HP Insight Remote Support Advanced
A.05.40 受管系统指南

HP 部件号：5900-0372
出版日期：2010 年 1 月 18 日 - A.05.40 - 第 6.0 版

法律声明

机密计算机软件。必须有 HP 授予的有效许可证，方可拥有、使用或复制本软件。根据供应商的标准商业许可证的规定，美国政府应遵守 FAR 12.211 和 12.212 中有关“商业计算机软件”、“计算机软件文档”与“商业货物技术数据”条款的规定。

本文档中的信息如有更改，恕不另行通知。随 HP 产品及服务提供的明示性担保声明中列出了适用于此 HP 产品及服务的专用担保条款。本文中的任何内容均不构成额外的担保。HP 对本文中的技术或编辑错误以及缺漏不负任何责任。

致谢

Java、咖啡杯徽标以及所有基于 Java 的标志都是 Sun Microsystems, Inc. 在美国或其他国家（地区）的商标或注册商标。

Microsoft 和 Windows 是 Microsoft Corporation 在美国的注册商标。

UNIX 是 The Open Group 的注册商标。

目录

图列表

表格清单

关于本文档

目标读者

本文档供安装、配置及使用 Insight Remote Support Advanced A.05.40 的 HP 客户与 HP 技术支持人员使用，他们可以在配置CMS之前和配置期间使用本文档来验证受管系统是否已正确配置。

版本历史

不再发布或支持 Insight Remote Support Advanced A.05.20 之前的版本。

制造部件号	版本	变更摘要	版本号	发布日期
5900-0372	A.05.40	A.05.40 版软件的新版本	6.0	2010 年 1 月 18 日
5992-6223	A.05.30	A.05.30 版软件的新版本	5.0	2009 年 7 月 7 日
5993-6210	A.05.20	修订版，包含虚拟库和适用于 Integrity Windows、Linux 及 HP-UX 受管系统的 WBEM 配置详细描述。	4.1	2009 年 3 月 6 日
5992-6302	A.05.20	Insight Remote Support Advanced A.05.20 的新版本	4.0	2009 年 1 月 27 日

产品简介

Insight Remote Support Advanced 不是独立的软件应用程序。而是一个通过协同合作构成“远程支持解决方案”的应用程序集。Insight Remote Support Advanced 能够提供主动式和被动式远程支持来提高数据中心内 HP 支持的服务器及相关存储系统的可用性。

完整的 Insight Remote Support Advanced 解决方案依靠多个 HP 组件，客户企业中各种软件应用程序之间的通信，以及客户企业与 HP 之间的通信来提供这些支持服务。本文档说明在 CMS 上安装或配置 Insight Remote Support Advanced 之前，为受管系统建立一个稳定环境所需的准备工作。软件组件将根据其用途安装在 CMS 或受管系统上。**Insight Remote Support Advanced 是一种包含许多变数的复杂解决方案，因此在继续完整安装 Insight Remote Support Advanced 之前，请务必通读本文档。**

缩略词说明

虽然本指南附有正式词汇表，但该缩略词指南可以供您快速检索本文档中的常见词汇。

缩略词	正式词汇	定义
ACC	Advanced Configuration Collector	ACC 规则安装在 CMS 上。ACC 软件库安装在 HP-UX 受管系统上。
CMS	中央管理服务器	CMS 是管理域中执行 HP Systems Insight Manager 软件的系统。HP Systems Insight Manager 中的所有核心操作都是从该系统执行。
ELMC	Event Log Monitoring Collector	ELMC（以前称为 WCCProxy）用于检测事件日志的错误状况并向 WEBES 通知这些事件。
EVA	企业虚拟阵列	EVA 是针对高端企业环境的一种高性能、高容量、高可用性虚拟 RAID 存储解决方案。

缩略词	正式词汇	定义
HP SIM	Hewlett-Packard Systems Insight Manager	HP SIM 是一个统一的服务器与存储管理平台。系统管理员从一个管理控制台即可使用安全管理工具集来管理整个 HP 服务器与存储环境。
ISEE	Instant Support Enterprise Edition	ISEE 是 Insight Remote Support Advanced 软件的前身，已不再支持。
MC3	Remote Support 公共组件	MC3 为发送至 HP 的事件提供唯一标识信息。
MVAA	Multi-Vendor and Application Adapter	MVAA 是能够使 Management Platform Synchronizer 支持 HP Operations Manager 与 Multi Vendor Support 的软件包。HP 客户服务团队可提供有关这些产品的其他信息。
OSEM	Open Service Event Manager	OSEM 自 Insight Remote Support Advanced A.05.40 起停用，已替换为 WEBES 5.6。
RDC	远程设备收集	RDC 是通过远程支持技术收集配置信息，以提供主动式远程支持服务的过程。
RDM	远程设备监控	RDM 是一个完整的监控过程，包括从受管系统捕获硬件事件，在 CMS 上过滤这些事件，通过 Insight Remote Support Advanced 将可响应事件提交给 HP，并由 HP 根据客户的支持授权级别为这些事件提供支持。
RSCC	Remote Support Configuration Collector	RSCC 安装在 CMS 上来处理配置数据集合。
RSCCE	Remote Support Configuration Collector Extension	RSCCE 支持 SAN 设备的配置数据收集。
RSNC	Remote Support Network Component	面向 HP 授权客户的支持网络服务。
RSP	以前称为 Remote Support Pack 的解决方案，现在称为 Insight Remote Support Advanced	Insight Remote Support Advanced 提供主动式远程监控、诊断与故障排除来帮助提高数据中心内 HP 支持的服务器与存储系统的可用性。HP 远程支持通过系统支持来降低成本和复杂程度。HP 远程支持将硬件事件信息通过防火墙和/或 Web 代理安全地传送到 HP 支持中心以进行响应式支持。此外还会根据支持协议的规定，收集系统信息进行主动分析与服务。
RSSWM	Remote Support Software Manager	RSSWM 是 Insight Remote Support Advanced 解决方案不可或缺的组件。它通过 HP SIM 安装在 CMS 上。
SFM	系统故障管理	SFM 是实施 WBEM 标准的 HP-UX 故障管理解决方案。SysFaultMgmt 与其他易于管理的应用程序（如 HP SIM 和 HP SMH）以及其他任何基于 WBEM 的客户端（如 WEBES）集成在一起。
SMH	System Management Homepage	SMH 是一个基于 Web 的界面，它整合并简化了在 HP-UX、Linux 和 Windows 操作系统上对 HP 服务器进行单系统管理的过程。
SMS/SMA	存储管理服务器或应用程序	SMS/SMA 是安装了 HP StorageWorks 企业虚拟阵列 (EVA) 软件的系统，包括 HP Command View EVA 和 HP Replication Solutions Manager（如果使用）。它是独占运行 EVA 管理软件的专用管理服务器。
WBEM	基于 Web 的企业管理	WBEM 实质上是一项业界倡议，用来将不同平台间的管理信息进行标准化。
WEBES	基于 Web 的企业服务	安装在CMS上的远程支持组件，可通过产品的专属规则集来执行实时服务事件分析。改进功能推出后，这些规则集会定期更新。

