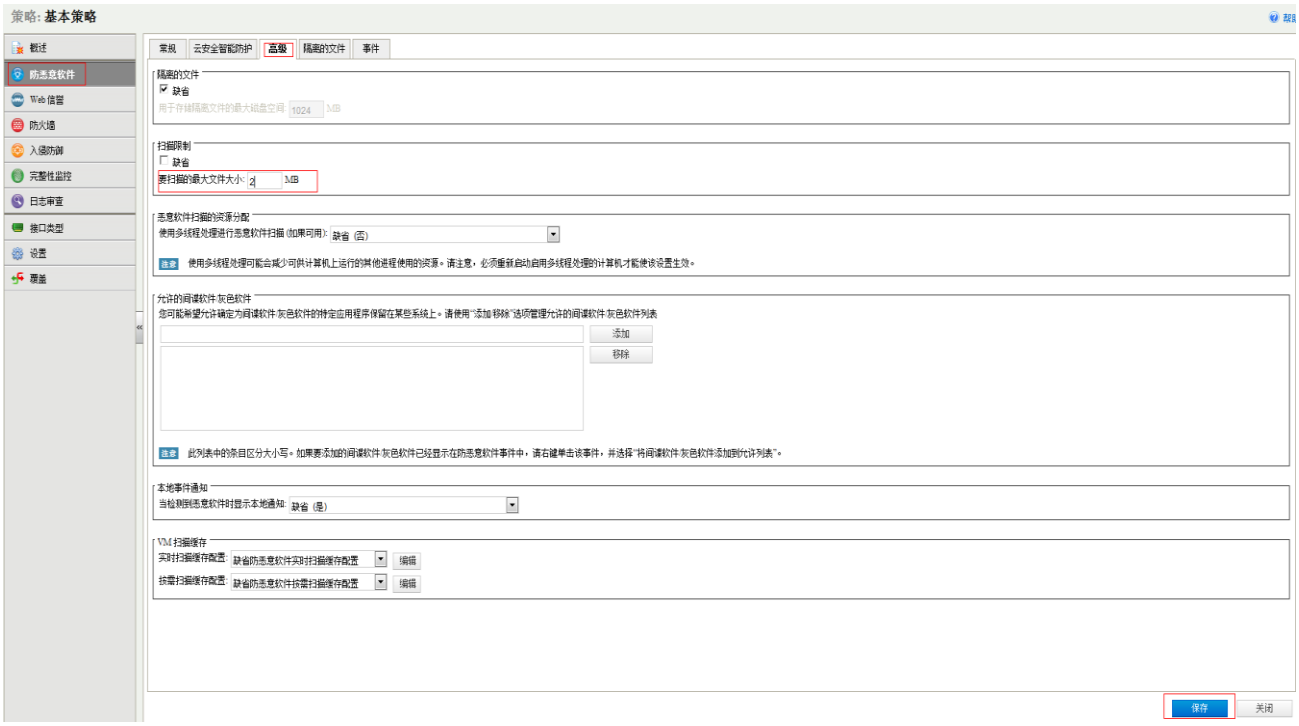
6) 选择“选项”选项卡，取消勾选“扫描压缩文件”、“扫描嵌入式 Microsoft Office 对象”、“启用 IntelliTrap”、“启用网络目录扫描”等选项，文件扫描选择为“读取”，以上设置完成后，点击“应用—确定”



7) 选择“策略 > 策略”，右击“基本策略”的“详细信息”。



8) 点击“防恶意软件 > 高级”，将要扫描的最大文件大小设置为 2M，点击“保存”。



十、趋势科技厂商资源

800 免费技术支持热线

800-820-8839

800 免费商务热线

800-820-8876

售后电子邮件地址

service@trendmicro.com.cn

趋势科技中文网站

http://cn.trendmicro.com/cn/home/

病毒查询

www.trendmicro.com.cn/vinfo

趋势科技英文网站

http://us.trendmicro.com/us/home/

趋势科技病毒递交信箱

virus_doctor@trendmicro.com.cn