趋势科技 Deep Security
产品常见问题（FAQ）

趋势科技技术支持部

2014 年 3 月

目录

一. 安装部署

Deep Security 8.0 是否支持使用 IDE 磁盘控制器的 VM 虚拟机？

由于 vShield Endpoint 5.0 不再限制支持范围为 SCSI LSI logic 控制器，因此 Deep Security 8.0 虚拟机即时采用 IDE 磁盘格式也支持 Agent-less Anti-malware 功能。

Deep Security 部署在虚拟化环境时需要作哪些准备？

当 DS 8.0 需要对 Vmware vSphere5.0 虚拟化环境启用“无代理-反病毒”保护时需要对虚拟化环境进行作相应准备：

一台 vCenter Server 服务器（物理服务器/虚拟服务器）

SQL Server 或 Oracle 数据库服务器（物理服务器/虚拟服务器）

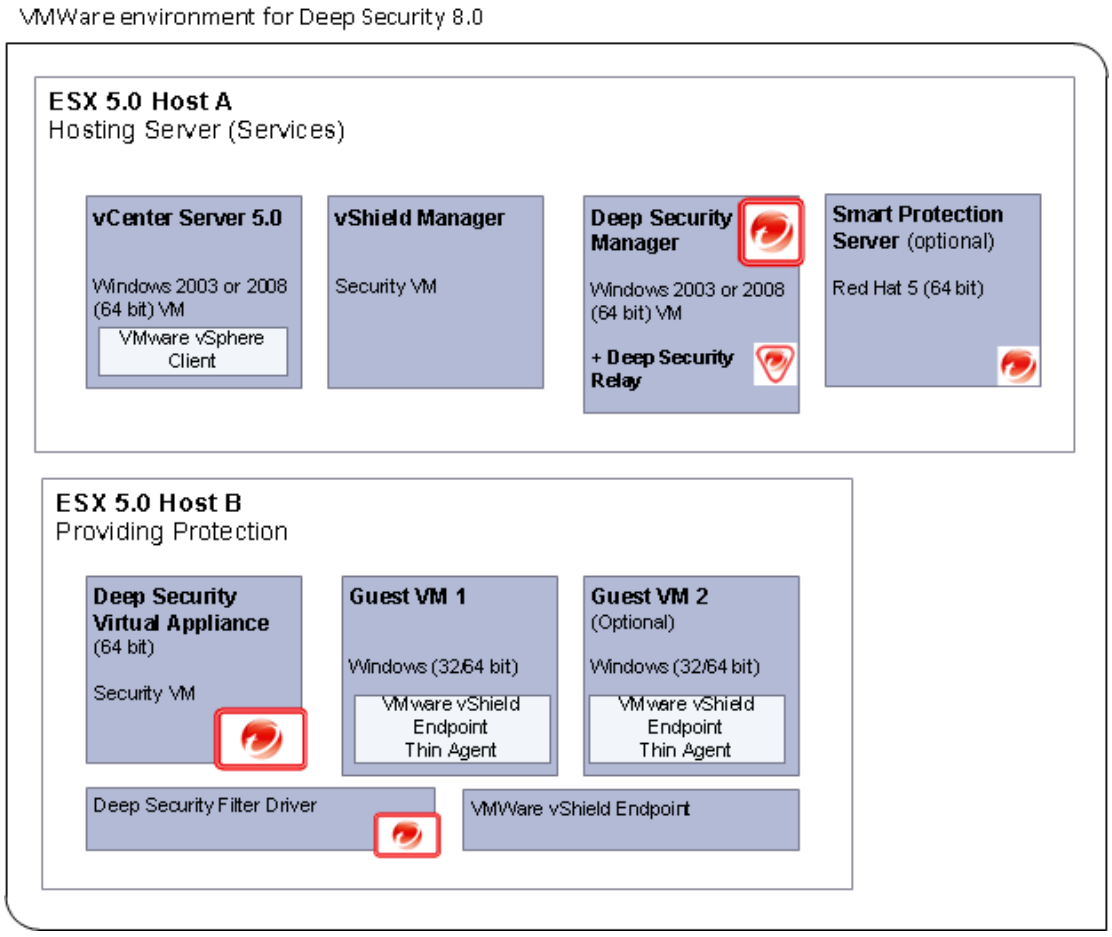
Deep Security Manager 服务器（物理服务器/虚拟服务器）

ESXi 5.0 服务器

vShield Manager（虚拟机）

Deep Security Virtual Agent （虚拟机）

注意：必须确保 Deep Security Manager ，vCenter Server 不作为虚拟机运行在受 DSVA 保护的 ESXi 5.0 服务器上



如上图所示，典型的 Deep Security Agent-less 保护模式下，VC,VSM,DSM,SPS 不在受 DSVA 保护的 HOSTB 主机上运行。

此外如果使用 MS SQL Server 数据库或 Oracle 数据库时需要在 DSM 安装前手动创建 DSM 数据库。

Deep Security 8.0 在企业 vSphere 5.0 环境部署时无代理保护时有哪些注意事项？

Deep Security Manager,Vcenter Server，vShield Manager Server(非强制)，Database Server 不建议作为虚拟机部署在受 DSVA 保护的 ESX 主机上

每台 DSVA 与受保护的 ESXi 5.0 一一对应，避免 DSVA 受到由于 DRS 或 HA 而被 *Vmotion* 迁移到其他 ESXI 5.0 主机。

可以通过以下方式防止 DSVA 发生 vMoiton 迁移动作：

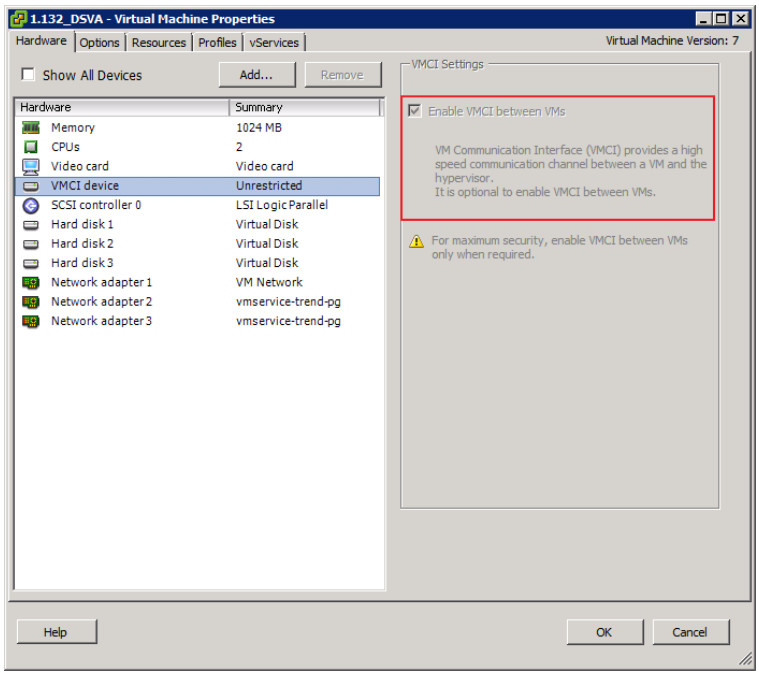
DSVA 虚拟机文件存储在 ESXi5.0 本地 Data Store 中

把 DSVA 虚拟机设置为 DRS 和 HA 的例外列表（具体步骤请参考 VMWARE 相关文档）

确保 ESXi5.0 已经安装(ESXI5 patch ESXi500-201109001 for vShield Endpoint Driver)补

丁

启用虚拟机之间的的 VMCI 功能，确保 Deep Security Notify 在虚拟机无代理保护模式下可以正常工作，如图所示：



Deep Security Manager 的软硬件需求是什么？

基本要求：

- 内存：4GB
- 磁盘空间：1.5GB ，推荐 5GB（不包括数据库大小）
- 操作系统：

Windows：Microsoft Windows Server 2008 (32-bit and 64-bit),

Windows Server2008 R2 (64-bit),

Windows 2003 Server SP2 (32-bit and 64-bit)

Linux：RHEL 5 (64-bit), RHEL 6 (64-bit)

- 数据库 (推荐非必选)：

Oracle 11g, Oracle 10g,

Microsoft SQL Server 2008 SP1, Microsoft SQL Server 2005 SP2. (20GB recommended for preallocation)

- 浏览器：

Mozilla Firefox 3+ (启用 cookies)

Internet Explorer 7+（启用 cookies）

Internet Explorer 8+（启用 cookies）

Deep Security 8.0 部署时 ESXi 主机是否需要重启？

Deep Security 8.0 在部署时的以下情况需要重启 ESXi 5.0 服务器

在对 ESXi 5.0 执行准备（prepare）操作时需要重启 ESXi5.0 服务器

安装 ESXi500-201109001 补丁时需要重新启动

调整 ESXi5.0 heap memory 设置（针对 DSVA 的性能调整）

Deep Security Manager 与 VMWARE 兼容性列表

Deep Security9.0 SP1:

	ESXi								ESX/ESXi
vShield Endpoint	5.5	5.1 U2	5.1 U1	5.1	5.0 U3	5.0 U2	5.0 U1	5.0	4.1
5.5a	Y[A]	Y	Y	Y	Y	Y	Y	Y	N
5.5	Y[A]	Y	Y	Y	Y	Y	Y	Y	N
5.1.2	N	Y	Y	Y	Y	Y	Y	Y	N
5.1.1	N	N	Y	Y	Y	Y	Y	Y	N
5.1	N	N	Y	Y	Y	Y	Y	Y	N
5.0.2	N	N	N	N	Y	Y	Y	Y	N
5.0.1	N	N	N	N	Y	Y	Y	Y	N
5.0	N	N	N	N	Y	Y	Y	Y[B]	N
1.x	N	N	N	N	N	N	N	N	N

[A] Deep Security 9.0 SP1 Patch 2 必须被安装.

[B] 需要 ESXi500-201109401-BG:Updates esx-base 和 ESXi500-201109402-BG:Updates tools-light.

Deep Security 9.0 注意事项:

- *无代理扫描，扫描缓存和完整性监控功能要求 ESXi 至少为 5.1 版本.*
- *Deep Security Virtual Appliance (DSVA) 9.0 和 Filter Driver (FD) 9.0 不支持 ESX 4.1. DSVA 8.0 SP1 和 FD 8.0 SP1 可以支持 ESX 4.1,但它们无法被 DSM 9.0 管理.*

Deep Security8.0 SP2:

	ESXi								ESX/ESXi			
vShield Endpoint	5.5	5.1 U2	5.1 U1	5.1	5.0 U3	5.0 U2	5.0 U1	5.0	4.1 U3	4.1 U2	4.1 U1	4.1
5.5a	N	Y	Y	Y	Y	Y	Y	Y	N	N	N	N
5.5	N	Y	Y	Y	Y	Y	Y	Y	N	N	N	N
5.1.2	N	Y	Y	Y	Y	Y	Y	Y	Y	N	N	N
5.1.1	N	N	Y	Y	Y	Y	Y	Y	Y	N	N	N
5.1	N	N	Y	Y	Y	Y	Y	Y	Y	N	N	N
5.0.2	N	N	N	N	Y	Y	Y	Y	Y	N	N	N
5.0.1	N	N	N	N	Y	Y	Y	Y	Y	N	N	N
5.0	N	N	N	N	Y	Y	Y	YA	Y	YB	YB	YB
1.x	N	N	N	N	N	N	N	N	N	N	N	N

[A] 需求 ESXi500-201109401-BG:Updates_esx-base 和 ESXi500-201109402-BG:Updates_tools-light.