印刷字体约定

find(1)　　HP-UX 联机帮助页。在此示例中，“find”是联机帮助页的名称，“1”是联机帮助页的小节编号。

《书名》	表示文档中引用的书籍、手册的名称，以宋体表示。
《链接的书名》	指向一本书或其他文档的超链接。
http://www.hp.com	网站地址，它是指向某个站点的超链接。
系统字体	表示计算机显示的文本和系统项。
键盘操作	键盘键名称。注意 **Return** 和 **Enter** 指的是同一个键。键序列（如 **Ctrl+A**）表示在按住 **Ctrl** 键盘的同时按下 **A** 键。
术语	表示文档中引用的专用术语，以宋体表示。
变量	环境变量的名称，例如，`PATH` 或 `errno`。
可替换变量	命令、功能中可以替换的变量名以仿宋表示。
<元素>	在一种标记语言中使用的元素。
属性=	在一种标记语言中使用的属性。

相关文档与必需文档

如需其他 Insight Remote Support Advanced 文档，请访问： http://docs.hp.com/en/netsys.html#Remote Support Pack

表 1 支持文档

文档	必读文档或推荐文档
《HP Systems Insight Manager Installation and Configuration Guide for Microsoft Windows》	在 CMS 上安装与配置 HP SIM、SMH 和 Remote Support Software Manager (RSSWM) 时，请先阅读此文档。
位置： http://h18013.www1.hp.com/products/servers/management/hpsim/infolibrary.html#b2	
《Insight Remote Support Advanced 受管系统指南》	必读文档
位置： http://docs.hp.com/en/netsys.html#Remote Support Pack	
《HP Insight Remote Support Advanced CMS 配置与使用指南》	必读文档
位置： http://docs.hp.com/en/netsys.html#Remote Support Pack	
《A.05.40 Insight Remote Support Advanced Release Notes》	确定受管系统的支持级别时，请先阅读此文档。
位置： http://docs.hp.com/en/netsys.html#Remote Support Pack	
《HP Remote Support Software Manager Configuration, Usage and Troubleshooting Guide for Insight Remote Support Advanced》	仅在修改 Insight Remote Support Advanced 包与 RSSWM 工具自身的设置时，才需要先阅读此文档。
位置： http://docs.hp.com/en/netsys.html#Remote Support Pack	

表 1 支持文档 (续)

文档	必读文档或推荐文档
《Remote Support Software Manager A.05.40 Upgrade Guide》	仅在从先前版本升级 Insight Remote Support Advanced 时，才需要先阅读此文档。对于全新安装，请参阅《HP Systems Insight Manager Installation and Configuration Guide for Microsoft Windows》 中的相关说明。
位置： http://docs.hp.com/en/netsys.html#Remote Support Pack	
《EVA CommandView Installation Guide》	仅在安装 Insight Remote Support Advanced 以监控 EVA 设备时，才需要先阅读此文档。
位置： http://bizsupport2.austin.hp.com/bc/docs/support/SupportManual/c01681292/c01681292.pdf	
HP Insight Management WBEM Providers 网站	有关 WBEM Providers 和凭据的详细信息，请访问 WBEM Providers 网站。
位置： http://h18013.www1.hp.com/products/servers/management/wbem/documentation.html?jumpid=reg_R1002_USEN	
《HP WEBES Reference Guide》	提供关于 System Event Analyzer (SEA) 用户界面的详细信息。
位置： http://h18023.www1.hp.com/support/svctools/webes/index.html	
《HP WEBES Installation, Configuration, and Usage Guide》	如果您在安装 Insight Remote Support Advanced 组件之前，遇到无法删除旧版 HP WEBES 或 WCCProxy 的情况，建议您参阅此手册。
位置： http://h18023.www1.hp.com/support/svctools/webes/index.html	
《HP-UX 系统故障管理管理员指南》	如果因为未达到 《Insight Remote Support Advanced 受管系统指南》 中定义的 SFM 最低要求而无法获得 HP-UX 受管系统支持，建议阅读此文档。
位置： http://docs.hp.com/en/5992-6257/5992-6257.pdf	

1 Insight Remote Support Advanced：受管系统概述

1.1 了解受管系统的先决条件

要使用 Insight Remote Support Advanced，至少需要两个硬件：充当中央管理系统 (CMS) 的兼容 Windows ProLiant 设备以及至少一个受管系统。 需要先确认您的受管系统确实易于管理，然后再开始使用 Insight Remote Support Advanced。本文档 《Insight Remote Support Advanced 受管系统指南》 提供了在 CMS 上安装和配置 Insight Remote Support Advanced 软件**之前**，验证是否已正确配置硬件的必要信息。

1.1.1 受管系统上的通信协议

受管系统可以使用下列一种或多种协议与 CMS 进行通信：

- SNMP
- WBEM
- ELMC

适当的通信协议由受管系统类型和所需的通信决定。请阅读本文档中的相应受管系统章节，了解特定受管系统所需的配置。

在某些情况下，可能需要多种协议。这是因为 CMS 上的 HP SIM 可能会使用某些协议来发现受管系统，而其他协议可能会用来监控硬件事件或从受管系统检索数据集合信息。下表特别指出了各种要求，但您必须根据受管系统类型阅读相应的受管系统章节来了解详细信息。

