Cisco Security Manager 4.8 部署规划指南

首次发布日期：2015 年 3 月 6 日

简介

本文档提供 Cisco Security Manager 4.8 的部署规划指南。其中包含以下主题：包括的应用、推荐使用的服务器硬件、客户端硬件、根据参考网络确定规模和软件、安全管理器附带的一系列应用的部署选项、安全管理器服务器高级调整选项以及许可。有关安全管理器软件功能的详细信息，请参阅产品文档，网址为 http://www.cisco.com/go/csmanager。

本文档是对其他安全管理器用户文档（例如 *Cisco Security Manager 4.8 用户指南*和 *Cisco Security Manager 4.8 安装指南*）的补充。

Cisco Security Manager 4.8 应用

安装的每个 Cisco Security Manager 4.8 都包含六个主要应用和一个专为移动设备设计的应用：

- 配置管理器
- 事件查看器
- 报告管理器
- 运行状况和性能监控器
- 映像管理器
- 控制面板
- CSM Mobile

配置管理器

通过配置管理器，可以集中管理超过 250 个不同类型和型号的思科安全设备的安全策略。安全管理器支持跨以下设备集成调配防火墙、IPS 和 VPN（大多数站点到站点 VPN、远程接入 VPN 和 SSL VPN）服务：

- IOS/ISR/ASR 路由器
- Catalyst 交换机
- ASA 和 PIX 安全设备
- 与防火墙、VPN 和 IPS 相关的 Catalyst 服务模块
- 适用于路由器和 ASA 设备的 IPS 设备和各种服务模块

有关安全管理器所支持设备和操作系统版本的完整列表，请参阅 Cisco.com 上的 *Cisco Security Manager 支持的设备和软件版本*。

事件查看器

通过易于使用的高性能集成事件查看器，可以集中监控 IPS、ASA 和 FWSM 设备中的事件，并将这些事件与相关的配置策略关联。这有助于您确定问题并排除配置故障。然后，可以使用配置管理器调整配置并进行部署。事件查看器支持思科 ASA、IPS 和 FWSM 设备的事件管理。

除了主要事件数据存储区之外，还可以复制事件并将其存储在扩展事件数据存储区中。扩展事件数据存储区可用于备份和存档大量事件。这对于查看和分析事件查看器可以从主要事件数据存储和扩展事件数据存储收集其事件数据的事件历史记录很有用。扩展事件数据存储区可以在安全管理器的管理设置的“事件管理”(Event Management) 中启用。

有关受支持的平台和详细信息，请参阅 Cisco.com 上 *Cisco Security Manager 4.8 用户指南*和 *Cisco Security Manager 支持的设备和软件版本*的“监控、报告和诊断”部分。

报告管理器

通过集成的报告管理器应用，可以生成和安排 ASA、IPS 和远程接入 VPN 报告。ASA 和 IPS 设备的报告通过汇聚和总结事件查看器收集的事件而创建。安全报告可用来高效地监控、跟踪和审核受管设备报告的网络使用情况和安全问题。用户可以使用报告管理器为思科 ASA 和 IPS 设备开发和定制报告。

有关受支持的平台和详细信息，请参阅 Cisco.com 上 *Cisco Security Manager 4.8 用户指南*和 *Cisco Security Manager 支持的设备和软件版本*的“监控、报告和诊断”部分。

运行状况和性能监控器

运行状况和性能监控器具有以下功能：

- 为 ASA、VPN 和 IPS 设备提供监控功能
- 为关键指标提供趋势图
- 提供一个摘要面板，以便在一个视图内显示整合的运行状况、警报和指标值信息。
- 为不同的监控参数提供一种警报机制
- 提供一组预定义的监控视图
- 允许用户创建、编辑和删除自定义监控视图

映像管理器

映像管理器提供对 ASA 设备的完整映像管理。具体而言，它通过执行以下操作帮助用户完成 ASA 映像升级过程的各个阶段：

- 下载和维护不同类型和版本的映像的存储库
- 评估映像
- 分析将这些映像升级到设备所产生的影响（分析包括进行设备配置时升级所产生的影响）
- 准备和规划升级
- 利用内置的充分回退和恢复机制提供可靠且稳定的设备升级方式，确保将停机时间缩至最短

控制面板

控制面板是安全管理器的一个可配置启动点，可使 IPS 和 FW 任务的执行更简便。除原始的控制面板之外，您还可以创建其他新的控制面板，并且可以定制所有控制面板。使用控制面板，可以在一个位置完成分布于安全管理器多个其他区域的许多任务，例如“IPS 运行状况监控器”(IPS Health Monitor) 页面、报告管理器、运行状况和性能监控器和“IP 智能设置”(IP Intelligence Settings)。

CSM Mobile

通过 CSM Mobile，可以从移动设备访问设备运行状况摘要信息。通过这种方式向您提供的信息与控制面板中“设备运行状况摘要”(Device Health Summary) 构件提供的信息相同：HPM 当前生成的高度或中度严重性主动警报。警报可以根据警报说明、预定义类别、设备或警报技术分组。

CSM Mobile 的主要用户预期为使用 Apple iPad、Apple iPhone、Google Chrome 浏览器或 Apple Safari 浏览器的用户。

系统日志中继

事件除了由安全管理器服务器进行接收之外，还可以转发到最多两个外部/远程控制器（系统日志主机）。该系统日志中继功能会将收到的消息转发到使用 UDP 系统日志协议的另一个系统日志主机。

保留消息的原始源地址

此功能提供保留消息的原始源 IP 地址的选项。也就是说，用户是否希望显示在远程控制器源 IP 地址收到的事件。这是默认配置。

使用 CSM 服务器 IP 地址作为源 IP 地址

在配置文件中启用此选项后，从安全管理器服务器转发的所有系统日志消息都使用安全管理器服务器的 IP 地址作为系统日志消息的源 IP 地址。

有关配置和设置的详细信息，请参阅 Cisco.com 上的 *Cisco Security Manager 4.8 用户指南*。

小心 欺骗 IP 地址必须在获得网络策略允许的情况才能实现。

Common Services 4.2.2

安全管理器 4.8 和自动更新服务器 4.8 需要有 CiscoWorks Common Services 4.2.2（下称“Common Services”）才能正常工作。默认情况下，当您选择安装安全管理器 4.8 和自动更新服务器 4.8 时，也会安装 Common Services。

Common Services 提供数据存储、登录、用户角色定义、访问权限、安全协议和导航的框架。它还提供安装、数据管理、事件和消息处理以及作业和流程管理的框架。Common Services 为安全管理器提供至关重要的服务器端组件，包括：

- SSL 库
- 嵌入式 SQL 数据库
- Apache Web 服务器
- Tomcat servlet 引擎
- CiscoWorks 主页
- 备份和恢复功能

有关详细信息，请参阅安全管理器安装附带的 Common Services 文档。要执行此操作，请登录安装了安全管理器的服务器，双击 Cisco Security Manager 图标，登录，然后依次点击**服务器管理 (Server Administration)** 和**帮助 (Help)**。

使用 Common Services 的本地 RBAC

在安全管理器 4.3 之前的版本中，使用思科安全 ACS 的主要优势是：(1) 能够使用专用权限集创建高度精细的用户角色（例如，允许用户配置特定策略类型而不是其他类型）；(2) 能够通过配置网络设备组 (NDG) 限制用户访问某些设备。在安全管理器 4.2 及更早的版本中，不提供这些精细权限（有效的“基于角色的访问控制”，RBAC），除非使用的是思科安全 ACS。在安全管理器 4.3 及更高版本中提供这些精细权限 (RBAC)，因为这些版本使用的是无需通过 ACS 即可提供本地 RBAC 的 Common Services 4.0 或更高版本。有关详细信息，请参阅 *Cisco Security Manager 4.8 安装指南*。