[B] 需求 ESX410-201107001(ESX) 或 ESX410-201107001(ESXi)，以及 ESXi500-201109402-BG:Updates_tools-light.

Deep Security 8.0 注意事项:

- *针对 ESXi 5.0 或 ESX/ESXi 4.x，我们建议在部署时使用相同的 Filter Driver 和 Deep Security Virtual Appliance (DSVA) build. 有 2 种版本:*
  - *针对 ESXi 5.0，使用 FilterDriver-ESX_5.0-8.0.0-xxxx.x86_64.zip.*
  - *针对 ESX/ESXi 4.x，使用 FilterDriver-ESX_4.1-8.0.0-xxxx.x86_64.zip.*
- *由于修改了 VMCI 通讯，在 vSphere 5.1 通知程序功能将不可用.*

Deep Security 7.5

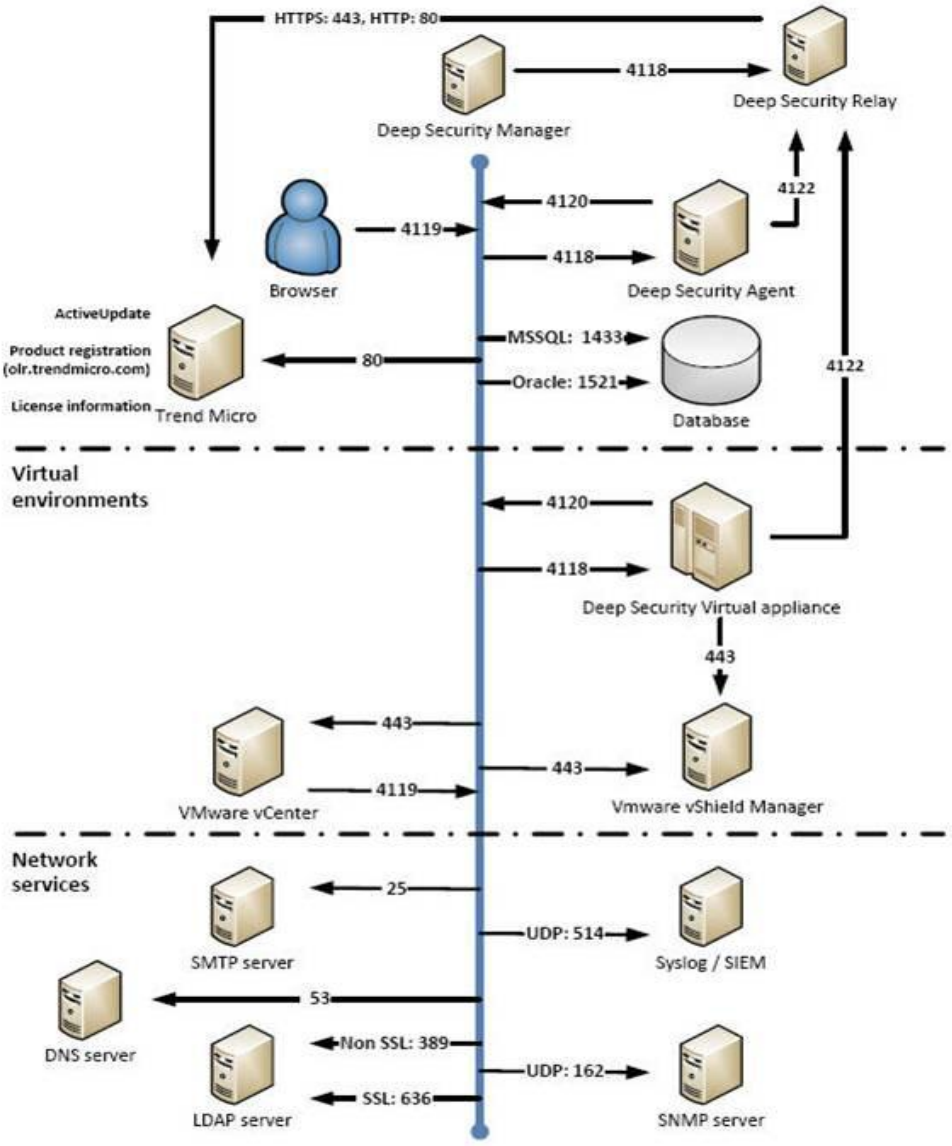
	ESXi	ESX/ESXi			
vShield Endpoint	5.x	4.1 U3	4.1 U2	4.1 U1	4.1
5.x	N	N	N	N	N
1.0 U3	N	Y	Y	Y	Y
1.0 U1	N	N	N	Y	Y
1.0	N	N	N	Y	Y

相关 VMware 支持信息，可以参考下列 VMware 文档:

- VMware Product Interoperability Matrixes
- Downloading and enabling vShield Endpoint 5.0/5.1 on supported vSphere platforms

Deep Security 通讯端口列表

下图列出了部署 DS 前，所需要开通的对应端口：


HTTPS: 443, HTTP: 80
4118
Deep Security Relay
Deep Security Manager
4122
4120
4119
4118
Browser
Deep Security Agent
ActiveUpdate
Product registration
(olr.trendmicro.com)
License information
80
Trend Micro
MSSQL: 1433
Oracle: 1521
Database
4122
Virtual environments
4120
4118
Deep Security Virtual appliance
443
443
VMware vCenter
4119
443
Vmware vShield Manager
Network services
25
SMTP server
UDP: 514
Syslog / SIEM
53
DNS server
Non SSL: 389
SSL: 636
LDAP server
UDP: 162
SNMP server

序号	源地址	目标地址	目标端口	方向
1	DSM	VC	443	单向
2	DSM	ESXi	443	单向
3	DSM	VSM	443	单向
4	DSM	DSVA	4118	单向
5	DSM	SQL	1433、1434	单向
6	DSM	TMAU	80、443	单向
7	DSVA	VSM	443	双向
8	DSVA	DSM	4119、4120、4122	单向
9	VSM	VC	443	双向
10	VSM	ESXi	443	双向
11	VSM	DSVA	443	
12	VC	DSM	4119	单向
13	VC	VSM	443	
14	ESXi	DSM	4119	单向
15	VC	VSM	443	
16	DSM	ESXi	443	单向
17	ESXi	DSM	4119	单向
18	VC	VSM	80,443	双向
19	ESXi	VSM	80,443	双向
20	VSM	ESXi	902,903	单向

Deep Security 平台支持列表功能

下面的表按版本（9.0、8.0、7.5 和 7.0）的趋势科技服务器深度安全防护系统客户端/虚拟设备列出了不同平台上支持的趋势科技服务器深度安全防护系统 8.0 的功能。表中信息的假设前提是您正在运行趋势科技服务器深度安全防护系统管理中心 8.0。

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）

趋势科技服务器深度安全防护系统客户端/虚拟设备 8.0 (SP1)

模块	功能	客户端 （8.0）					虚拟设备 （8.0）
		Windows	Linux	Solaris	AIX	HP-UX	ESX/ESXi 4.1、5.0
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	ESX/ESXi 4.1、5.0
Web 信誉服务	全部功能	●					●
		Windows	Linux	Solaris	AIX	HP-UX	ESX/ESXi 4.1、5.0
防火墙	全部功能	●	●	●			●
		Windows	Linux	Solaris	AIX	HP-UX	ESX/ESXi 4.1、5.0
DPI	IDS/IPS	●	●	●			●
	应用程序控制	●	●	●			●
	Web 应用程序防护	●	●	●			●
	SSL	●	●	●			
		Windows	Linux	Solaris	AIX	HP-UX	ESX/ESXi 4.1、5.0
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	ESX/ESXi 4.1、5.0
日志审查	全部功能	●	●	●	●	●	
		Windows	Linux	Solaris	AIX	HP-UX	ESX/ESXi 4.1、5.0
建议扫描	全部功能	●	●	●	●	●	
		Windows	Linux	Solaris	AIX	HP-UX	ESX/ESXi 4.1、5.0
用户通知	全部功能	●					● （使用通知程序）

趋势科技服务器深度安全防护系统客户端/虚拟设备 7.5

模块	功能	客户端（7.5）					虚拟设备（7.5）
		Windows	Linux	Solaris	AIX	HP-UX	ESX 4.1
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	ESX 4.1
Web 信誉服务	全部功能						
		Windows	Linux	Solaris	AIX	HP-UX	ESX 4.1
防火墙	全部功能	●	●	●			●
		Windows	Linux	Solaris	AIX	HP-UX	ESX 4.1
DPI	IDS/IPS	●	●	●			●
	应用程序控制	●	●	●			●
	Web 应用程序防护	●	●	●			●
	SSL	●	●	●			
		Windows	Linux	Solaris	AIX	HP-UX	ESX 4.1
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	ESX 4.1
日志审查	全部功能	●	●	●	●	●	
		Windows	Linux	Solaris	AIX	HP-UX	ESX 4.1
建议扫描	全部功能	●	●	●	●	●	
		Windows	Linux	Solaris	AIX	HP-UX	ESX 4.1
用户通知	全部功能						

趋势科技服务器深度安全防护系统客户端/虚拟设备 7.0

模块	功能	客户端（7.0）					虚拟设备（7.0）
		Windows	Linux	Solaris	AIX	HP-UX	ESX 4.0
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	ESX 4.0
Web 信誉服务	全部功能						
		Windows	Linux	Solaris	AIX	HP-UX	ESX 4.0
防火墙	全部功能	●	●	●			●
		Windows	Linux	Solaris	AIX	HP-UX	ESX 4.0
DPI	IDS/IPS	●	●	●			●
	应用程序控制	●	●	●			●
	Web 应用程序防护	●	●	●			●
	SSL	●	●	●			
		Windows	Linux	Solaris	AIX	HP-UX	ESX 4.0
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	ESX 4.0
日志审查	全部功能	●	●	●	●	●	
		Windows	Linux	Solaris	AIX	HP-UX	ESX 4.0
建议扫描	全部功能	●	●	●	●	●	
		Windows	Linux	Solaris	AIX	HP-UX	ESX 4.0
用户通知	全部功能						

Deep Security Manager 多节点部署步骤

准备工作：

1. 一台独立的 DB 服务器，安装有 SQL Server 或 Oracle
2. 已经部署一台 DSM Server

安装步骤：

1. 安装第一台 DSM 服务器(Node1)，DB 指向独立的 DB Server 服务器
2. Node 1 安装完毕后，在其他服务器上运行 DSM setup 程序安装 Node2, Node3 以此类推