表 1-1 受管系统的必要信息

受管系统类型	设备发现	硬件事件的远程监控	远程数据收集
Windows ProLiant	SNMP 或 WBEM	SNMP 或 WBEM	SNMP 或 WBEM
ProLiant Linux	SNMP 或 WBEM	SNMP 或 WBEM	SNMP 或 WBEM
Integrity Linux	WBEM	WBEM	WBEM
Integrity Windows 2003	WBEM	ELMC	WBEM
Integrity Windows 2008	WBEM	WBEM	WBEM
HP-UX	WBEM (SFM)	WBEM (SFM)	WBEM (SFM)
OpenVMS	ELMC	ELMC	ELMC
Tru64 Unix	ELMC	ELMC	ELMC
SanSwitch 和磁带库	SNMP	SNMP	SNMP
基于目标的 MSA	SNMP	SNMP	SNMP
EVA	SNMP 或 WBEM	ELMC	CommandView for EVA

1.2 受管系统建议

1.2.1 常规建议

注释： 使用 WBEM 凭据监控受管系统时，如果更改了用户名/密码（无论是由于凭据太旧或过期而自动更改，还是在维护时手动更改），您都必须在 CMS 上的 HP SIM 中修改这些凭据，才能继续监控受管系统。

以下建议针对本文档未提及或未详细说明的受管系统类型

- 关于多供应商或多平台支持，请联系 HP 客户服务团队成员了解详细信息。
- 对于 NonStop Systems，请参阅本文档的 Windows Integrity 一章。

注释： 为支持 NonStop，受管系统需要有 Open System Management (OSM) T0682 SPR H02 ABU。

CMS 还有其他专门针对 NonStop 支持的软件要求。有关详细信息，请参阅《HP Insight Remote Support Advanced CMS 配置与使用指南》 。

1.3 收集必要的受管系统信息

注释： 使用下表可了解各个受管系统的相关信息。配置 CMS 时将会用到此信息，您还可能需要此信息来确认受管系统是否兼容且已做好与 Insight Remote Support Advanced 一起使用的准备。

表 1-2 受管系统的必要信息

必需的项目	值
标准主机名	
IP 地址	
将在此受管系统上使用的 WBEM 帐户名称	
场所（受管系统的物理位置）	
序列号	
产品编号	
SAID 或系统标识号	
主要支持联系人	
主要联系人的电话号码	
主要联系人的电子邮件地址	
主要联系人的可联系时间	
其他联系人的电话号码	
其他联系人的电子邮件地址	

1.4 关于本文档

《A.05.40 Insight Remote Support Advanced Release Notes》（可从 http://docs.hp.com/en/netsys.html#Remote Support Pack 获取）中包含受支持受管系统的硬件和操作系统要求。

相应章节中会详细介绍专用于**受管系统远程支持**的软件和配置要求。

重要信息： 受管系统章节结构合理，因此如果您**不需要**对下列任何一种受管系统类型进行监控，就可以直接跳过相应章节。

- 第 2 章“配置运行 Windows 的 ProLiant 受管系统”
- 第 3 章“为 ProLiant Linux 受管系统配置 SNMP 支持”
- 第 4 章“配置运行 VMware ESX-i 的 ProLiant 受管系统”
- 第 5 章“配置运行 VMware ESX 的 ProLiant 受管系统 ”
- 第 6 章“Linux Integrity 受管系统的先决条件”
- 第 7 章“Windows Integrity 服务器受管系统先决条件”
- 第 8 章“安装并配置 NonStop 受管系统”
- 第 9 章“Insight Remote Support 对 HP-UX 受管系统的要求”
- 第 10 章“OpenVMS 受管系统支持 Insight Remote Support Advanced 的先决条件”

- 第 11 章“Tru64 Unix 受管系统支持 Insight Remote Support Advanced 的要求”
- 第 12 章“HP Insight Remote Support Advanced 支持 EVA 的要求 ”
- 第 13 章“Insight Remote Support Advanced 支持的 SAN 交换机与磁带库的要求”
- 第 14 章“配置 MSA 受管系统，使其支持基于目标的 SNMP”

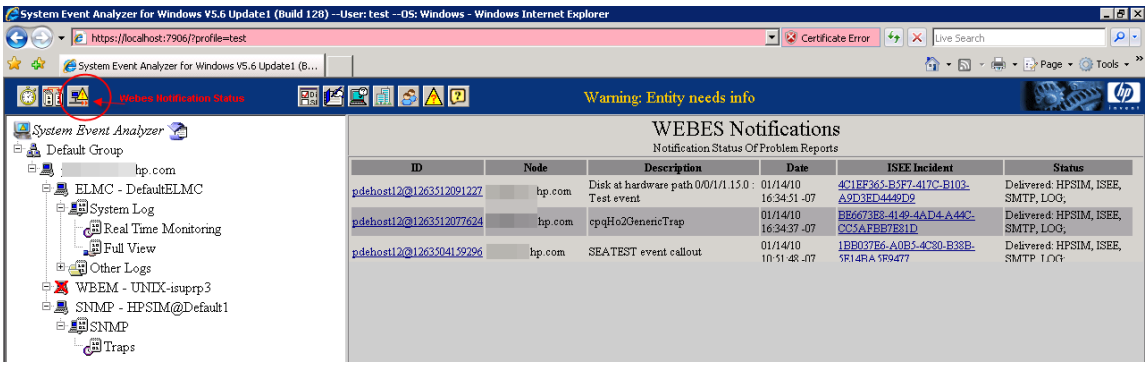
1.5 检查从受管系统发送的测试事件

有些类型的受管系统允许您向CMS发送测试事件、陷阱或指示。配置完受管系统并向CMS发送测试事件后，请执行下列过程在 CMS 上查找测试事件、陷阱或指示。

1. 登录 System Event Analyzer (SEA)：
   a. 单击开始→程序→ **Hewlett-Packard Service Tools → System Event Analyzer → System Event Analyzer**。