自动更新服务器 4.8

使用自动更新服务器 (AUS)，可以在使用自动更新功能的 PIX 安全设备 (PIX) 和自适应安全设备 (ASA) 设备上升级设备配置文件和软件映像。AUS 支持拉模型的配置，您可以使用该模型进行设备配置、配置更新、设备操作系统更新和定期配置验证。此外，将动态 IP 地址与自动更新功能结合使用的受支持设备可以使用 AUS 升级其配置文件和传递设备和状态信息。

在此方法中，安全管理器会将配置更新部署到 AUS 服务器，然后受管设备会与 AUS 服务器通信，以按照定期的时间间隔、特定的日期和时间或按需下载新配置更新。

AUS 可提高远程安全网络的可扩展性、降低维护远程安全网络过程中产生的成本，并且让您能够管理动态寻址的远程防火墙。

AUS 使用基于浏览器的图形用户界面，并且需要 Common Services 4.2.2。有关 AUS 的详细信息，请参阅位于 http://www.cisco.com/go/csmanager 的文档。

相关应用

思科还提供了其他一些与安全管理器集成以提供附加功能和优势的应用：

思科安全访问控制服务器 (ACS) 4.2.x

您可以选择将安全管理器配置为使用 ACS 对安全管理器用户进行身份验证和授权。ACS 支持为精细的基于角色的访问控制 (RBAC) 定义自定义用户配置文件，并能够限制用户访问特定的一组设备或执行特定的一组操作。

有关配置安全管理器和 ACS 集成的详细信息，请参阅 *Cisco Security Manager 4.8 安装指南*。有关 ACS 的详细信息，可以访问 http://www.cisco.com/go/acs。

思科 CNS 配置引擎 3.5 和 3.5(1)

安全管理器支持使用思科配置引擎 3.5 和 3.5(1) 作为部署设备配置的机制。安全管理器会将增量配置文件部署到思科配置引擎，该文件存储在此处以便日后从设备进行检索。思科 IOS 路由器、PIX 和 ASA 防火墙等使用动态主机配置协议 (DHCP) 服务器的设备会与思科配置引擎通信，以获得配置（和映像）更新。安全管理器还支持通过 CNS 配置引擎管理具有静态 IP 地址的设备。在此类情况下，发现会实时完成，并通过 CNS 配置引擎部署到设备。

有关配置引擎的详细信息，可以访问 http://www.cisco.com/c/en/us/products/cloud-systems-management/configuration-engine/index.html。

最低硬件和软件要求

安装的每个安全管理器服务器都需要一个专用于配置管理器、事件查看器、报告管理器、运行状况和性能监控器、映像管理器和控制面板的物理服务器或虚拟机。自动更新服务器（可选组件）可以安装在同一系统上，也可以安装在单独的系统上。

表 1 列出了 Cisco Security Manager 服务器软件和其他可选模块安装的最低硬件和软件规格。虽然安全管理器软件在具有最低规格要求的系统上可以安装，但其性能和容量将限于进行较小型的部署（最多管理 25 台设备）。对于较大型的部署，应使用满足建议的硬件和软件规格部分建议的规格要求的物理服务器。

表 1　　服务器硬件和软件最低要求

服务器硬件最低要求	
建议使用的服务器	思科 UCS C220 M3 或同等设备
CPU	1 个 Intel Xeon 四核 5600 系列。此四个内核（四核）CPU 是最低要求。内核越多，性能越优。
内存 (RAM)	16 GB 是使用安全管理器所有功能的最低要求。内存小于此值，事件管理和报告管理等功能会受影响。 特别是，如果操作系统可用的 RAM 量小于 8 GB，则会在安装期间禁用事件查看器和报告管理器。 如果操作系统可用的内存介于 8 GB 和 12 GB 之间，则可以关闭事件查看器和报告管理器（假定您不打算使用这些功能）。此类系统中，可以使用配置管理功能。 完成安装后，可以通过安全管理器客户端在低内存系统中启用事件查看器和报告管理器（依次选择“工具”[Tools] > “安全管理器管理”[Security Manager Administration] > “事件管理”[Event Management]），但不建议这么做。请记住，在低内存系统中启用事件查看器和报告管理器可能会严重影响整个应用的性能。 如果在单独的服务器上安装 AUS，需要满足以下最低要求： • 仅 AUS 服务器，4 GB。我们建议使用 4 GB 以上。 **注意**　执行配置操作时，服务器的内存利用率（如 Windows 任务管理器所示）可能为 99%。这并非表示存在问题；这是正常现象，因为安全管理器的所有进程和功能都使用或分配各自的已分配内存。

表 1　服务器硬件和软件最低要求（续）

硬盘空间	使用合适的 HDD 组合获得所需的磁盘空间，如下： • 思科建议 100 GB 用于操作系统分区。 • 思科建议 150 GB 用于应用（安全管理器）分区。仅安全管理器安装所需的*最低*可用磁盘空间为 7 GB。如果达不到 7 GB，则安装将中止。 **注意**　思科强烈建议在单独的分区中安装此类操作系统和应用。 **注意**　当在 HA （高可用性）模式下使用 Veritas 时，上面所述的应用分区和任何其他事件存储区分区可能不相关。有关进一步的详细信息，请参阅相应的安全管理器高可用性文档 (http://www.cisco.com/c/en/us/support/security/security-manager/products-installation-guides-list.html) 和 Veritas 文档。 • 需要在单独的分区中为事件查看器提供额外的 1.0 TB 空间用于存储日志：仅当您计划使用事件查看器时才需要满足此要求。思科建议在直接连接存储设备上创建此单独分区。 • 提供额外的 1.0 TB 或更多空间：仅当您计划启用事件存档时才需要满足此要求。当所需的日志存储空间超出主存储容量（用于长期保存等）时，事件存档功能会为事件创建一个辅助存储。所需的辅助事件存储区大小应大于配置的主存储大小，因此，需要提供额外 1.0 TB 或更多磁盘空间才能使用事件存档功能。主要和辅助事件存储区可以位于 SAN 上，但建议在直接连接存储设备 (DAS) 上创建主要存储分区，以获得最佳性能。 要想获得更好的性能，思科建议使用 RAID 10。如果需要，也可以使用 RAID 5。将连续操作（并非大多数情况）的写入策略设置为写回；否则，请将写入策略设置为始终通写。将写入策略设置为通写也可以提高性能。 **提示** 如果每秒事件数 (EPS) 维持 10,000 个，则每天会耗用约 86 GB 压缩磁盘空间。耗用的磁盘空间占到为事件存储区（主要/辅助）分配的磁盘空间的 90% 时，会发生日志回滚。磁盘越小，回滚速度越快。根据您预期的 EPS 速率和回滚要求，在使用事件管理功能时，可以增加或减少最低磁盘大小。
支持的设备	最多 25 个
网络适配器	1 Gbps
服务器软件最低要求	
操作系统	以下项之一： • Microsoft Windows Server 2008 R2 SP1 Enterprise - 64 位 • Microsoft Windows Server 2012 R2 Standard - 64 位 • Microsoft Windows Server 2012 Standard - 64 位 • Microsoft Windows Server 2012 R2 Datacenter - 64 位 • Microsoft Windows Server 2012 Datacenter - 64 位