注意：所有 DSM 节点必须配置相同的数据库服务器和数据库

3. 从安装第二个节点的 DSM 服务器开始，DSM 安装程序在安装时会提示用户是否添加一个节点，你只需根据向导选择添加一个新节点即可。

后续安装步骤与部署 DSM 单节点服务器步骤完全相同。

4. 验证多节点 DSM 是否部署成功
   a) 登录到任意一台 DSM 服务器
   b) 进入“系统 > 系统信息”页面确认是否已经识别了多个节点。

DSVA 保护超过 25 台 VM 时，DSVA 的内存推荐值，ESX 的 Heap Memory 增加值和计算方法

当 DSVA 安装在单一的 ESX 服务器，使用预设设置便可以保护 25 台虚拟机，然而，如果您在 ESX 服务器上需要保护超过 25 台虚拟机时，您需要按照以下方案修改配置。
要永久增加 fast path driver 内的 heap memory 最大值，您需要登录到 ESX shell 命令行控制台执行“esxcfg-module”命令，并设定最大 heap memory 值，此数值以 字节为单位。

例如，您需要保护 32 台虚拟机，请按照以下步骤设定适当的数值。
公式为：
<虚拟机数量> * 10MB

所以 32 台虚拟机所需字节数为：
32 * 10 = 320 MB = 335544320 Byte

执行以下命令：
% esxcfg-module -s DSAFILTER_HEAP_MAX_SIZE=335544320 dvfilter-dsa

要使配置更改生效，需要重新加载驱动。推荐在更改设置以后对 ESX 服务器执行重启操作，或通过以下命令重新加载驱动程序：

```
% esxcfg-module -u dvfilter-dsa
% esxcfg-module dvfilter-dsa
```

附注：以上命令执行时，需要先关闭 ESX 上所有虚拟机

如何安装 vShield Endpoint 5.0 驱动程序？

在 VMWARE Guest 虚拟机下载并安装 VMware-tools-8.6.0-446312-i386.msi 文件，选择自定义安装，确保选择安装 VM Tool 时勾选 VMCI 驱动中的“vShield Drivers”项目，如图：

完成安装

如何为 ESXi5.0 使用 Update Manager 安装 vShield Manager 补丁

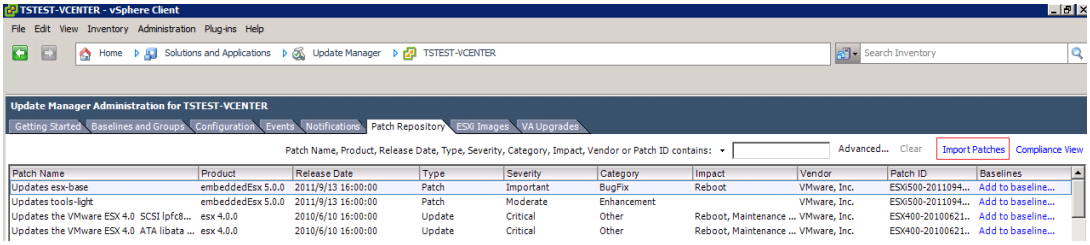
这个补丁程序通常通过 Vmware Update Manager 程序部署,具体步骤如下:

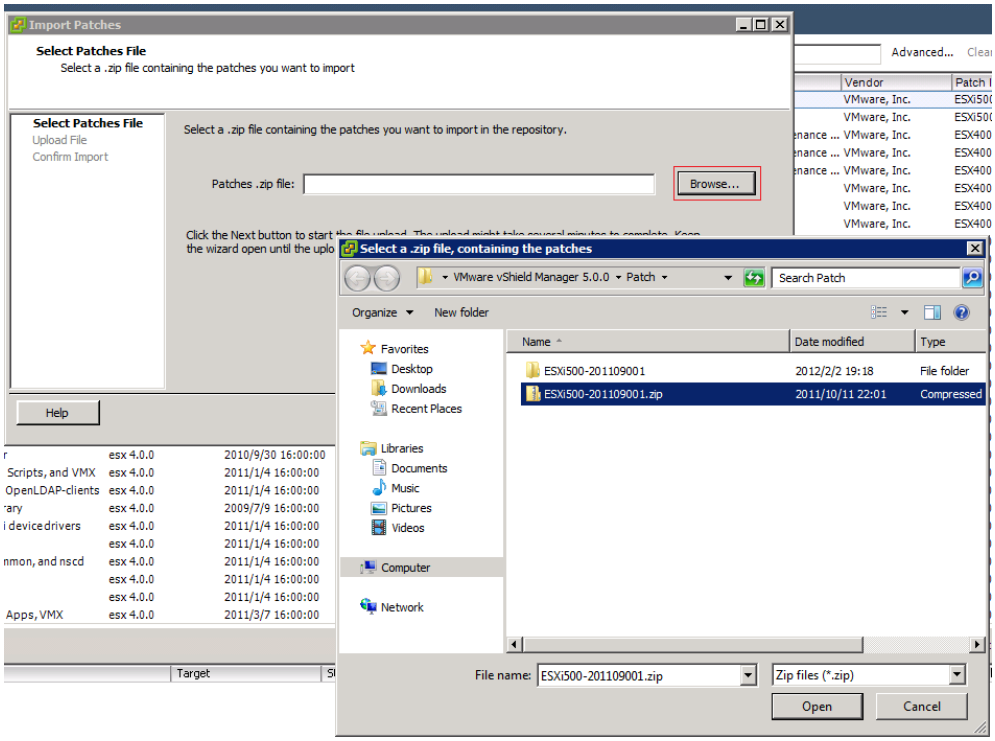
确保已经安装 Update Manager Server 和 Update Manager client

从 Vmware 官网下载补丁程序 ESXi500-201109001

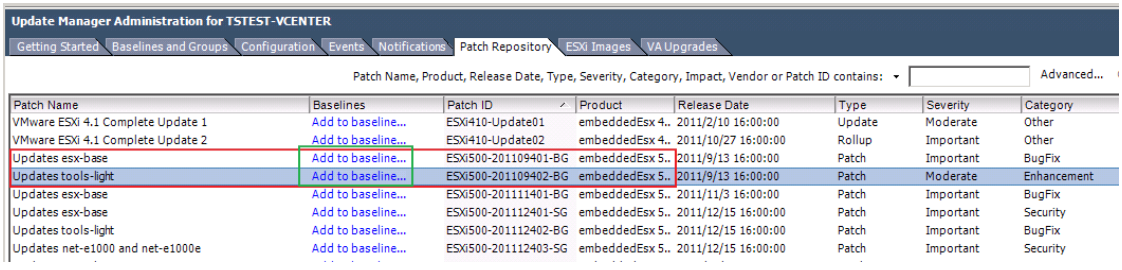
https://hostupdate.vmware.com/software/VUM/OFFLINE/release-313-20110906-767411/ESXi500-201109001.zip

在 Update Manger 控制台中导入补丁,如图所示

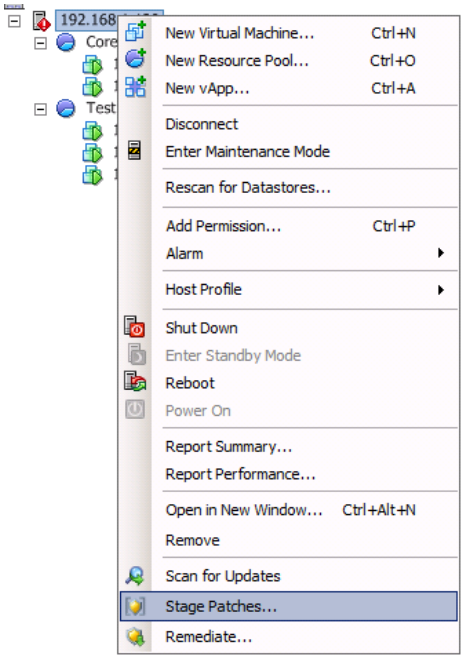




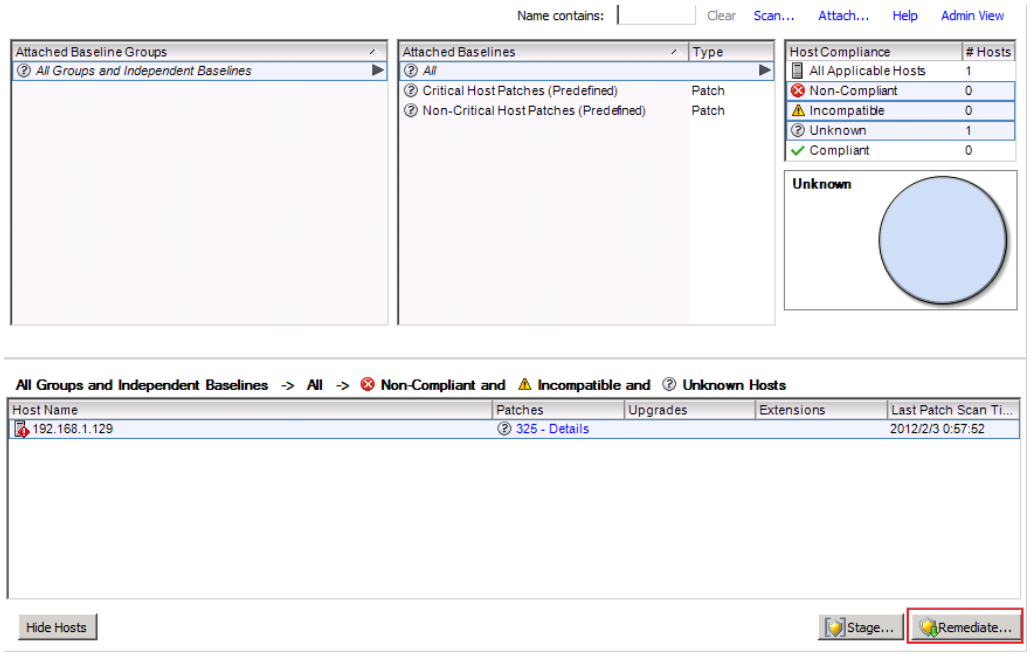
把补丁添加到'baseline'如图:



向 ESXi5.0 服务器推送补丁



向 ESXi 部署补丁



Deep Security 9.0 支持从哪些版本升级？

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》。

Deep Security 8.0 SP1 支持从哪些版本升级？

Deep Security 8.0 SP1 支持从 Deep Security 7.5 或 Deep Security 8.0 升级。

Deep Security 9.0 是否支持 ESX/ESXi4.1 环境

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。

Deep Security 9.0 是否支持 ESXi5.5 环境

Deep Security 9.0 SP1 Patch 2 版本开始支持 ESXi5.5 版本，如需在 ESXi5.5 环境下部署 DS，请安装该版本

Deep Security 8.0 SP1 是否支持 ESX/ESXi4.1 和 ESXi5.0 混合虚拟化环境？

是的，Deep Security 8.0 SP1 同时支持 ESX/ESXi4.1 与 ESXi5.0 虚拟化环境，关于支持虚拟化环境的详细内容请参考趋势科技中文知识库 71957