   注释： 如果从其他系统登录到 CMS，请打开 Web 浏览器并输入以下 URL 地址：`https://localhost:7906`
   如果 `localhost` 对您不适用，请使用 CMS 的标准主机名或 IP 地址代替。

   b. 系统将提示您为会话输入配置文件用户名，您可以选择任何名称。输入名称并单击 **Logon**。
   c. 如果浏览器提示该站点没有已签署的证书，请单击链接以继续浏览网页。此应用程序在 CMS 上运行。
2. 在 SEA 界面中单击 **WEBES 通知状态**图标（参见下图中带圆圈的图标）。



3. 如果您的受管系统已正确配置，并且您发送了测试事件，该测试事件将显示在 SEA 的输出中。

2 配置运行 Windows 的 ProLiant 受管系统

必须执行下列操作，才能监控 Windows ProLiant 受管系统：

- 参阅 《A.05.40 Insight Remote Support Advanced Release Notes》，验证您的受管系统是否受支持。
- 从受管系统中删除所有旧版或冲突的远程支持软件。
- 确认 ProLiant 受管系统上已安装 SNMP（如果您更喜欢用 SNMP）。HP 建议您安装 Windows SNMP 操作系统支持包。
- 确认受管系统上已安装并配置正确的 ProLiant Support Pack (PSP) 工具。如果使用 WBEM，请确认已正确配置 IM Providers。
- 测试从受管系统到 CMS 的连接。

2.1 从 Windows ProLiant 受管系统删除冲突的软件

下面几个小节将介绍从受管系统删除旧版远程支持软件应用程序所需的步骤。

2.1.1 删除 HP ISEE

仅当受管系统上安装了 HP Instant Support Enterprise Edition (ISEE) 时，才需要执行这些步骤。如果受管系统上未安装 ISEE，可以跳过本节。

重要信息： Instant Support Enterprise Edition (ISEE) A.03.95 及更早版本与 Insight Remote Support Advanced 不是相同的应用程序，不应安装在任何带有 Insight Remote Support Advanced 的系统上。

要删除 ISEE，请执行以下步骤：

1. 在控制面板中，双击**添加/删除程序**。
2. 在**添加/删除程序**对话框中，找到 ISEE 条目（如果存在），然后单击**删除**。

2.1.2 删除 WEBES

注释： 一旦删除了 ISEE，删除 WEBES 时应该也会将 WCCProxy 一并删除。如果尚未删除 ISEE，则 WEBES 不会删除 WCCProxy。

提示： 在删除 WEBES 之前，建议您访问 System Event Analyzer (SEA) UI，并在 Managed Entities 页面中找到系统序列号和产品 ID。以后在 CMS 的 HP Insight Remote Support 中配置受管系统的属性时，可以使用此信息。

要卸载所有 WEBES 工具（包括 WCCProxy），请执行以下步骤：

1. 使用具有管理员权限的帐户登录受管系统。
2. 完全关闭所有正在运行的工具。
3. 在控制面板中双击**添加/删除程序**。
4. 在**添加/删除程序**对话框中，找到 WEBES 条目并单击**更改/删除**以运行安装向导。
5. 看到提示时，选择 **Remove** 选项。
6. 按照提示继续卸载。
7. 在**添加/删除程序**对话框中，确认不存在 WCCProxy 条目。如果存在此项目，可以通过选择并单击**删除**，手动将其删除。

2.1.3 删除 OSEM

卸载时会完全删除 OSEM 目录下的所有文件。如果需要，可以手动备份配置文件，例如 `working.props`、`hosts.txt` 或 `communities.txt`。

您可能还想备份通知文件夹，以保留所有问题报告的副本。OSEM 1.3.7 或更高版本在卸载过程中会复制所有配置和状态信息。

要卸载所有 OSEM 工具，请执行以下步骤：

1. 使用具有管理员权限的帐户登录。
2. 完全关闭所有正在运行的工具。
3. 在控制面板中双击**添加/删除程序**。
4. 在**添加/删除程序**对话框中，找到 OSEM 条目并单击**删除**以运行安装向导。

注意： 在安装向导中，只能通过第一个 **Cancel** 按钮完全退出卸载例程。之后，即使提供取消或退出选项，也无法取消或停止卸载。

5. 按照提示继续执行卸载过程。

2.1.4 关于 ProLiant Support Pack (PSP)

ProLiant Support Pack (PSP) 是系统的特定软件包，其中包含适用于 ProLiant 设备的驱动程序、实用程序以及管理代理程序。PSP 在 HP SmartStart CD 中随每个 ProLiant 一起提供。也可以在 www.hp.com/servers/psp 上获得最新版本。

注释： PSP 安装默认使用 SNMP，而 WMI 则是可选项目。

2.1.4.1 适用于 Windows 的 IM Providers 或 IM Agents

运行 MS Windows 的 HP ProLiant 系统不仅受 Insight Management Providers（支持 WBEM/WMI Mapper 的 IM Providers）支持，还受 Insight Management Agents（支持 SNMP 的 IM Agents）支持。提供程序和代理程序通过相同的 PSP 光盘提供。SmartStart CD 上和/或 ProLiant Support Pack (PSP) 8.1 版或更高版本中的 IM Providers 均受 Insight Remote Support Advanced 支持。

有关 WBEM Providers、安全性和凭据的更多信息，请访问 HP Insight Management WBEM Providers 网站，网址为 http://h18013.www1.hp.com/products/servers/management/wbem/documentation.html?jumpid=reg_R1002_USEN。

如果 Windows Proliant 受管系统上有 SNMP 和 WBEM，建议您在 HP SIM 上禁用其中一个协议的监控功能，防止发生单个受管系统故障时收到双重通知。如果没有任何智能分离存储设备（如 MSA）连接到受管系统，请禁用 SNMP。如果已安装智能分离存储设备，请在 HP SIM 中禁用 WMI 协议。通过在 HP SIM 中编辑受管系统，然后从该协议的下拉框中选择 **off**，即可完成此操作。