表 2 列出了 Cisco Security Manager 客户端软件安装的最低硬件和软件规格。思科建议在专用计算机上安装安全管理器客户端软件：

表 2　　客户端硬件和软件最低要求

客户端硬件最低要求	
CPU	双核 2.0 GHz 或更高
内存	32 位系统： • 最低：2 GB • 建议：大于 2 GB 64 位系统： • 最低：4 GB • 建议：大于 4 GB。
硬盘	10 GB 可用空间
显示屏	1280 x 1024
网络适配器	1 Gbps
客户端软件最低要求	
操作系统	以下项之一： • Microsoft Windows 7 SP1 Enterprise - 64 位和 32 位 • Microsoft Windows 8.1 Enterprise Edition - 64 位和 32 位 • Microsoft Windows Server 2008 R2 SP1 Enterprise - 64 位 • Microsoft Windows Server 2012 R2 Standard - 64 位 • Microsoft Windows Server 2012 Standard - 64 位 • Microsoft Windows Server 2012 R2 Datacenter - 64 位 • Microsoft Windows Server 2012 Datacenter - 64 位 安全管理器仅支持美国英语和日语版 Windows。从“开始”菜单打开 Windows 控制面板，打开用于配置区域和语言设置的面板，然后设置默认区域设置。（我们不支持将英语作为任何日语版 Windows 中的语言。）
浏览器	以下项之一： • Internet Explorer 8.x、9.x、10.x 或 11.x，但仅限在兼容性视图中 **注意** 当使用 Internet Explorer （任何版本）下载客户端时，请确保以下设置正确无误：Internet Explorer > “工具” > “Internet 选项” > “高级” > “安全” > 清除 “不将加密的页存盘”复选框。如果此设置不正确 （即已选中此复选框），则尝试下载客户端将失败。 • 支持并建议使用 Firefox 15.0.1 及更高版本

虚拟机硬件和软件要求

有关虚拟机硬件和软件的要求，请参阅表 3 与 VMware ESX 4.1 和 ESXi 5.5 及之前的 VMware ESXi 版本相关的小型部署。

建议的硬件和软件规格

经观察发现，当从单处理器（或核心）服务器转到多处理器（或核心）服务器时，安全管理器的性能会提高。思科建议您使用适当规格的硬件和软件，以获得最佳性能。思科还建议调整服务器的大小，以供将来扩展之用。

为了获得最佳性能，对安全管理器服务器的最低要求是采用 2.66 MHz Intel Xeon 四核或更快的处理器（具有超线程）。如果使用事件管理功能，强烈建议使用专用于安全管理器应用的硬盘或存储卷以及专用于事件存储的磁盘或卷。对于安全管理器客户端系统，可以使用本文档的*最低硬件和软件要求*部分指定的最低硬件规格。

以下规格列表是针对安全管理器服务器不同部署规模的建议规格：

- 与 VMware ESX 4.1 和 ESXi 5.5 及之前的 VMware ESXi 版本相关的小型部署
- 小型企业部署
- 中型企业部署
- 大型企业部署
- 大型零售部署

这些规格是根据设备数量确定支持此类部署所需的适当硬件和软件的一般准则；性能结果可能会因本文档部署方案一节讨论的其他因素而异。安全管理器的这些硬件和软件要求对于新安装以及从旧版安全管理器升级到版本 4.8 而言是相同的。

与 VMware ESX 4.1 和 ESXi 5.5 及之前的 VMware ESXi 版本相关的小型部署

表 3 列出了与 VMware ESX 4.1 和 ESXi 5.5 及之前的 VMware ESXi 版本相关的小型部署的建议安全管理器服务器规格：

表 3　　与 VMware ESX 4.1 和 ESXi 5.5 及之前的 VMware ESXi 版本相关的小型部署

注意 VMware 性能取决于同一主机系统上其他虚拟机产生的负载，因此，这些虚拟机的大小根据未处于其他虚拟机产生的重负载之下的系统得出。	
建议的主机服务器	思科 UCS C220 M3 或同等设备
虚拟 CPU	6 个 vCPU。vCPU 越多，性能越优。
内存 (RAM)	16 GB 是使用安全管理器所有功能的最低要求。内存小于此值，事件管理和报告管理等功能会受影响。 特别是，如果操作系统可用的 RAM 量小于 8 GB，则会在安装期间禁用事件查看器和报告管理器。 如果操作系统可用的内存介于 8 GB 和 12 GB 之间，则可以关闭事件查看器和报告管理器（假定您不打算使用这些功能）。此类系统中，可以使用配置管理功能。 完成安装后，可以通过安全管理器客户端在低内存系统中启用事件查看器和报告管理器（依次选择“工具”[Tools] >“安全管理器管理”[Security Manager Administration] >“事件管理”[Event Management]），但不建议这么做。请记住，在低内存系统中启用事件查看器和报告管理器可能会严重影响整个应用的性能。 如果在单独的服务器上安装 AUS，需要满足以下最低要求： • 仅 AUS 服务器，4 GB。我们建议使用 4 GB 以上。 **注意** 执行配置操作时，服务器的内存利用率（如 Windows 任务管理器所示）可能为 99%。这并非表示存在问题；这是正常现象，因为安全管理器的所有进程和功能都使用或分配各自的已分配内存。

表 3　与 VMware ESX 4.1 和 ESXi 5.5 及之前的 VMware ESXi 版本相关的小型部署（续）

硬盘空间	使用合适的 HDD 组合获得所需的磁盘空间，如下： • 思科建议 100 GB 用于操作系统分区。 • 思科建议 150 GB 用于应用（安全管理器）分区。仅安全管理器安装所需的*最低*可用磁盘空间为 7GB。如果达不到 7 GB，则安装将中止。 **注意**　思科强烈建议在单独的分区中安装此类操作系统和应用。 **注意**　当在 HA （高可用性）模式下使用 Veritas 时，上面所述的应用分区和任何其他事件存储区分区可能不相关。有关进一步的详细信息，请参阅相应的安全管理器高可用性文档 (http://www.cisco.com/c/en/us/support/security/security-manager/products-installation-guides-list.html) 和 Veritas 文档。 • 需要在单独的分区中为事件查看器提供额外的 1.0 TB 空间用于存储日志：仅当您计划使用事件查看器时才需要满足此要求。思科建议在直接连接存储设备上创建此单独分区。 • 提供额外的 1.0 TB 或更多空间：仅当您计划启用事件存档时才需要满足此要求。当所需的日志存储空间超出主存储容量（用于长期保存等）时，事件存档功能会为事件创建一个辅助存储。所需的辅助事件存储区大小应大于配置的主存储大小，因此，需要提供额外 1.0 TB 或更多磁盘空间才能使用事件存档功能。主要和辅助事件存储区可以位于 SAN 上，但建议在直接连接存储设备 (DAS) 上创建主要存储分区，以获得最佳性能。 要想获得更好的性能，思科建议使用 RAID 10。如果需要，也可以使用 RAID 5。将连续操作（并非大多数情况）的写入策略设置为写回；否则，请将写入策略设置为始终通写。将写入策略设置为通写也可以提高性能。 **提示** 如果每秒事件数 (EPS) 维持 10,000 个，则每天会耗用约 86 GB 压缩磁盘空间。耗用的磁盘空间占到为事件存储区（主要/辅助）分配的磁盘空间的 90% 时，会发生日志回滚。磁盘越小，回滚速度越快。根据您预期的 EPS 速率和回滚要求，在使用事件管理功能时，可以增加或减少最低磁盘大小。
主机服务器 HDD RAID	虚拟机内的 RAID 不适用，因为它使用构建在基础主机系统的 HDD 配置之上的虚拟化文件系统。此外，基于软件的 RAID 不能与 VMware ESX 虚拟机配合使用。有关详细信息，请参阅 VMware, Inc. 发布的文档。
网络适配器	1 Gbps
操作系统	以下项之一： • Microsoft Windows Server 2008 R2 SP1 Enterprise - 64 位 • Microsoft Windows Server 2012 R2 Standard - 64 位 • Microsoft Windows Server 2012 Standard - 64 位 • Microsoft Windows Server 2012 R2 Datacenter - 64 位 • Microsoft Windows Server 2012 Datacenter - 64 位