如何批量升级虚拟机 Vm Tools，并加载 vSheld Endpoint Thin Driver 驱动

前提条件

当前的 VM 虚拟机已经部署有 VM Tools

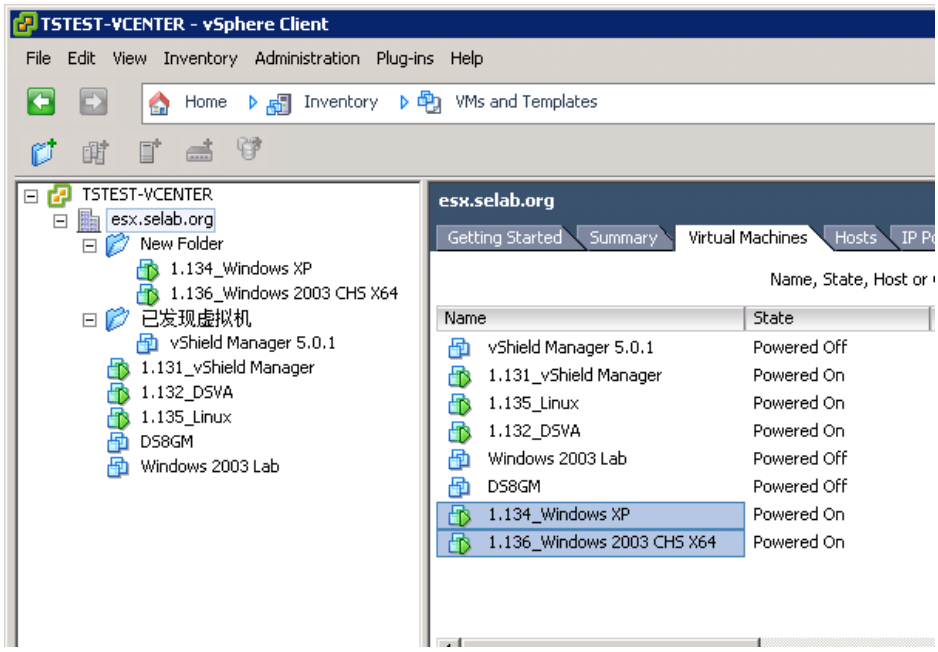
ESXi 5.0 已经安装 patch ESXi500-201109001 补丁程序

具体步骤如下：

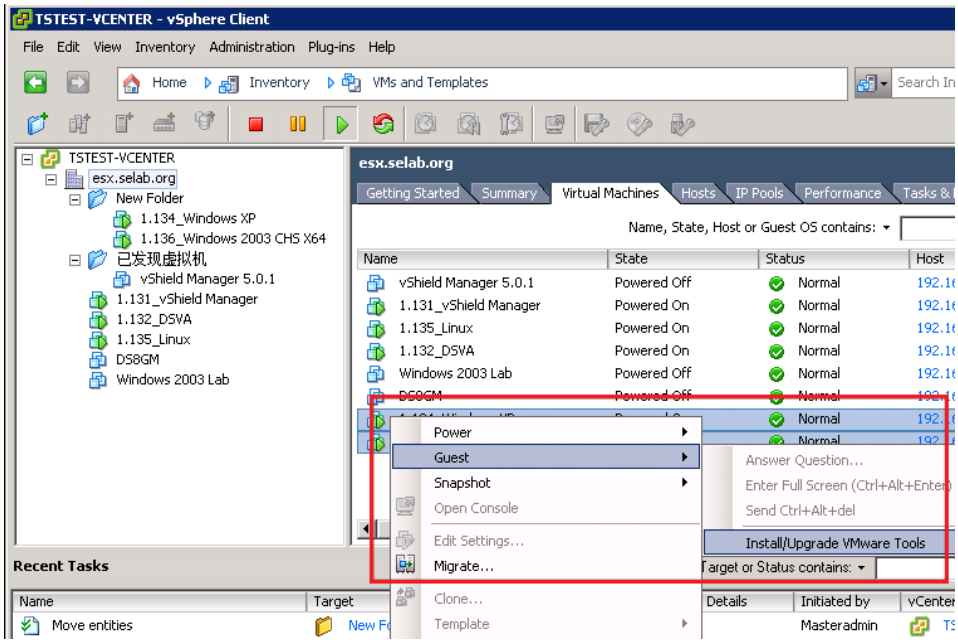
进入 VC 管理控制台

进入 Home > Inventory > VMs and Templates

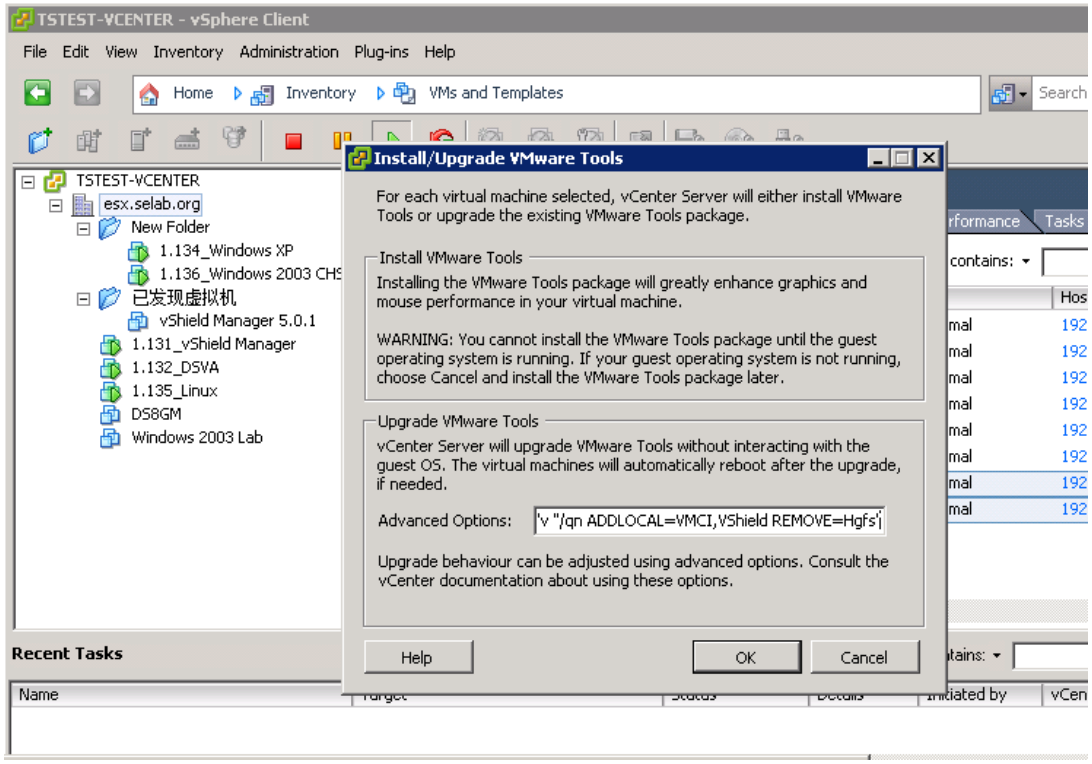
选中需要升级 VMTOOLS 的虚拟机，如图：



右键点击被选中的虚拟机 > Guest > Install/Upgrade Vmware Tools



在弹出升级 VM TOOLS 窗口文本框中输入命令： /v "/qn ADDLOCAL=VMCI,VShield REMOVE=Hgfs" 按 OK 执行 VM TOOLS 升级

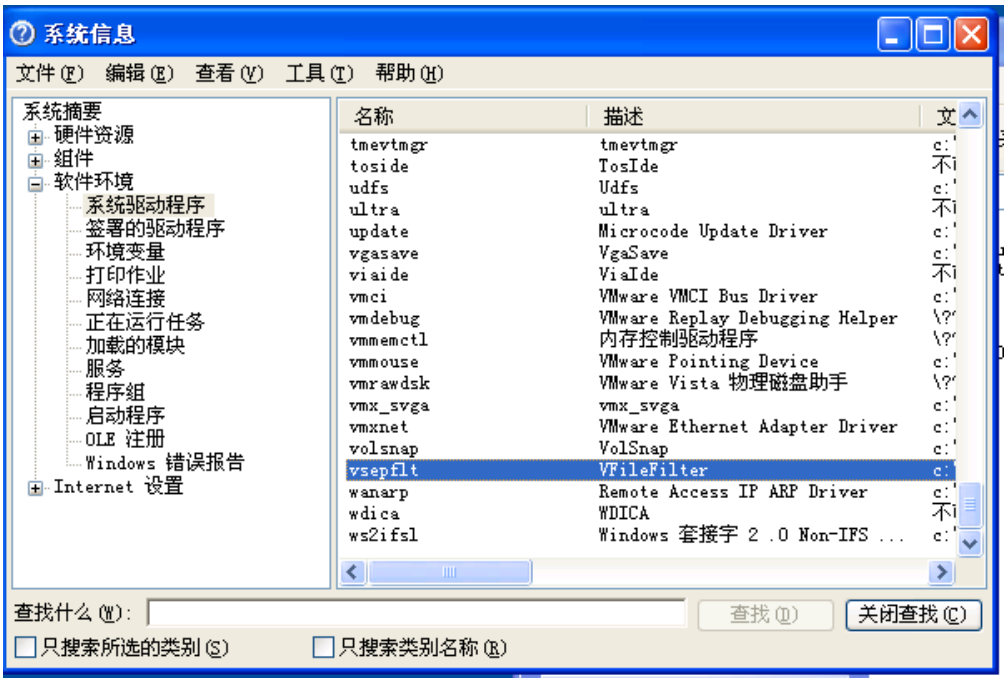


虚拟机会自动升级 VM TOOLS 工具并加载 vShield Endpoint 模块

登录虚拟机确认 VM TOOL 中的 vShield Endpoint 模块是否安装

For Windows XP/2003

在“开始”---“运行” 中输入 winmsd ，然后检查系统驱动程序中是否 vsepflt 驱动，如图：



For Vista /Win7/2008

在运行中输入 msinfo32,打开系统信息程序，同样确认系统驱动程序中是否包含 ‘vsepflt’驱动程序。

关于 VM TOOL 安装升级相关命令还可以参考 VMWARE 在线帮助文档，

http://pubs.vmware.com/vsphere-50/index.jsp?topic=/com.vmware.vmtools.install.doc/GUID-CD6ED7DD-E2E2-48BC-A6B0-E0BB81E05FA3.html