如果使用 Windows SNMP Agents (IM Agents)，就必须将 SNMP 配置为与 CMS 进行通信。本章提供了关于此配置的说明。

如果使用 Windows WBEM Providers (IM Providers)，可以随时手动或自动更改 WBEM 凭据，您**必须**在 CMS 的 HP SIM 用户界面中修改这些凭据的条目。有关执行此过程的说明，请参见《HP Insight Remote Support Advanced CMS 配置与使用指南》。此外，您必须在 CMS 上使用 HP SIM 为每个受管系统设置 WBEM 凭据，然后才能对它们进行监控。

注释： 在 ProLiant Support Pack 安装中，WBEM IM Providers 是可选的。请确保安装 PSP 时选择了它们。

2.1.4.2 System Management Homepage

System Management Homepage (SMH) 也是 PSP 的一部分。它会在受管系统上提供其他报告功能。在 Insight Remote Support Advanced 未强制要求的情况下，如果在安装 Insight Management Agent 期间未将 SNMP 服务正确配置为与 CMS 进行通信，可以使用 SMH 重新配置这些设置。

如果安装 ProLiant Support Pack (PSP) 的同时已安装了缺省的 SNMP 配置和可选的 WMI 配置，此时 SMH 将默认为 WMI 配置，如果选择通过 SNMP 获取硬件事件，可能需要将其重置为 SNMP。

注释： 缺省情况下，SMH 与 HP Insight Remote Support Solution 一起安装在 **CMS** 上。

2.1.5 在 Windows ProLiant 受管系统上配置 SNMP

必须将 Linux 受管系统配置为与 CMS 进行通信。如果选择使用 SNMP，需要执行以下步骤才能使受管系统与 CMS 完整通信。

参与 SNMP 通知的受管系统必须包含下列内容：

- 所有受管系统都必须具有已安装并运行 TCP/IP 的正常 Intranet 连接（例如，通过以太网适配器）。受管系统必须通过此连接与 CMS 进行双向通信。
- 受管系统需要 Insight Management Agent 软件来检测问题并生成陷阱。由 HP 发布的 IM Agents 旨在生成 SNMP 陷阱，其中包含进行更全面地分析所需的信息。
- 最后，所有受管系统都需要有 CMS 主机（已定义为陷阱目标）的 IP 地址。

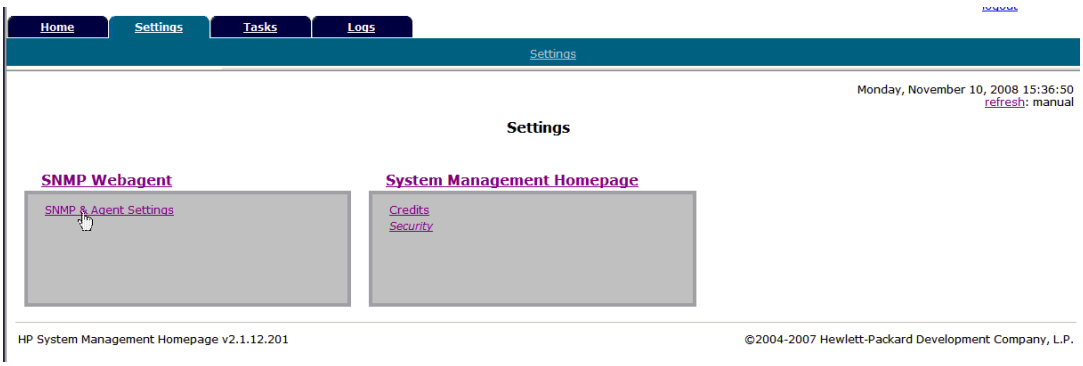
2.1.5.1 Windows 受管系统 SNMP 配置

CMS 必须能够与受管系统通信，但缺省情况下 Windows Server 2003 只接受来自 localhost 的 SNMP 包。要将 Windows Server 2003 配置为将陷阱发送至 CMS，请执行以下操作：

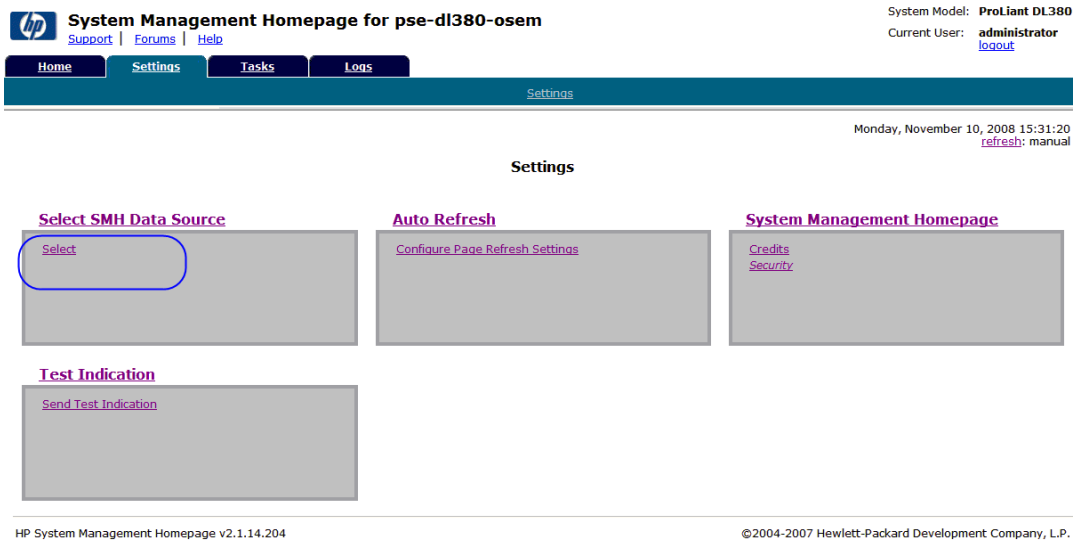
1. 在 Web 浏览器中，访问受管系统上的 System Management Homepage (SMH)：`https://ipaddress:2381`。
2. 使用受管系统的管理员用户名和密码进行登录。