表 3　与 VMware ESX 4.1 和 ESXi 5.5 及之前的 VMware ESXi 版本相关的小型部署（续）

建议的大小	
最大设备数	最多 25 个
支持的最大累计 EPS	每秒事件数为 5000 [在此值中，系统日志与 IPS SDEE 的比率为 9:1（即，4500 个系统日志 + 500 个 SDEE）]
最大并发用户数	大多数情况下为两个并发用户（一个仅配置用户，一个使用事件和/或报告屏幕的用户）

小型企业部署

表 4 列出了针对小型企业部署的建议安全管理器服务器规格：

表 4　小型企业部署

建议使用的服务器	思科 UCS C220 M3 或同等设备
CPU	1 个 Hex Core（建议使用 X5670 或同等系列）
内存 (RAM)	16 GB 是使用安全管理器所有功能的最低要求。内存小于此值，事件管理和报告管理等功能会受影响。 特别是，如果可供操作系统使用的 RAM 容量小于 8 GB，会在安装期间禁用事件管理和报告管理器。 如果可供操作系统使用的内存介于 8 和 12 GB 之间，则可以关闭事件管理和报告管理功能（假定您不打算使用这些功能）。此类系统中，可以使用配置管理功能。 完成安装后，可以通过安全管理器客户端在低内存系统中启用事件管理和报告管理（依次选择“工具”[Tools] >“安全管理器管理”[Security Manager Administration] >“事件管理”[Event Management]），但不建议这么做。请记住，在低内存系统中启用事件管理和报告管理功能可能会严重影响整个应用的性能。 如果在单独的服务器上安装 AUS，需要满足以下最低要求： • 仅 AUS 服务器，4 GB。我们建议使用 4 GB 以上。 **注意**　执行配置操作时，服务器的内存利用率 （如 Windows 任务管理器所示）可能为 99%。这并非表示存在问题；这是正常现象，因为安全管理器的所有进程和功能都使用或分配各自的已分配内存。

表 4　小型企业部署（续）

硬盘空间	使用合适的 HDD 组合获得所需的磁盘空间，如下： • 思科建议 100 GB 用于操作系统分区。 • 思科建议 150 GB 用于应用（安全管理器）分区。仅安全管理器安装所需的*最低*可用磁盘空间为 7 GB。如果达不到 7 GB，则安装将中止。 **注意**　思科强烈建议在单独的分区中安装此类操作系统和应用。 **注意**　当在 HA （高可用性）模式下使用 Veritas 时，上面所述的应用分区和任何其他事件存储区分区可能不相关。有关进一步的详细信息，请参阅相应的安全管理器高可用性文档 (http://www.cisco.com/c/en/us/support/security/security-manager/products-installation-guides-list.html) 和 Veritas 文档。 • 需要在单独的分区中为事件查看器提供额外的 1.0 TB 空间用于存储日志：仅当您计划使用事件查看器时才需要满足此要求。思科建议在直接连接存储设备上创建此单独分区。 • 提供额外的 1.0 TB 或更多空间：仅当您计划启用事件存档时才需要满足此要求。当所需的日志存储空间超出主存储容量（用于长期保存等）时，事件存档功能会为事件创建一个辅助存储。所需的辅助事件存储区大小应大于配置的主存储大小，因此，需要提供额外 1.0 TB 或更多磁盘空间才能使用事件存档功能。主要和辅助事件存储区可以位于 SAN 上，但建议在直接连接存储设备 (DAS) 上创建主要存储分区，以获得最佳性能。 要想获得更好的性能，思科建议使用 RAID 10。如果需要，也可以使用 RAID 5。将连续操作（并非大多数情况）的写入策略设置为写回；否则，请将写入策略设置为始终通写。将写入策略设置为通写也可以提高性能。 **提示** 如果每秒事件数 (EPS) 维持 10,000 个，则每天会耗用约 86 GB 压缩磁盘空间。耗用的磁盘空间占到为事件存储区（主要/辅助）分配的磁盘空间的 90% 时，会发生日志回滚。磁盘越小，回滚速度越快。根据您预期的 EPS 速率和回滚要求，在使用事件管理功能时，可以增加或减少最低磁盘大小。
网络适配器	1 Gbps
操作系统	以下项之一： • Microsoft Windows Server 2008 R2 SP1 Enterprise - 64 位 • Microsoft Windows Server 2012 R2 Standard - 64 位 • Microsoft Windows Server 2012 Standard - 64 位 • Microsoft Windows Server 2012 R2 Datacenter - 64 位 • Microsoft Windows Server 2012 Datacenter - 64 位
建议的大小	
最大设备数	最多 100 个
支持的最大累计 EPS	每秒事件数为 5000 [在此值中，系统日志与 IPS SDEE 的比率为 9:1（即，4500 个系统日志 + 500 个 SDEE）]
最大并发用户数	大多数情况下为四个并发用户（两个仅配置用户，两个使用事件和/或报告屏幕的用户）

中型企业部署

表 5 列出了针对中型企业部署的建议安全管理器服务器规格：

表 5　　中型企业部署

建议使用的服务器	思科 UCS C220 M3 或同等设备
CPU	1 个 Hex Core（建议使用 X5670 或同等系列）
内存 (RAM)	• 16 GB 专用于配置管理器 • 24 GB 用于所有功能 **注意** 执行配置操作时，服务器的内存利用率 （如 Windows 任务管理器所示）可能为 99%。这并非表示存在问题；这是正常现象，因为安全管理器的所有进程和功能都使用或分配各自的已分配内存。
硬盘空间	使用合适的 HDD 组合获得所需的磁盘空间，如下： • 思科建议 100 GB 用于操作系统分区。 • 思科建议 150 GB 用于应用（安全管理器）分区。仅安全管理器安装所需的*最低*可用磁盘空间为 7 GB。如果达不到 7 GB，则安装将中止。 **注意** 思科强烈建议在单独的分区中安装此类操作系统和应用。 **注意** 当在 HA （高可用性）模式下使用 Veritas 时，上面所述的应用分区和任何其他事件存储区分区可能不相关。有关进一步的详细信息，请参阅相应的安全管理器高可用性文档 (http://www.cisco.com/c/en/us/support/security/security-manager/products-installation-guides-list.html) 和 Veritas 文档。 • 需要在单独的分区中为事件查看器提供额外的 1.0 TB 空间用于存储日志：仅当您计划使用事件查看器时才需要满足此要求。思科建议在直接连接存储设备上创建此单独分区。 • 提供额外的 1.0 TB 或更多空间：仅当您计划启用事件存档时才需要满足此要求。当所需的日志存储空间超出主存储容量（用于长期保存等）时，事件存档功能会为事件创建一个辅助存储。所需的辅助事件存储区大小应大于配置的主存储大小，因此，需要提供额外 1.0 TB 或更多磁盘空间才能使用事件存档功能。主要和辅助事件存储区可以位于 SAN 上，但建议在直接连接存储设备 (DAS) 上创建主要存储分区，以获得最佳性能。 要想获得更好的性能，思科建议使用 RAID 10。如果需要，也可以使用 RAID 5。将连续操作（并非大多数情况）的写入策略设置为写回；否则，请将写入策略设置为始终通写。将写入策略设置为通写也可以提高性能。 **提示** 如果每秒事件数 (EPS) 维持 10,000 个，则每天会耗用约 86 GB 压缩磁盘空间。耗用的磁盘空间占到为事件存储区（主要/辅助）分配的磁盘空间的 90% 时，会发生日志回滚。磁盘越小，回滚速度越快。根据您预期的 EPS 速率和回滚要求，在使用事件管理功能时，可以增加或减少最低磁盘大小。