二. 策略设置

Deep Security Anti-malware 对于 Domino 服务器的推荐例外设置是什么？

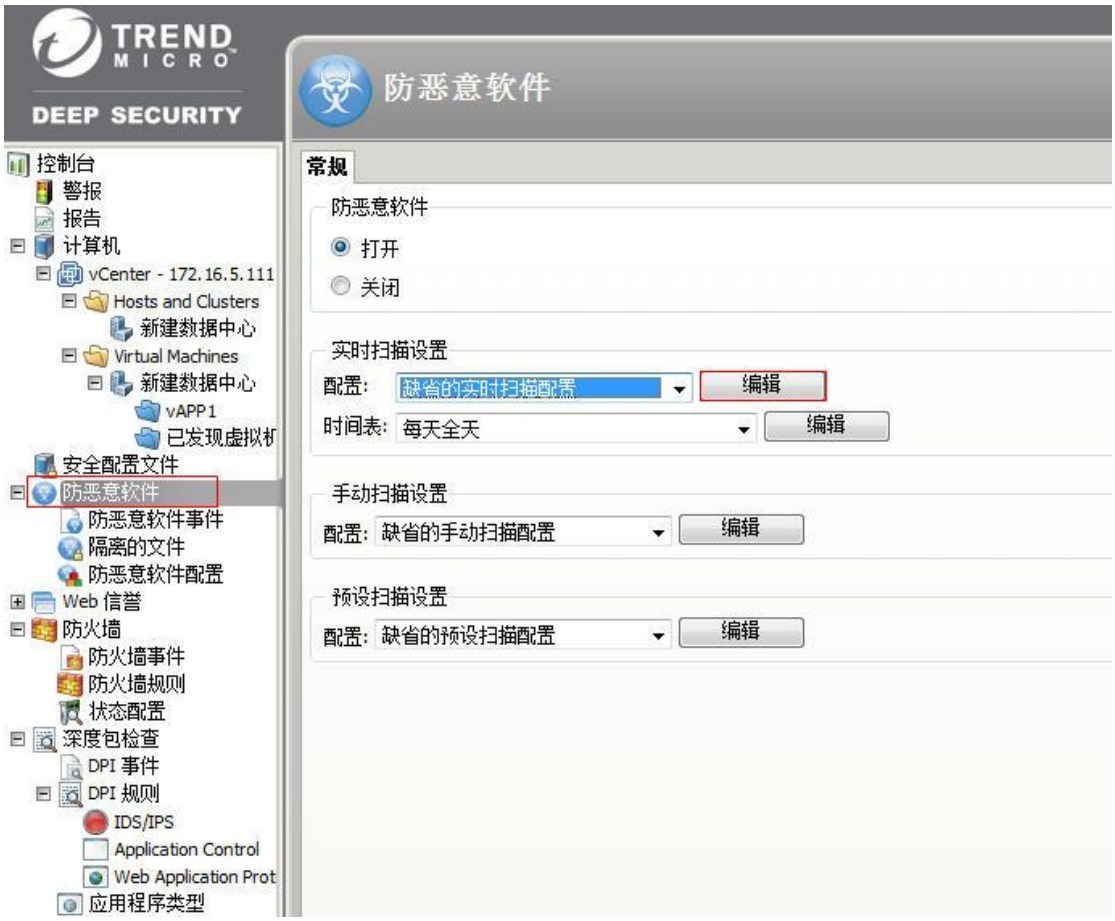
对于 domino 服务器建议把服务器的数据目录添加到例外 <drive>: \Lotus \ Domino \ Data.