注释： 如果未提示您登录，请检查 SMH 界面的右上角，并单击 **Sign In** 链接。如果不是以管理员身份登录受管系统，您将无法获得全部相关配置选项。

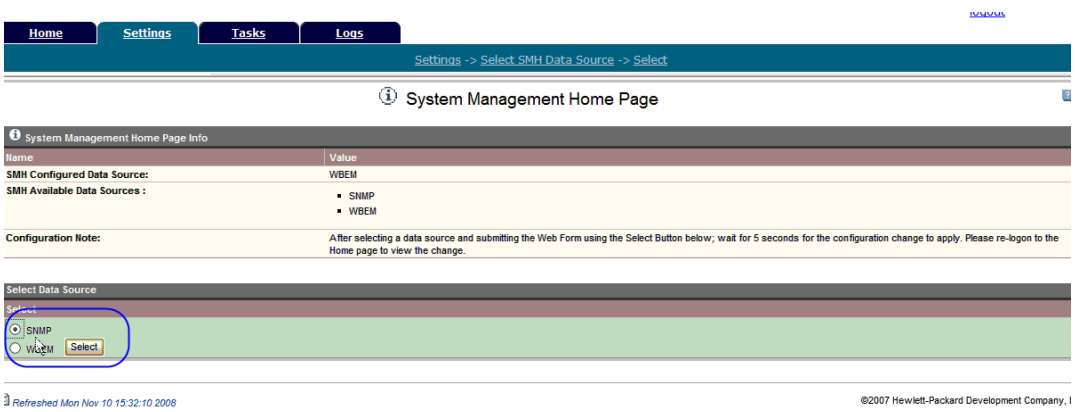
3. 单击 **Settings** 选项卡/选项。



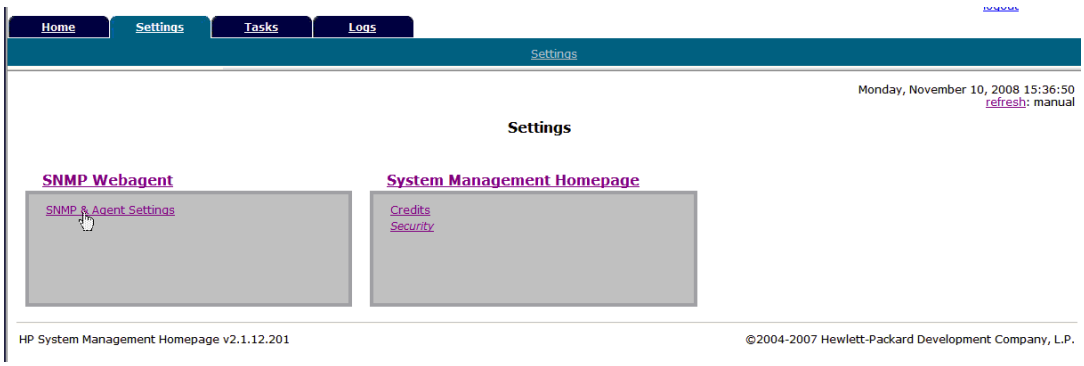
重要信息： 如果 **Settings** 选项卡未显示上述图像，却显示了以下图像，请在 **Select SMH Data Source** 框中单击 **Select** 链接。



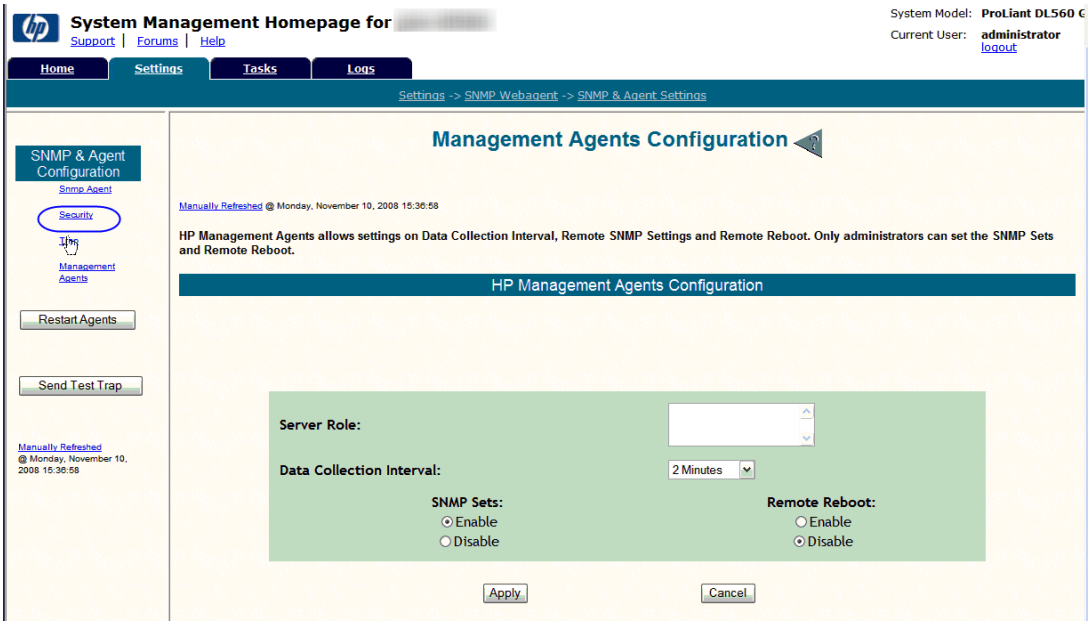
如果已在此受管系统上设置了 WBEM/WMI Providers，可能需要切换到 SNMP 设置（参见下图）。如果需要切换，可将单选按钮切换成SNMP，然后单击 **Select**。如果在受管系统上远程登录 SMH 时发生这种情况，则必须再次登录，并返回到 **Settings** 选项卡。