表 5　中型企业部署（续）

网络适配器	1 Gbps
操作系统	以下项之一： • Microsoft Windows Server 2008 R2 SP1 Enterprise - 64 位 • Microsoft Windows Server 2012 R2 Standard - 64 位 • Microsoft Windows Server 2012 Standard - 64 位 • Microsoft Windows Server 2012 R2 Datacenter - 64 位 • Microsoft Windows Server 2012 Datacenter - 64 位
建议的大小	
最大设备数	最多 200 个
支持的最大累计 EPS	每秒事件数为 10,000 [在此值中，系统日志与 IPS SDEE 的比率为 9:1（即，9000 个系统日志+ 1000 个SDEE）]
最大并发用户数	大多数情况下为七个并发用户（五个仅配置用户，两个使用事件和/或报告屏幕的用户）

大型企业部署

表 6 列出了针对大型企业部署的建议安全管理器服务器规格：

表 6　大型企业部署

建议使用的服务器	思科 UCS C220 M3 或同等设备
CPU	2 个 Hex Core（建议使用 X5670 或等效系列）
内存 (RAM)	• 24 GB 专用于配置管理器 • 32 GB 用于所有功能 **注意** 执行配置操作时，服务器的内存利用率 （如 Windows 任务管理器所示）可能为 99%。这并非表示存在问题；这是正常现象，因为安全管理器的所有进程和功能都使用或分配各自的已分配内存。

表 6　大型企业部署（续）

硬盘空间	使用合适的 HDD 组合获得所需的磁盘空间，如下： • 思科建议 100 GB 用于操作系统分区。 • 思科建议 150 GB 用于应用（安全管理器）分区。仅安全管理器安装所需的*最低*可用磁盘空间为 7 GB。如果达不到 7 GB，则安装将中止。 **注意**　思科强烈建议在单独的分区中安装此类操作系统和应用。 **注意**　当在 HA （高可用性）模式下使用 Veritas 时，上面所述的应用分区和任何其他事件存储区分区可能不相关。有关进一步的详细信息，请参阅相应的安全管理器高可用性文档 (http://www.cisco.com/c/en/us/support/security/security-manager/products-installation-guides-list.html) 和 Veritas 文档。 • 需要在单独的分区中为事件查看器提供额外的 1.0 TB 空间用于存储日志：仅当您计划使用事件查看器时才需要满足此要求。思科建议在直接连接存储设备上创建此单独分区。 • 提供额外的 1.0 TB 或更多空间：仅当您计划启用事件存档时才需要满足此要求。当所需的日志存储空间超出主存储容量（用于长期保存等）时，事件存档功能会为事件创建一个辅助存储。所需的辅助事件存储区大小应大于配置的主存储大小，因此，需要提供额外 1.0 TB 或更多磁盘空间才能使用事件存档功能。主要和辅助事件存储区可以位于 SAN 上，但建议在直接连接存储设备 (DAS) 上创建主要存储分区，以获得最佳性能。 要想获得更好的性能，思科建议使用 RAID 10。如果需要，也可以使用 RAID 5。将连续操作（并非大多数情况）的写入策略设置为写回；否则，请将写入策略设置为始终通写。将写入策略设置为通写也可以提高性能。 **提示** 如果每秒事件数 (EPS) 维持 10,000 个，则每天会耗用约 86 GB 压缩磁盘空间。耗用的磁盘空间占到为事件存储区（主要/辅助）分配的磁盘空间的 90% 时，会发生日志回滚。磁盘越小，回滚速度越快。根据您预期的 EPS 速率和回滚要求，在使用事件管理功能时，可以增加或减少最低磁盘大小。
网络适配器	1 Gbps
操作系统	以下项之一： • Microsoft Windows Server 2008 R2 SP1 Enterprise - 64 位 • Microsoft Windows Server 2012 R2 Standard - 64 位 • Microsoft Windows Server 2012 Standard - 64 位 • Microsoft Windows Server 2012 R2 Datacenter - 64 位 • Microsoft Windows Server 2012 Datacenter - 64 位
建议的大小	
最大设备数	最多 500 个
支持的最大累计 EPS	每秒事件数为 10,000 [在此值中，系统日志与 IPS SDEE 的比率为 9:1（即，9000 个系统日志+ 1000 个SDEE）]
最大并发用户数	大多数情况下为十个并发用户（五个仅配置用户，五个使用事件和/或报告屏幕的用户）

注意 如要启用事件存档功能，额外存储容量大小需要与主存储区的容量大小相同或更大。

注意 上述大小基于平均有 3000 - 5000 个规则的防火墙设备。如果规则数大于此数字，应减少部署中支持的设备数或考虑下一更高规格的硬件。

大型零售部署

表 7 列出可针对大型零售部署的建议安全管理器服务器规格：

表 7　　大型零售部署

建议使用的服务器	Cisco UCS C460 M2 或同等设备
CPU	4 x 8 核心
内存 (RAM)	64 GB（所有情况下的最低要求）。有关更多详细信息，请参阅即刻显示在此句子下面的 UCS C460 内存配置的注意。 **注意** **1)** 应用可能不会使用此处指定的所有较高的 RAM，但在 Cisco UCS C460（其中大多数填充的是 DIMM 模块）等较高端的型号中，RAM 配置越高，硬件的性能越优。 UCS C460 M1 用户文档重点介绍了以下要点：“每个 CPU 有 16 个 DIMM 插槽（每个内存扩充卡 8 个）。当所有 CPU 中所有内存通道的内存类型和数量都相同时，系统性能达到最优。（UCS C460 M1 服务器的每个 CPU 有四个内存通道）。” (http://www.cisco.com/en/US/prod/collateral/ps10265/ps10493/spec_sheet_c17-644207.pdf) **2)** UCS C460 M1 用户文档建议：采用 64 GB RAM 可获得一般性能，采用 128 GB RAM 可获得“出色”性能。 (http://www.cisco.com/en/US/prod/collateral/ps10265/ps10493/spec_sheet_c17-644207.pdf) **3)** UCS 460 M1 和 UCS 460 M2 规格文档可用于进一步了解 UCS 460 服务器中的内存配置： – UCS 460 M1：http://www.cisco.com/en/US/prod/collateral/ps10265/ps10493/spec_sheet_c17-644207.pdf – UCS 460 M2：http://www.cisco.com/en/US/prod/collateral/ps10265/ps10493/ps11587/spec_sheet_c17-662220.pdf