Deep Security Anti-malware 模块扫描优化配置

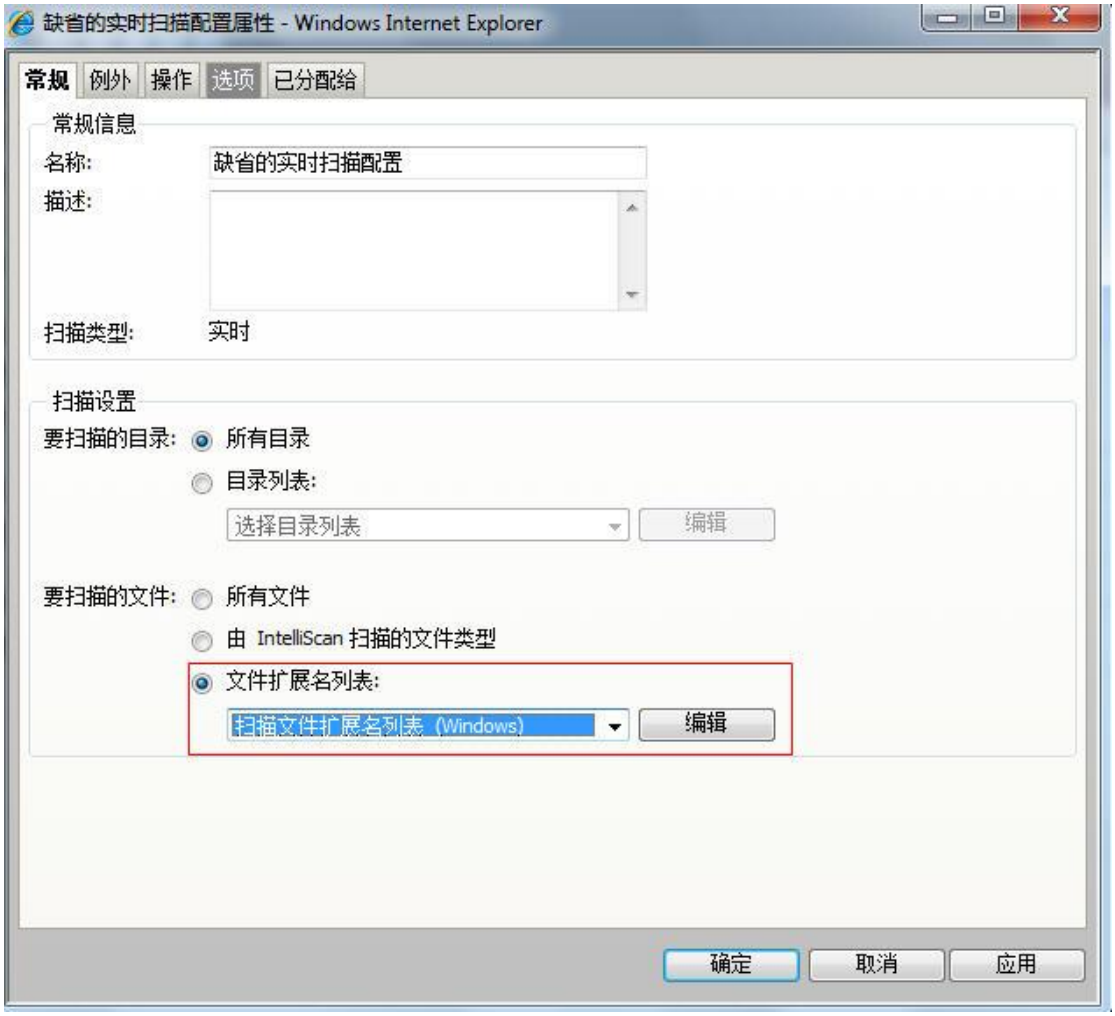
对于 DS 的防病毒模块，建议参考如下配置来优化扫描性能：

1) 登录 DSM 控制台

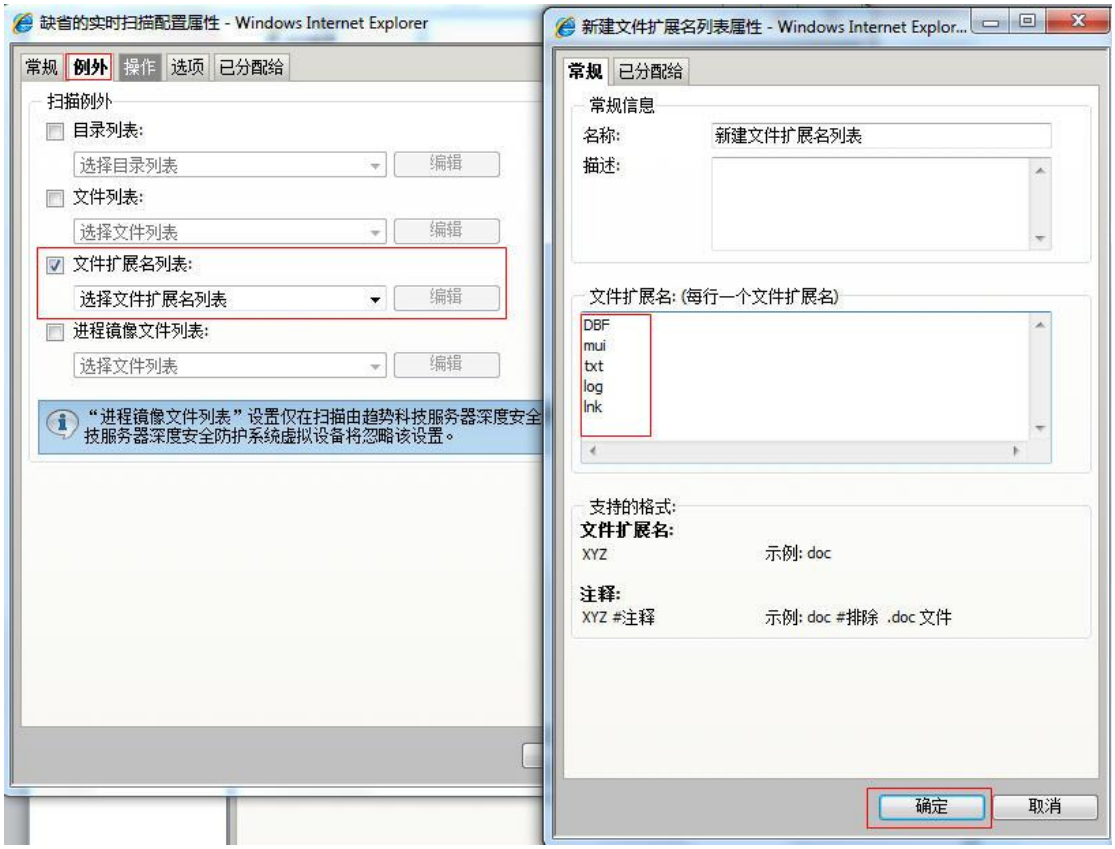
2) 点击“防恶意软件”选项卡，然后点击“实时扫描设置”的“编辑”选项



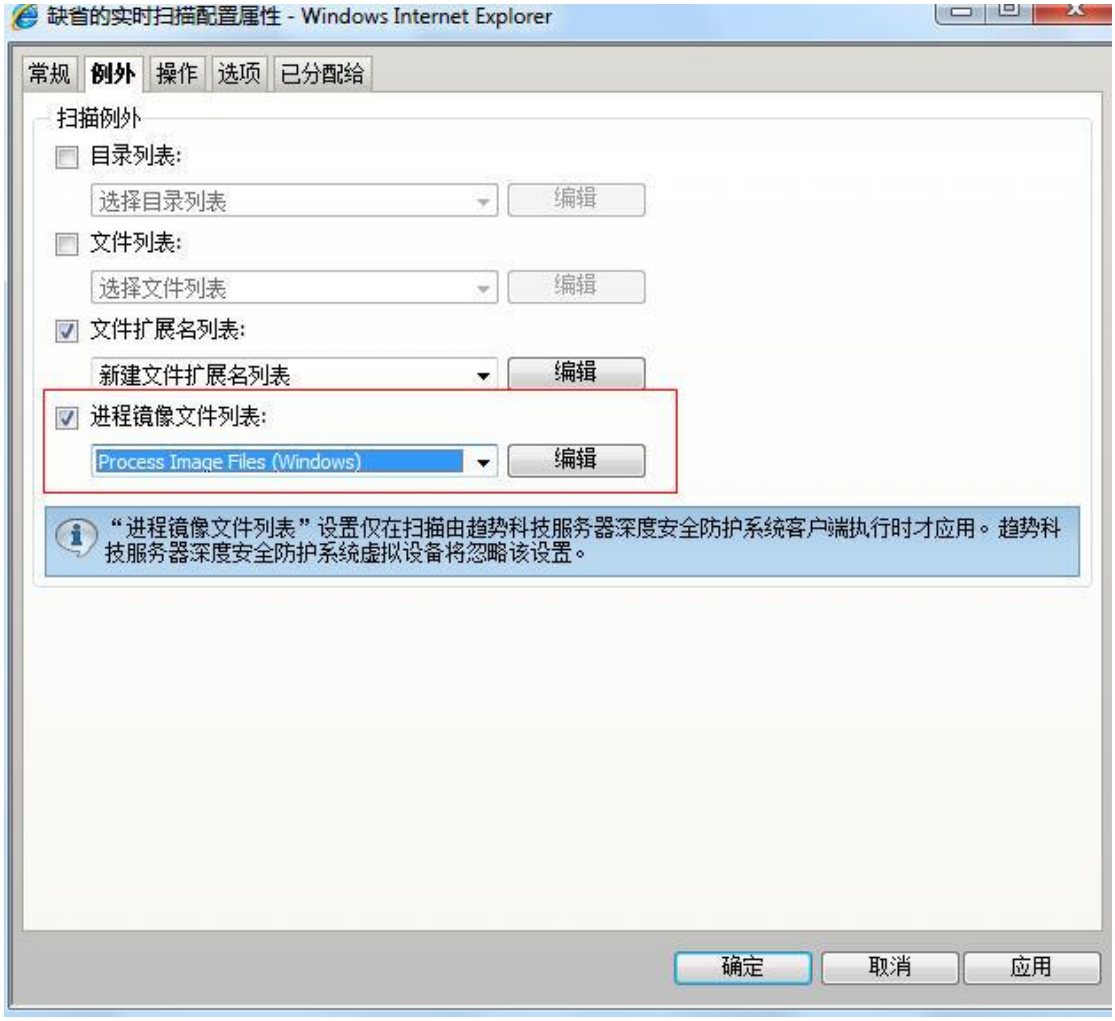
3) 在“常规”选项卡中，勾选“扫描文件扩展名列表（windows）”



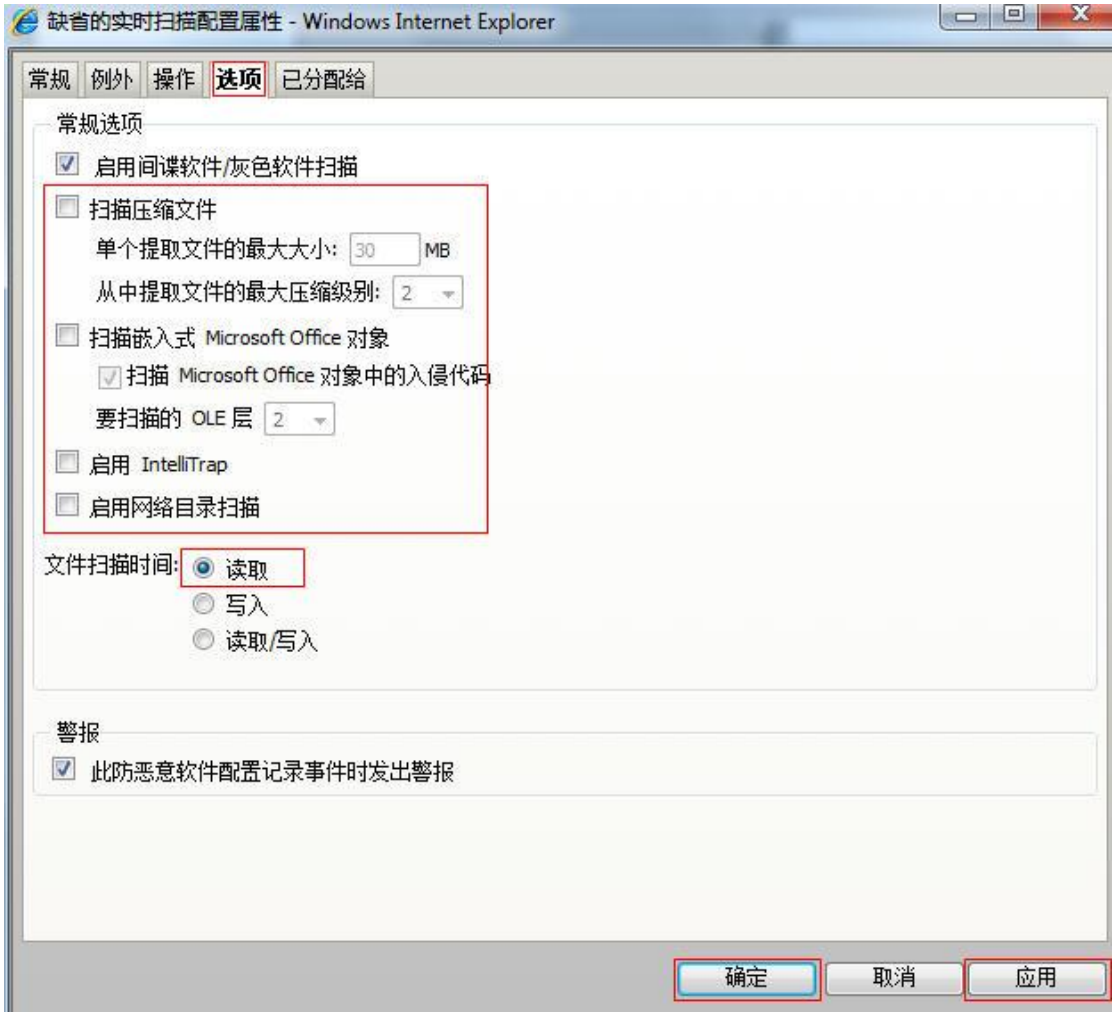
4) 单击“例外”选项卡，将 DBF、mui、txt、 log、 lnk 等扩展名类型设置为例外，设置完成后点击“确定”



5) 勾选“进程镜像文件列表”，选择“Process Image Files (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”



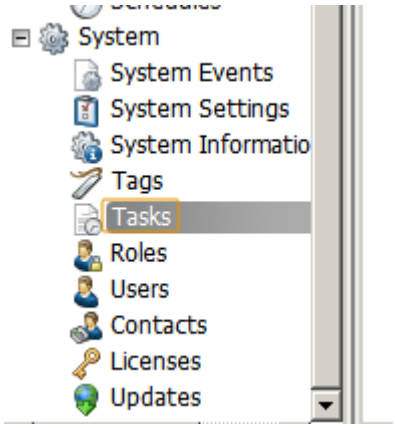
7) 点击“系统设置”，选择“恶意软件”选项卡，要“扫描的最大文件大小”设置为 2M，点击“保存”

如何针对自动创建的虚拟机和移动的虚拟机进行自动激活和分配策略?

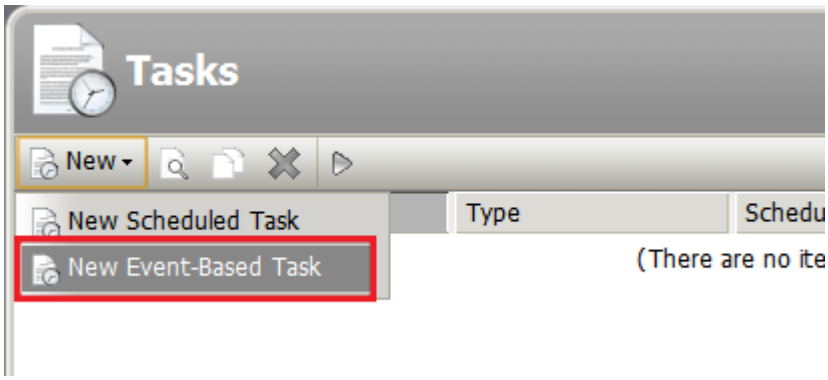
对于被 DSVA 保护的 VMware 虚拟机如果工作在”High Availability” 或 “VMware Distributed Resource Scheduler” 时 vCenter 会根据策略对虚拟机执行 Vmotion 迁移到其他 ESXi 主机上，这可能会导致 VMware 虚拟机在 DSM 控制台上的出现状态异常。当 VM 发生跨 ESXi 主机迁移动作以后需要对受保护的 VM 执行重新激活动作。我们可以对 DSM 设定自动任务来完成对发生迁移虚拟机的自动重新激活操作。