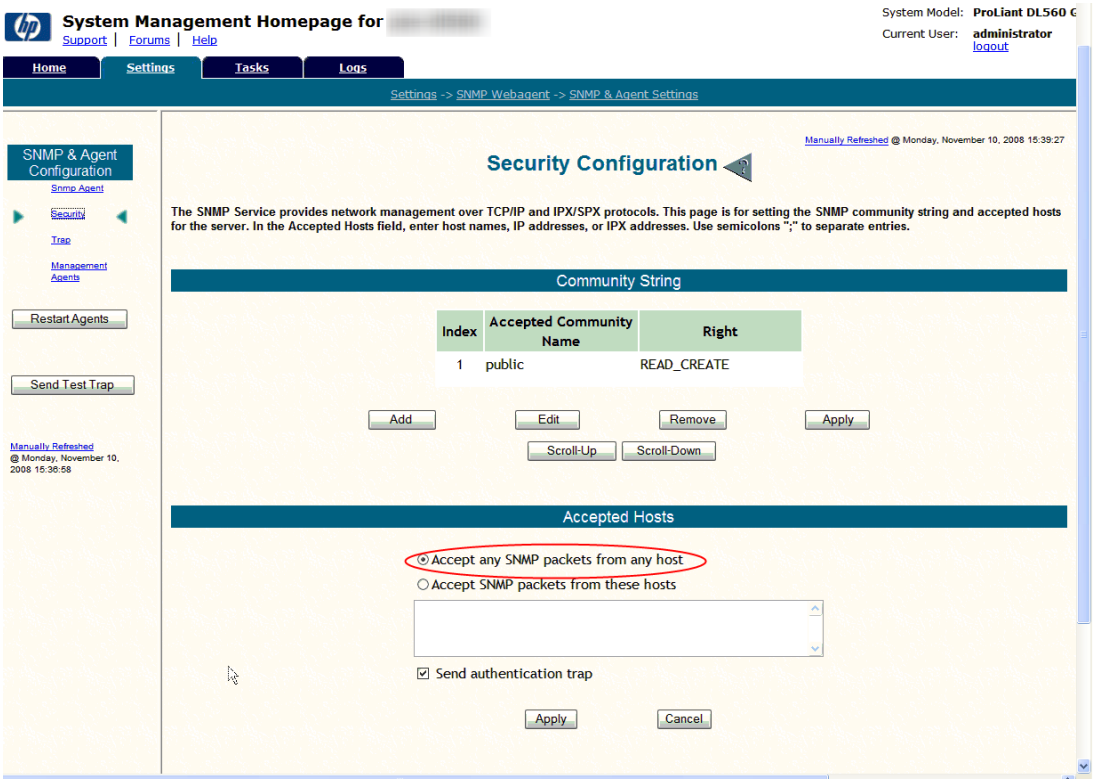
4. 在 **SNMP Web Agent** 框中，单击 **SNMP and Agent** 链接。



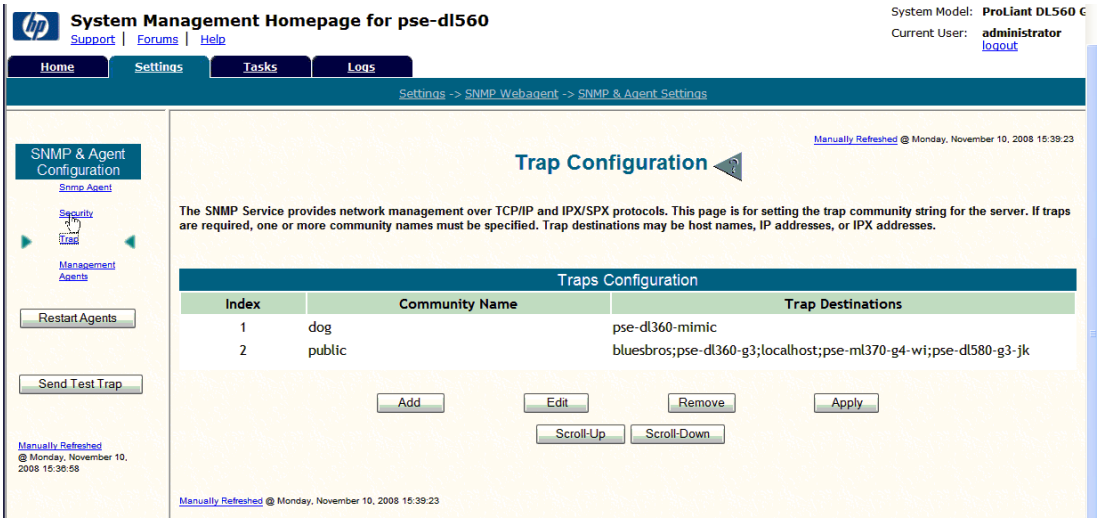
5. 在 Management Agent Configuration 屏幕的左侧导航列表中，单击 **Security** 链接。



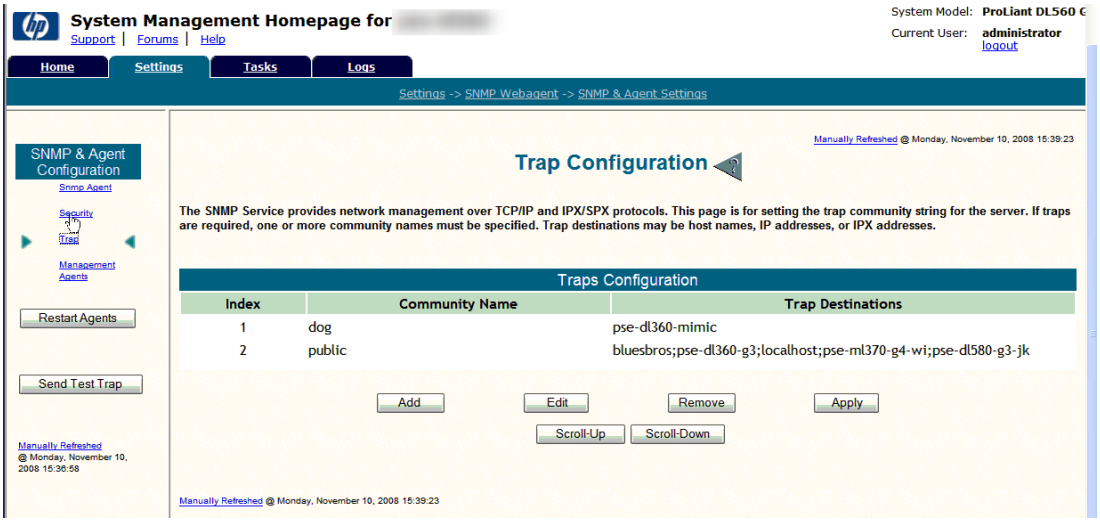
6. 在 Security 屏幕中，可以在 **Accept SNMP packets from these hosts** 选项中指定 CMS 的 IP 地址，也可以只选择 **Accept SNMP packets from any host** 选项。