表 7　大型零售部署（续）

硬盘空间	使用合适的 HDD 组合获得所需的磁盘空间，如下： • 思科建议 100 GB 用于操作系统分区。 • 思科建议 150 GB 用于应用（安全管理器）分区。仅安全管理器安装所需的*最低*可用磁盘空间为 7 GB。如果达不到 7 GB，则安装将中止。 **注意**　思科强烈建议在单独的分区中安装此类操作系统和应用。 **注意**　当在 HA （高可用性）模式下使用 Veritas 时，上面所述的应用分区和任何其他事件存储区分区可能不相关。有关进一步的详细信息，请参阅相应的安全管理器高可用性文档 (http://www.cisco.com/c/en/us/support/security/security-manager/products-installation-guides-list.html) 和 Veritas 文档。 • 需要在单独的分区中为事件查看器提供额外的 1.0 TB 空间用于存储日志：仅当您计划使用事件查看器时才需要满足此要求。思科建议在直接连接存储设备上创建此单独分区。 • 提供额外的 1.0 TB 或更多空间：仅当您计划启用事件存档时才需要满足此要求。当所需的日志存储空间超出主存储容量（用于长期保存等）时，事件存档功能会为事件创建一个辅助存储。所需的辅助事件存储区大小应大于配置的主存储大小，因此，需要提供额外 1.0 TB 或更多磁盘空间才能使用事件存档功能。主要和辅助事件存储区可以位于 SAN 上，但建议在直接连接存储设备 (DAS) 上创建主要存储分区，以获得最佳性能。 要想获得更好的性能，思科建议使用 RAID 10。如果需要，也可以使用 RAID 5。将连续操作（并非大多数情况）的写入策略设置为写回；否则，请将写入策略设置为始终通写。将写入策略设置为通写也可以提高性能。 对于应用分区，请使用 RAID 1/0。 **提示** 如果每秒事件数 (EPS) 维持 10,000 个，则每天会耗用约 86 GB 压缩磁盘空间。耗用的磁盘空间占到为事件存储区（主要/辅助）分配的磁盘空间的 90% 时，会发生日志回滚。磁盘越小，回滚速度越快。根据您预期的 EPS 速率和回滚要求，在使用事件管理功能时，可以增加或减少最低磁盘大小。
网络适配器	1 Gbps
操作系统	以下项之一： • Microsoft Windows Server 2008 R2 SP1 Enterprise - 64 位 • Microsoft Windows Server 2012 R2 Standard - 64 位 • Microsoft Windows Server 2012 Standard - 64 位 • Microsoft Windows Server 2012 R2 Datacenter - 64 位 • Microsoft Windows Server 2012 Datacenter - 64 位
建议的大小	
最大设备数	多达 2500 个零售分支机构防火墙
支持的最大累计 EPS	每秒事件数为 15,000 [在此值中，系统日志与 IPS SDEE 的比率为 9:1（即，13,500 个系统日志 + 1500 个 SDEE）]
最大并发用户数	大多数情况下为五 (5) 个并发用户（包括仅配置用户和使用事件和/或报告屏幕的用户）

注意 如要启用事件存档功能，额外存储容量大小需要与主存储区的容量大小相同或更大。

注意 **1)** 上述大小基于规则数平均为 600 个、关联对象总数约为 20,000 个的防火墙设备。如果规则数大于此数字，可以减少部署中支持的设备数或考虑跨多个服务器对设备管理进行分区。

2) 请注意，在单个作业中对大量设备执行配置更改部署时，部署的总时间取决于设备的实际响应时间（即，安全管理器连接到设备、获取最新配置等操作花费的时间）。因此，最好将作业部署为每个作业小于 100 (< 100) 台设备。

要提高部署的可扩展性，您还可以考虑以下事项：

a) AUS 适用于基于 ASA 的分支机构防火墙；请参阅自动更新服务器 4.8（第 5 页）。

b) Cisco CNS CE 适用于基于 IOS 的分支机构设备；请参阅思科 CNS 配置引擎 3.5 和 3.5(1)（第 5 页）。

3) 也可以调整安全管理器服务器，以增加可以并行发生部署更新的设备总数。这取决于库存中设备的配置规模、设备响应时间/位置等。要针对大型零售部署调整这些参数，请联系思科技术支持中心 (TAC)。

部署方案

可能有多种适用于安全管理器应用的部署方案。在决定部署方案时，应该考虑以下可能会影响系统性能的重要因素：

安全管理器将管理多少台设备？

每次安全管理器安装对于它可以管理的设备数没有硬性限制；但是，建议每台安全管理器服务器采用建议的硬件和软件，管理的企业级防火墙数量应少于 500，如果是零售分支机构防火墙，则少于 2500。您应该使用上一部分中列出的建议规格，使每台服务器管理适当数量的设备。如果受管设备的配置非常高，则管理的设备可能会较少。例如，具有 20,000 – 50,000 个规则的大量防火墙设备、大型 IPS 签名集或具有成千上万个分支机构的非常庞大且复杂的 VPN 策略，可能会导致安全管理器在性能欠佳的情况下运行。如果需要，应部署多个安全管理器服务器来管理更多设备和网络。

如何跨多个安全管理器服务器管理策略、对象和设备？

通过策略导出/导入功能，可以将共享策略、对象和设备从一个安全管理器服务器导出和导入到其他安全管理器服务器。通过此功能，可以轻松跨多个服务器同步共享策略和对象。此功能还可用于在需要时将受管设备从一台服务器迁移（移动）到另一台服务器。

安全管理器可以管理哪些类型的设备？不同类型设备的性能是否会有所不同？

安全管理器可以管理的设备类型有许多，但其中最常见的是防火墙、IPS 传感器和 VPN 设备；这些类型的设备很好地说明了不同类型设备的性能会有何差异。

某些类型的设备需要比其他类型的设备更频繁地更改策略。例如，防火墙和 IPS 传感器等设备需要比 VPN 设备更频繁地更改策略；因此，防火墙和 IPS 传感器需要的资源比 VPN 设备更多。因此，一般来说，安全管理器可以在 VPN 环境中管理的设备比在防火墙或 IPS 环境中管理的设备要多。

常用的配置规模是怎样的？

对于小型环境来说，管理的行数介于 100 到 1000 之间。对于中型环境来说，可以管理的 ACL 数介于 1000 到 5000 之间；而对于某些大型环境来说，此数字可能介于 5000 到 50,000（甚至更多）ACL 之间。在更大型的环境中，应考虑减少每个安全管理器服务器的设备数，以准备好足够的空间来满足将来发展的需要。

安全管理器可以管理多少个事件？防火墙和 IPS 日志记录的正确设置是什么？

事件管理可能会消耗大量系统资源，特别是在包含许多用户和设备的大规模环境中更是如此。虽然一台具有合适硬件和软件规格的安全管理器服务器每秒最高可管理 10,000 个事件，但建议您将设备配置为仅发送操作所需的重要日志。建议的防火墙设备日志记录级别为从“0：紧急”到“5：通知”，其中 0 级别所产生的要发送到安全管理器的日志数最少。对于其他日志记录，您始终可以在需要进行故障排除和调试时在每台设备上开启。在使用日志记录的“7：调试”或“6：信息”级别时，一定要谨慎。仅应在需要时在设备的控制台或设备管理器中开启这些级别，完成后立即关闭。对于 IPS 设备，签名设置可以在“低”(Low)、“中”(Medium)、“高”(High) 或“信息”(Informational) 间调整。这些设置因环境而异，可能会影响系统性能。有关详细信息，请参阅 IPS 配置指南。