如图所示：

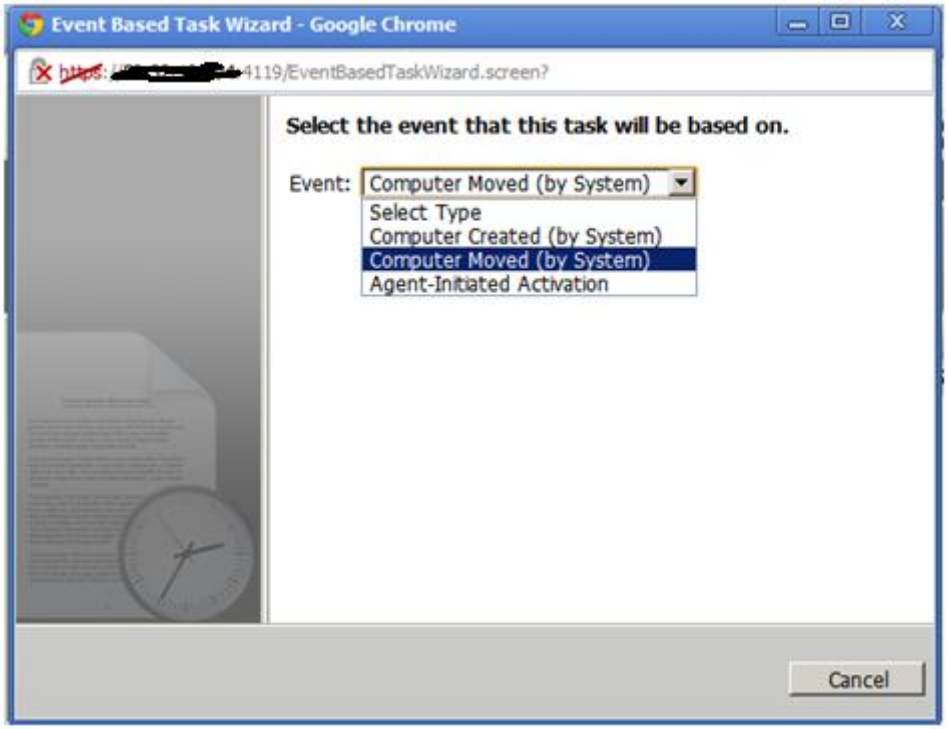
进入 DSM 控制台 > system > task 页面



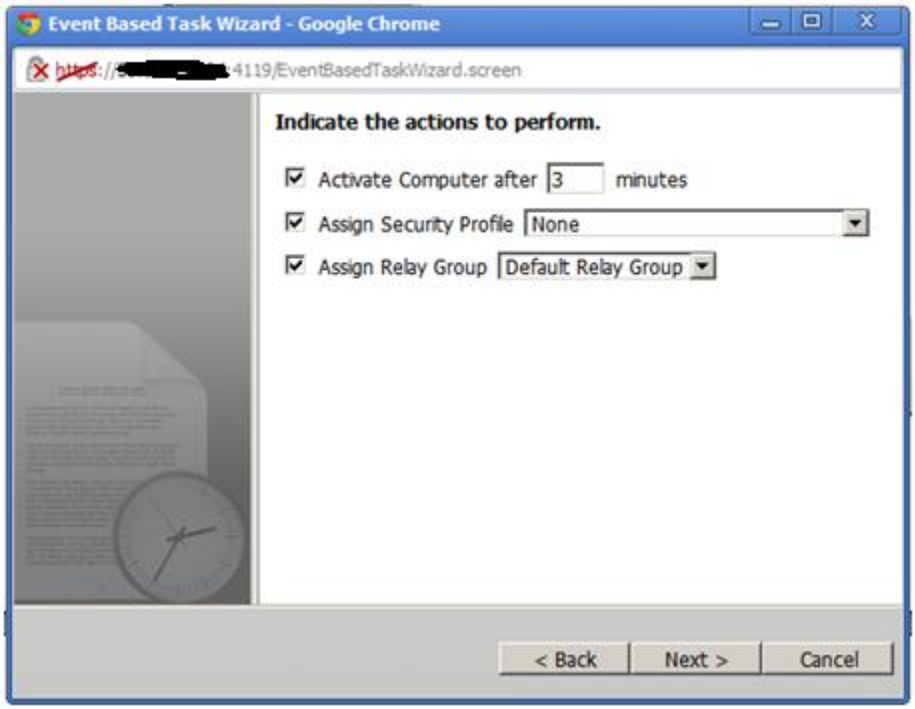
新建任务



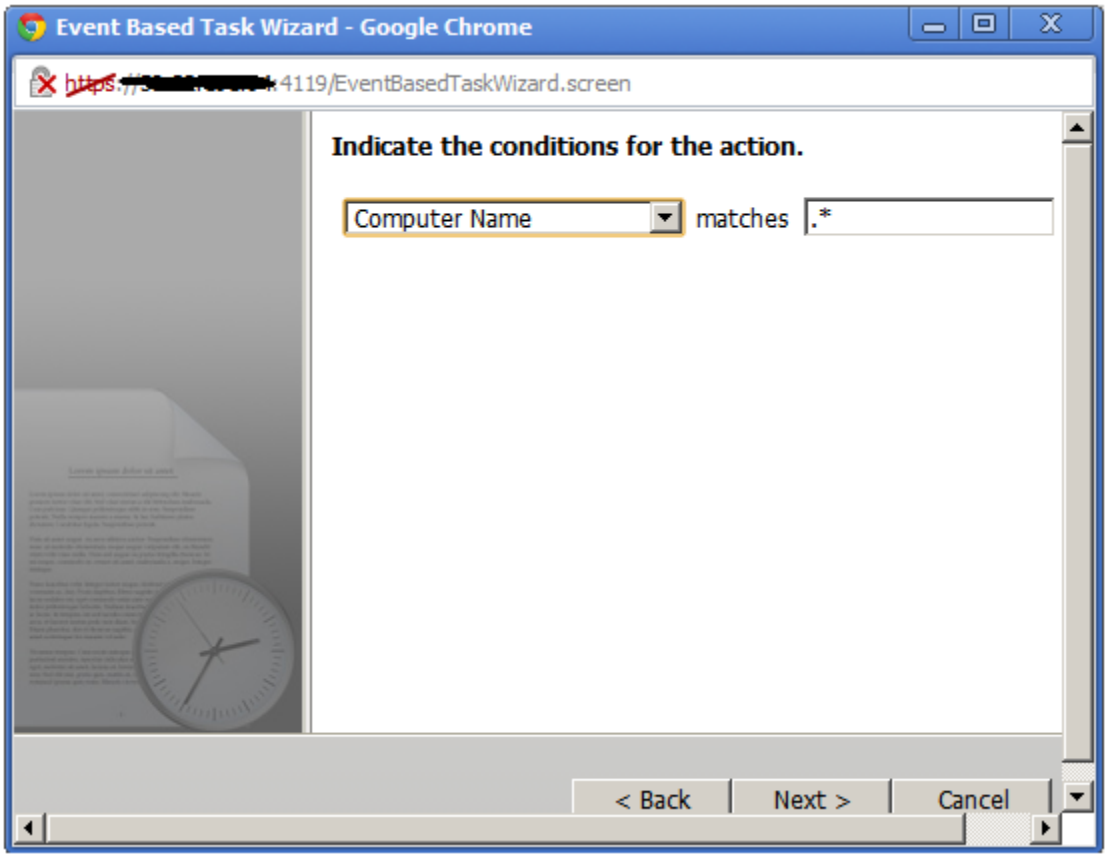
3) 设定触发任务的事件为”Computer Moved”



4) 设定时间触发以后自动执行的动作：



5) 设定 Action 条件

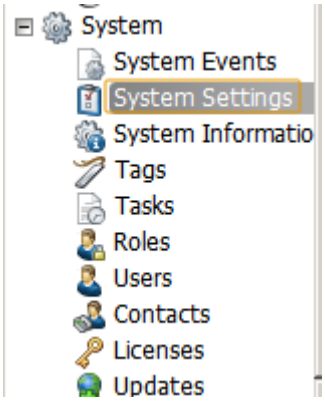


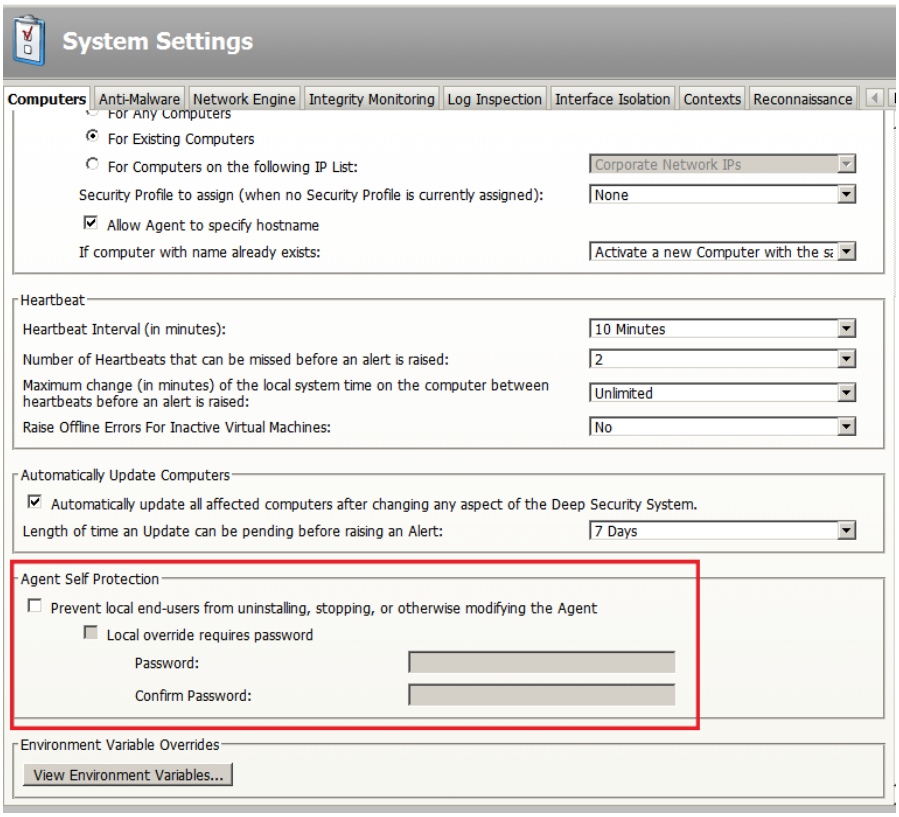
6）点击 finish 完成任务创建。

如何取消 DSA 8.0 客户端自我保护功能

方法一：对 DSA8.0 执行取消激活（Deactive）操作

方案二：进入 DSM 管理控制台取消 DSA 自我保护功能，如图：





当 DS8.0 工作在内外网隔离环境时如何更新 DS 产品组件？

可以通过 TMUT 离线更新工具对 DSM 8.0 进行组件更新，具体方法请联系趋势科技技术支持部门。

Deep Security 8.0 帐号被锁定时如何进行解锁

请按照如下方案进行操作：

1）.打开操作系统的命令提示符，转到 Deep Security 的安装目录，默认为：

C:\Program Files\Third Brigade\Deep Security Manager

2）.输入以下命令进行解锁：

dsm_c -action unlockout -username USERNAME

USERNAME 为您需要解锁的账号。

备注：默认 Deep Security 的管理员账号为：Masteradmin

当忘记 Deep Security Manager 登录密码时如何重置管理控制台密码？

要重置 DSM 管理控制台密码，请从命令行进入趋势科技服务器深度安全防护系统管理中心安装目录并输入以下命令：

dsm_c -action unlockout -username USERNAME -newpassword NEWPASSWORD

其中 USERNAME 是用户名，NEWPASSWORD 是为用户设置的新密码。

三. 常见故障处理

Deep Security9.0 在 ESXi5.5 环境下无法部署 Filter Driver，报错“The installation transaction failed”

针对该问题请参考如下方式来解决：

1、登录 DSM 服务器，打开 DOS 命令行

2、切换到 DSM 安装目录，如 C:\Program Files\Trend Micro\Deep Security Manager\

3、执行如下命令：

dsm_c -action changesetting -name "settings.configuration.filterDriverNoSigCheck" -value true

4、重启 DSM 服务

5、登录 DSM WEB 控制台，再次部署 Filter Driver，确认问题能否解决

为什么会出现 Smart Scan 中断问题

Deep Security 8.0 默认会启用 Smart Scan 扫描访问，当完成 DS 8.0 初次部署以后默认设置下 DSA 和 DSVA 会通过 Global Smart Scan Server 完成 smart scan，只要求网络中的每一台 DSA 或 DSVA 可以访问 internet。如果 Deep Security 环境中的 DSA 或 DSVA 无法访问公网那么就会出现 Smart Scan 中断的错误提示。

您可以公司内部部署本地云安全服务器来避免这个问题的发生,最新版本的本地云安全服务器可以从以下地址下载：
http://downloadcenter.trendmicro.com/index.php?regs=CH&clk=latest&clkval=3217&lang_loc=15

如何设置 Deep Security Smart Scan 指向本地云安全服务器,请参考 Deep Security 8.0 User Guide 文档

Deep Security 启用 DPI Event 日志中出现大量 " URI 中的字符非法 " 日志记录

要解决此问题，请参考中文知识库编号 72162

Deep Security 8.0 执行"准备"ESXi 服务器时提示“操作不成功----There was an error resolving dependencies.”