多少用户会使用这些应用？

活动用户会话也会为服务器增加负载，因此在制定部署规模决策时应将此因素考虑在内。例如，应用可能未因设备数达到其上限，但可能因同步用户会话数二接近其最大负载，此时务必要为应用分配一个服务器。安全管理器支持五个以上的并发用户，但用户可以随时在事件查看器中最多打开五个实时事件视图。事件服务器不限制与其连接的事件查看器实例数，但硬性限制在所有活动事件查看器中最多打开 5 个并行实时事件视图。

是否需要通过安全管理器部署 AUS？

如果您需要通过安全管理器部署 AUS，是否需要 AUS 高度可用或在发生站点灾难或中断时抗毁？如果达到专用服务器上所安装 AUS 的规模限制，您需要考虑在多个服务器上部署多个实例。

影响应用性能的因素

有许多影响应用性能的因素。这包括但不限于以下因素：

- 服务器和客户端硬件（例如，处理器、内存和存储技术）
- 受管设备的数量，包括设备类型、设备复杂性和配置规模（如大量 ACL）
- 事件管理引擎、管理设备报告的事件数量和日志记录级别
- 策略对象的数量和复杂性
- 并发用户的数量和用户执行的具体活动
- 大量设备的配置部署或 IPS 签名更新的频率
- 部署作业中存在的设备数量
- 网络带宽和延迟，例如安全管理器客户端与服务器之间以及服务器与受管设备之间的网络带宽和延迟
- 虚拟化技术（例如 VMware ESX）的使用
- 适用于 AAA 服务的 ACS 服务器的使用
- 排定报告的数量
- 报告引擎、受管设备报告的事件数量以及事件汇聚

安全管理器客户端与服务器之间的超远地理距离会因延迟导致客户端响应能力变差。例如，不建议使用自身位于印度而服务器位于加利福尼亚的客户端，因为涉及的延迟时间太长。在这种情况下，我们建议您使用远程桌面或安排终端服务器，其中运行的客户端与服务器共置于同一数据中心内，或至少是在附近。

单个服务器安装

单个服务器是最简单的部署方案，在这类方案中，所需的所有安全管理器应用都安装在同一台服务器上。对于拥有一到两名网络安全管理员的小规模安全环境，在通常情况下部署单台服务器足矣。

多个服务器安装

在某些部署有数百或数千台设备的大型环境中，单个服务器无法高效地管理所有设备。出于性能考虑，您可以选择跨多个服务器部署所需的安全管理器应用。应用的一种可能分布如下：

服务器 A：防火墙策略和设备管理

- 公共服务
- 安全经理
- 事件/日志监控
- 报告管理器
- 自动更新服务器*（可选）*
- 映像管理器

服务器 B：IPS 策略和设备管理

- 公共服务
- 安全经理
- 事件/日志监控
- 报告管理器
- 运行状况和性能监控器

服务器 C：VPN 策略和设备管理

- 公共服务
- 安全经理
- 事件/日志监控
- 报告管理器
- 运行状况和性能监控器

服务器 A 专用于所有 ASA/PIX/FWSM 防火墙设备的配置和事件管理。服务器 B 专用于所有 IPS 设备的配置和事件管理，而服务器 C 专用于 ASA/IOS/ISR VPN 设备的 VPN 策略管理；服务器 C 还管理防火墙设备，因为这些设备将是 VPN 拓扑的组成部分。通过此部署方法，在服务器之间共享策略数据的需求会降至最低，因为每台服务器将使用该服务器内几乎相同的策略数据。但是，此配置不适合在距离受管设备很远的位置部署安全管理器服务器的网络，这可能会影响监控、配置发现和部署。

另一种方法是按区域划分设备，以便每台安全管理器仅管理该区域（例如，美国西部、美国中部、美国东部、欧洲或亚洲）的少数设备。这样可通过其当地的安全管理服务器为受管设备的管理控制台、事件监控和配置提供最优性能。

在多服务器部署中，通过策略导入/导出功能，可以在不同服务器之间导出和导入共享策略和对象。设备也可以使用策略导入/导出功能迁移（移动）到其他服务器。这有助于进行规模管理，同时仍使策略和对象在不同服务器中的大量设备间保持同步。

VMware 虚拟机环境中的安装

安全管理器支持在 VMware ESX 4.1 和 ESXi 5.5 及之前的 VMware ESXi 版本中运行。不支持 VMware Server 和 VMware Workstation 等其他 VMware 环境。

您可以将安全管理器支持的任何服务器操作系统用作 VMware 的访客操作系统。VMware 资格审批工作需要运行一组性能和耐用性测试，这组测试与在普通的非虚拟化服务器上运行的安全管理器上执行的测试相同。测试结果表明，在 VMware ESX Server 4.0 中运行安全管理器会造成应用性能适度的降低，性能降低程度因涉及的参考网络规模和特定测试案例而异。在 VMware 环境中部署安全管理器只适用于小型网络。

性能出现大幅降低的一种情况是部署大量 PIX 或 ASA 设备，或者部署具有大量规则的设备（大约五千到五万条规则）。在这种情况下，部署所花费的时间超出了可接受的范围。要了解 VMware 性能最佳实践，请参阅以下文档：http:// www.vmware.com/pdf/Perf_Best_Practices_vSphere4.1.pdf。

但通常情况下，默认值或默认设置都是最佳的，因此应避免调整任何高级 VMware 参数。

另外建议采用新一代服务器，而且其处理器采用专用于提高虚拟化效率的技术。例如，在 Intel® Xeon® X5500 系列四核处理器（采用英特尔®虚拟化技术 [IVT]）上测试 VMware ESX Server 4.0 中运行的安全管理器时，获得的结果非常好。AMD 提供具有虚拟化扩展的 64 位 x86 架构处理器，称为 AMD 虚拟化 (AMD-V)。

有关虚拟机硬件和软件的要求，请参阅表 3 与 VMware ESX 4.1 和 ESXi 5.5 及之前的 VMware ESXi 版本相关的小型部署。

高可用性/灾难恢复

您可以在高可用性或灾难恢复配置中部署安全管理器，以在服务器、存储、网络或站点发生故障时大幅提高应用可用性和生存能力。这些部署选项在相应的安全管理器高可用性文档 (http://www.cisco.com/c/en/us/support/security/security-manager/products-installation-guides-list.html) 中有详细介绍。

安装指南

有关安全管理器安装的详细说明，请参阅 *Cisco Security Manager 4.8 安装指南*。

可安装模块

安全管理器服务器安装适用于多种不同的组件，有些组件是可选的。安全管理器安装程序会安装以下组件：

- Common Services 4.2.2（默认情况下，会在您选择安装 Security Manager 4.8 和自动更新服务器 4.8 时安装）

- Security Manager 4.8 服务器（必需）
- 自动更新服务器 4.8（可选）
- Security Manager 4.8 客户端（如果客户端在专用客户机上安装，则为可选组件）

可以使用独立安装程序安装安全管理器客户端。访问此安装程序的最常用方式为：使用网络浏览器登录到服务器 (https://server_hostname_or_ip)，然后点击客户端安装程序。

有关安全管理器安装程序和安全管理器客户端安装程序的详细使用说明，请参阅 *Cisco Security Manager 4.8 安装指南*。

IP 地址、主机名和 DNS 名称

Cisco Security Manager 需要静态 IP 地址而不是 DHCP 地址。可以更改安全管理器服务器的 IP 地址，更改地址后需要重新启动系统。如果 DNS 服务器在安全管理器的 TCP/IP 设置中配置，请确保安全管理器服务器的主机名和 DNS 名称一致，并且可通过已配置的 DNS 服务器解析。在安装安全管理器之前，您应为服务器选择永久 DNS 和计算机主机名，因为主机名和 DNS 名称在安装之后不得修改。在安装之后更改安全管理器服务器的主机名可能需要重新安装安全管理器。

客户端部署

建议的常规做法是在单独的客户机上安装和运行安全管理器客户端。安全管理器仅支持在指定计算机上安装一个版本的客户端，因此，举例来讲，就不能在同一计算机上同时安装 Security Manager 4.7 和 4.8 的客户端。可以在服务器上安装和使用客户端；但是，这种做法仅适用于小型网络，不建议用于大型企业网络。

如影响应用性能的因素一节所述，您可能需要在服务器附近的终端服务器上部署客户端，以在最终用户距离服务器较远而遇到重大延迟（例如，洲际距离）时将性能维持在可接受的水平。

安全管理器服务器调整

安全管理器包括多个高级参数，您可以修改这些参数以调整应用性能。对于管理 50 台或更多设备的大中型部署，可以修改安全管理器中的以下参数来获得最佳性能：

- 磁盘碎片整理
- Windows 操作系统的交换文件大小
- Sybase 数据库注册表参数

磁盘碎片整理

建议以 50 GB 磁盘大小为增量进行磁盘分段，以获得最佳性能。

小心 频繁进行碎片整理还可能会导致扇区错误，最终造成磁盘故障。

Windows 操作系统的交换文件大小

虚拟内存（分页文件）应为已安装内存的 1.5 倍。这是 Microsoft 对 Windows 平台的建议。这不是思科的要求。只有在系统中已安装的 RAM 不足以处理负载时才需要进行内存分页。

小心 您必须取消选中（清除）复选框“自动管理所有驱动器的分页文件大小”。此复选框的导航路径为“控制面板”>“系统”>“高级系统设置”>“性能”>“设置”>“高级”选项卡>“虚拟内存”>“更改”。

Sybase 数据库注册表参数

对于大中型部署，应调整以下参数以提供最佳性能和可扩展性。

步骤 1 在安全管理器服务器上，使用文本编辑器修改 <NMSROOT>\databases\vms\orig\odbc.tmplorig，如下所示：

确保参数“**___Switches**”包含“**-gb high**”。

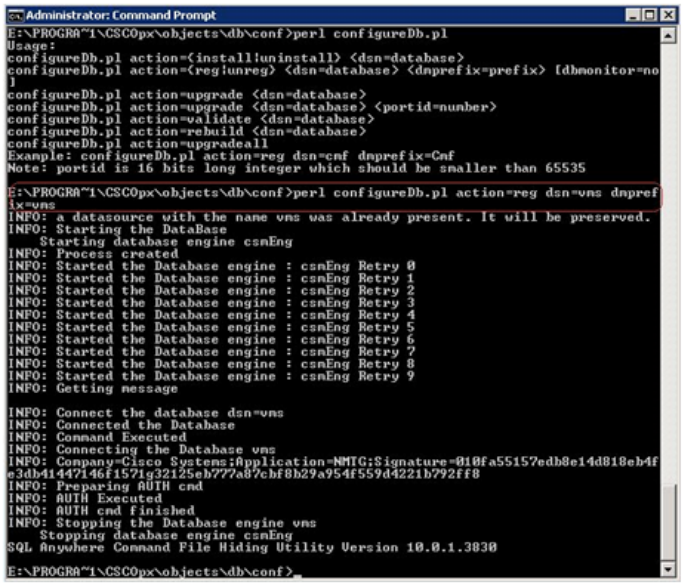
步骤 2 使用管理员权限打开命令提示符（右键点击命令提示图标并选择“以管理员身份运行”[Run as administrator]）。

步骤 3 在命令提示窗口输入“**net stop crmdmgtd**”以关闭安全管理器。请等到安全管理器完全关闭，然后再执行下一步。

步骤 4 在安全管理器完全关闭后，使用 **<NMSROOT>\objects\db\conf** 中提供的 configureDb.pl perl 实用程序在 Windows 注册表中重新注册数据库参数。该命令及其语法的示例如下：

“**perl configureDb.pl action=reg dsn=vms dmprefix=vms**”

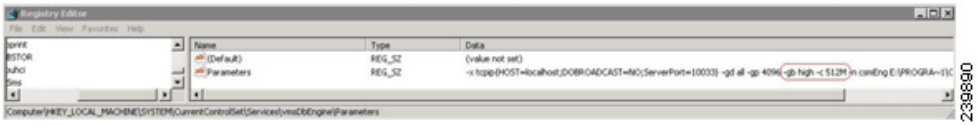
图 1 重新注册数据库参数



步骤 5 检查以下 Windows 注册表设置，验证上述参数是否已正确注册：

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\vmsDbEngine\Parameters，应为“**-gb high –c 512M**”注册表项：

图 2　　验证数据库参数的注册



步骤 6 在命令提示符窗口中输入“**net start crmdmgtd**”，启动安全管理器。请等到安全管理器完全运作之后再使用。

了解安全管理器许可

在规划安全管理器的配置时一定要了解安全管理器许可，以确保您有正确的基础许可证以及合适您要管理之设备的数量和类型的设备许可证数量。

有关重要的许可信息，请参阅以下文档：

- *Cisco Security Manager 4.8 安装指南*
- 有关安全管理器的最新主要版本的产品公告，请访问 http://www.cisco.com/c/en/us/products/security/security-manager/bulletin-listing.html

许可示例

本节提供一些代表性的许可示例，以帮助用户更好地了解安全管理器许可。

示例 1

托管网络说明：15 个思科集成多业务路由器。

所需许可：需要企业标准 25 设备许可证。由于不涉及 Catalyst 6500 服务模块，并且设备数少于 25 台，因此订购标准 25 许可证。

示例 2

托管网络说明：5 个 IDSM-2 模块，其中每个模块有两个虚拟传感器。

所需许可：需要十个许可证（五个模块之间分配 10 个虚拟传感器）。虽然标准 10 似乎是足够的，但因为涉及 Catalyst 6500 服务模块，所以至少需要专业 50 (PRO50)。

示例 3

托管网络说明：在故障转移模式下运行的 250 对 ASA（500 台设备）。

所需许可：专业 250 许可证。或者，您也可以订购专业 50 许可证或专业 100 许可证以及适当的增量（“附加”）设备许可证。增量设备许可证按照增量 50、100 和 250 台设备提供。

示例 4

托管网络说明：现在有了安全管理器标准 25 设备许可证，但现在需要管理在单模式下运行的 20 台额外的 ASA 设备。

所需许可：需要从企业标准 25 升级到专业 50 许可证。

示例 5

托管网络说明：在活动/备用或活动/活动配对组合中部署 10 对故障转移 ASA 设备，每对具有 5 个安全情景。

所需许可：企业专业 50 和企业专业增量 50 设备

在部署一对故障切换设备进行冗余设置时，您只需将活动设备和情景添加到安全管理器。这样，所需设备许可证的数量为 10 台设备 x 5 个情景 + 10 个机箱，共需要 60 个设备许可证。

注意 有关可用许可证类型和各种支持的升级路径的完整信息，以及可购买的思科软件应用支持服务协议合同的相关信息，请参阅安全管理器的最新主要版本的产品公告，网址为 http://www.cisco.com/c/en/us/products/security/security-manager/bulletin-listing.html。

注意 在上述所有示例中，您应该考虑订购相应的思科服务应用支持 (SAS)，以获得免费访问思科技术支持中心 (TAC) 以及细微应用版本更新的权限。