遇到此问题请先确认以下几点：

确认当前的 dvfilter 驱动版本是否与 ESXi 兼容，详细请参考 DS Installation Guide

确认 ESXi 在 VCENTER 中的 Host Image Profile Acceptance Level 设置，具体步骤：

a. 使用 vClient 登录 VC

b. 选中 ESXi 主机，并进入"Configuration" > "Security Profile"

c. 查看"Host Image Profile Acceptance Level"设定,确保 Acceptance Level 为“Vmware Accepted”

Deep Security 8.0 遇到更新问题时需要收集哪些信息？

当遇到 DS 8.0 更新问题时需要收集的日志信息有：

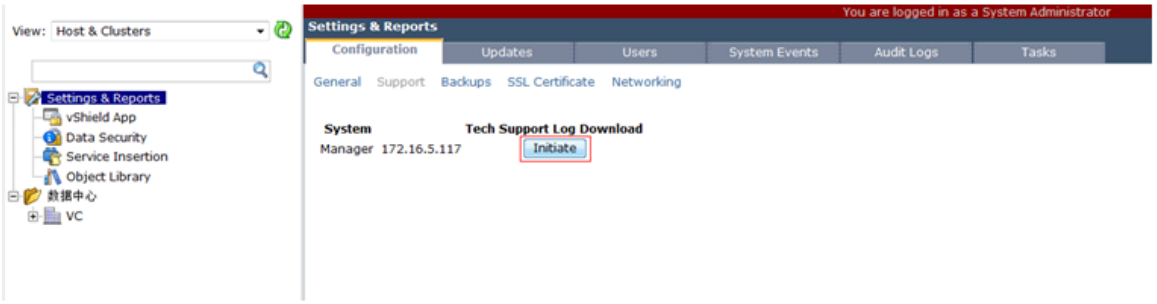
Deep Security Relay 诊断包程序

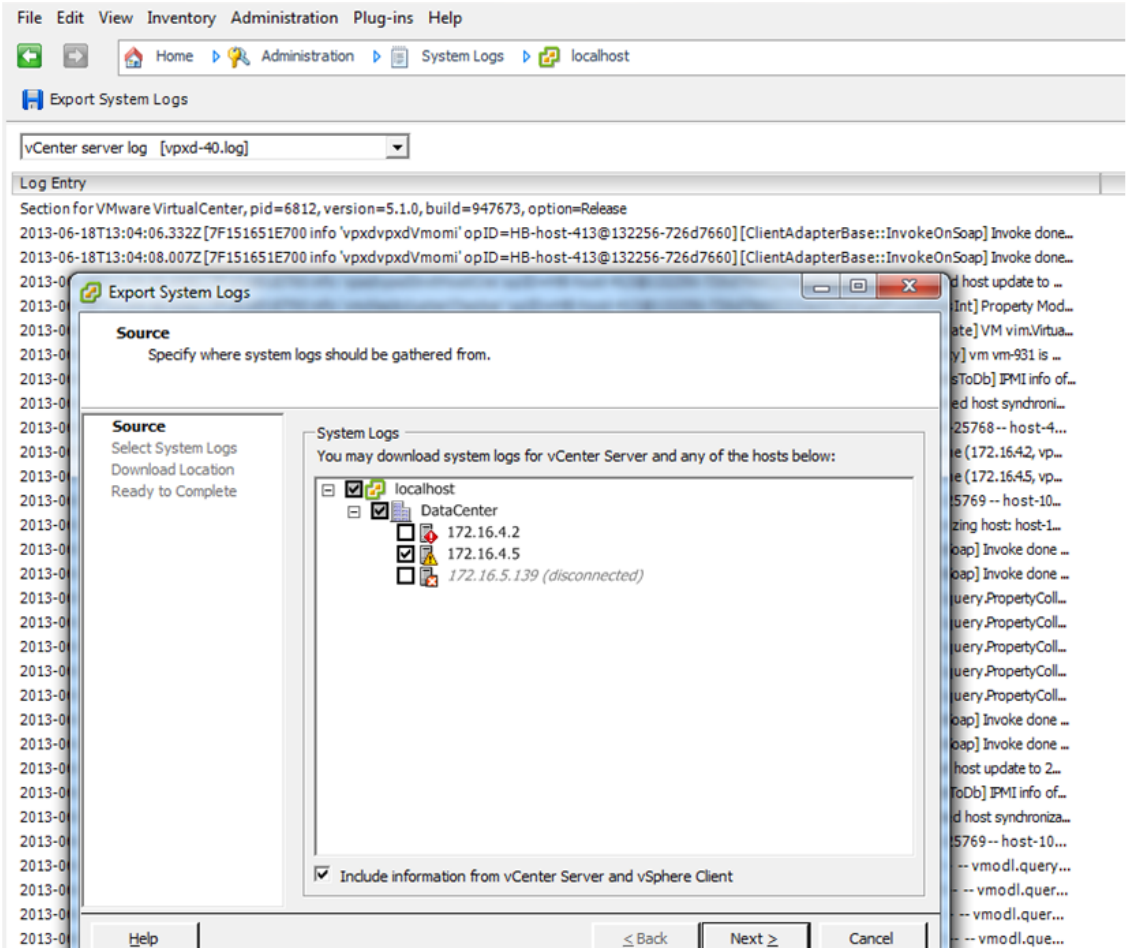
Deep Security Agent 或 Deep Security Virtual Agent 诊断包

具体收集步骤请参考中文知识库 71218

如何收集 vShield Manager 和 ESX 的日志

由于 DS 与 VMWARE 组件的紧密联动，有时在排查问题时需要收集 vShield Manager 和 ESX 的日志，具体收集方法参考如下截图设置：





Deep Security Manager(DSM)8.0 安装时提示“JVM could not be started”安装无法继续？

关于此问题是由于 Deep Security Manager 8.0 安装时所需的连续内存不足导致，这个问题通常比较容易发生在当DSM 部署在32bit 操作系统时，要解决此问题请参考趋势科技中文知识库 72001

Deep Security Agent 执行恶意软件手动扫描时提示报错“于客户端/设备发生以下错误，无法完成此操作：-1”应如何处理？

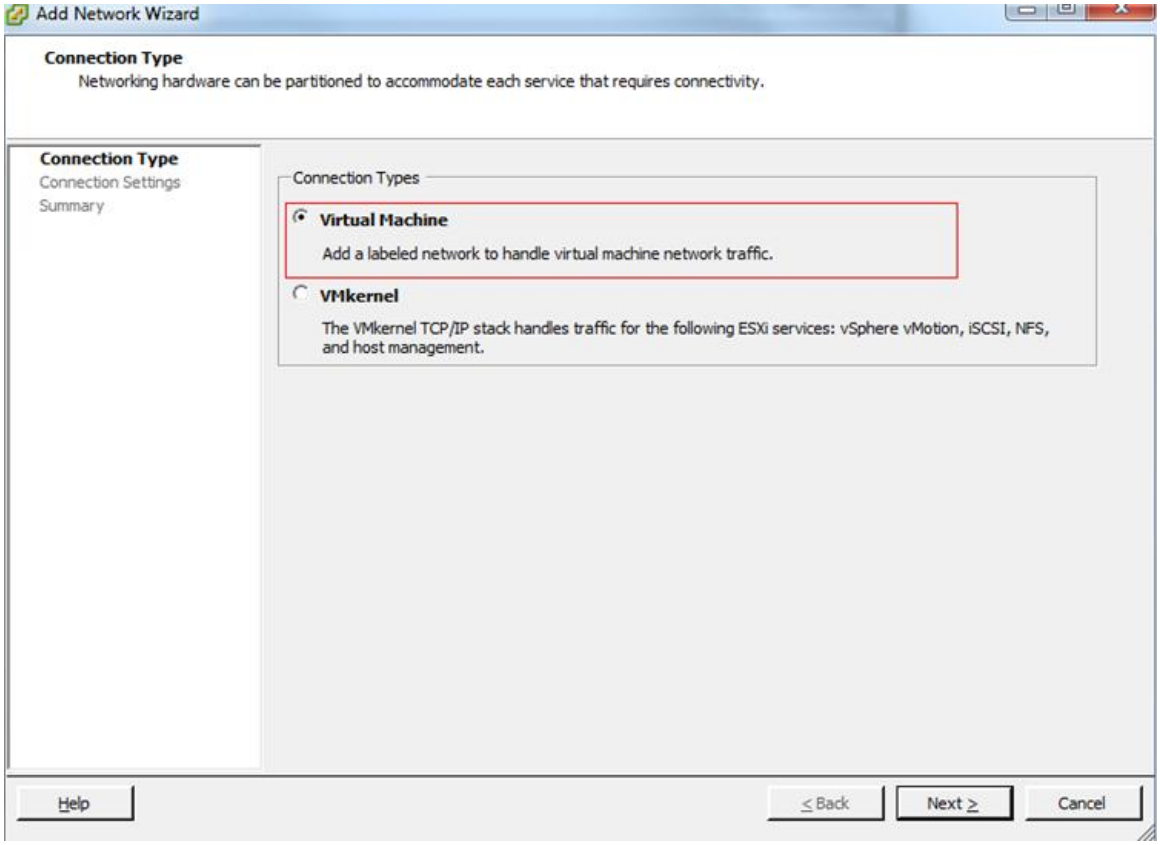
此问题通常发生在 DSA 初次部署成功执行组件更新时发生，要解决这个问题请先确保 Deep

Security Agent 已经成功完成了一次组件更新操作，并确保所有防恶意软件组件已经成功更新。

DSVA 部署失败，无法激活，提示“无法激活客户端设备……”

无法激活 DSVA，提示如下报错：

出现此问题，请检查部署 DSVA 时，选择的管理网络是 VMkernal 还是 Virtual Machine,管理网络的连接类型必须是 Virtual Machine，不能是 VMkernal



四. 其他

Deep Security Relay 的作用是什么？

Deep Security Relay 可直接部署于计算机上，可用于中转趋势全球 iAU 的更新至 Deep Security。
Deep Security Relay 支持更新 Deep Security 8.0 的 VSU, software 列表, AV 组件
至少具备一个 DEEP SECURITY Relay ，为符合扩展性和可用性要求也可以部署多个 DS Relay
在较小型的环境中，relay 服务器可以和 DSM 安装在同一台机器上
Deep Security Relay 包含完整的 DSA 功能
Deep Security Relay 支持多平台 (Windows / Linux)
DSM 将继续支持原 AU，直到 DSVA 7.x 被废弃

Deep Security 7.5 的激活号是否可以用来激活 Deep Security 8.0

是的，Deep Security 7.5 的激活号可以被用来直接激活 Deep Security 8.0 版本

Deep Security Agent 是否可以通过 DSM 管理控制台卸载？

不能，Deep Security Manager 只能执行远程取消激活 Deep Security Agent 操作，无法执行远程卸载操作。

当 DSA 无法与 DSM 通讯时是否支持离线更新？

DSA 在与 DSM 无法通讯时不能通过手动方式进行更新，因为在更新过程中 DSM 需要发送安全配置文件到 DSA 。

Deep Security 8.0 SP1 中新增功能无代理完整性监控是否支持实时监控?

由于 vShield Thin Driver 的限制，Deep Security8.0 无代理完整性监控暂时不支持实时监控功能