7. 在 Security 屏幕左侧，单击 **Traps** 链接。



8. 在 **Trap Configuration** 屏幕中，可以添加将包含 CMS 的团体字符串，也可以编辑公共字符串以包含 CMS。



注释： 您需要为每个要通过 SNMP 与 CMS 通信的 Windows ProLiant 受管系统完成上述步骤。

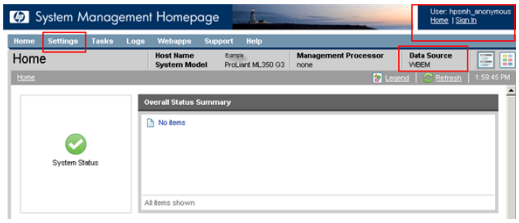
2.2 从受管系统发送测试事件到 CMS

2.2.1 发送 WBEM 测试指示

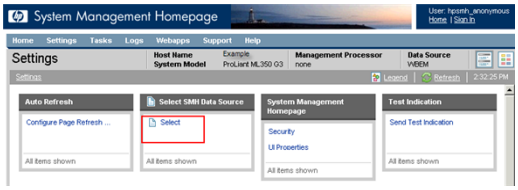
1. 在 Web 浏览器中，访问受管系统上的 System Management Homepage (SMH)：`https://ipaddress:2381`。
2. 使用受管系统的管理员用户名和密码进行登录。

注释： 如果未提示您登录，请检查 SMH 界面的右上角，并单击 **Sign In** 链接。如果不是以管理员身份登录受管系统，您将无法获得全部相关配置选项。

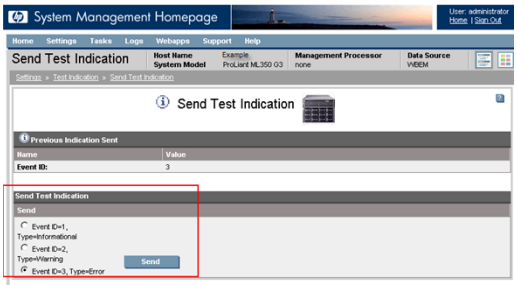
3. 单击 **Settings** 选项。



4. 如果选择用 ProLiant Support Pack 安装 WBEM，会将其设置为数据源，请单击 **Send Test Indication** 选项。



在 **Send Test Indication** 窗口中，选择事件 ID 类型（任何类型都可以），然后单击 **Send** 按钮。

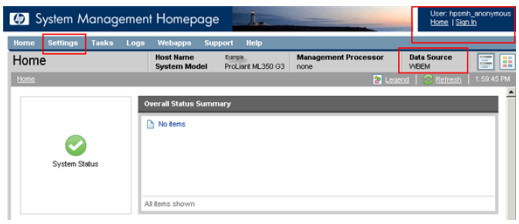


2.2.2 发送 SNMP 测试陷阱

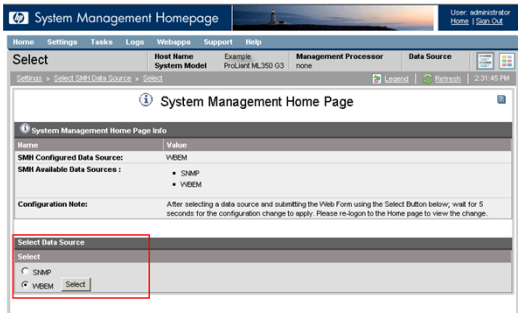
1. 在 Web 浏览器中，访问受管系统上的 System Management Homepage (SMH)：`https://ipaddress:2381`。
2. 使用受管系统的管理员用户名和密码进行登录。

注释： 如果未提示您登录，请检查 SMH 界面的右上角，并单击 **Sign In** 链接。如果不是以管理员身份登录受管系统，您将无法获得全部相关配置选项。

3. 单击 **Settings** 选项。



4. 如果选择用 ProLiant Support Pack 安装 WBEM，会将其设置为数据源。在这种情况下，要使用 SNMP，可以单击 **Select SMH Data Source** 标题下方的 **Select** 选项，将其更改为 SNMP。



在 Data Source 选项菜单中，选择 **SNMP** 单选按钮，然后单击 **Select** 按钮。

5. 将 Data Source 设置为 SNMP 后，立即单击 **Settings** 选项，然后选择 **SNMP & Agent Configuration** 设置。
6. 在 **Management Agents Configuration** 窗口中，单击 **Send Test Trap** 按钮。

请参阅“检查从受管系统发送的测试事件”，了解有关查看测试说明或陷阱的详细信息。

3 为 ProLiant Linux 受管系统配置 SNMP 支持

必须执行下列操作，才能使用 SNMP 监控 ProLiant 受管系统：

- 参阅 《A.05.40 Insight Remote Support Advanced Release Notes》 ，确认系统受支持。
- 确认已删除旧版远程支持工具（如果合适）。
- 确认系统上已安装并配置正确的 ProLiant Support Pack (PSP) 工具。

注释： 对于支持的 Linux ProLiant，您必须先从 PSP 安装（或确认是否已安装）IM Agents 7.1 版或更高版本，然后才能继续操作。当 SNMP 支持（包括 IM Agents 和 Health Drivers）与 WBEM（包括 IM Providers 和 Health Drivers）位于同一受管系统时，将不受支持。如果您打算支持带有 SNMP 的受管系统，则必须根据 ProLiant Support Pack 文档删除 WBEM 支持功能（如果已安装）。

- 确认已在 Linux ProLiant 受管系统上安装并正确配置了 SNMP
- 测试从受管系统到 CMS 的通信

3.1 从 Linux ProLiant 受管系统中删除发生冲突的软件

3.1.1 从 Linux ProLiant 受管系统中删除 HP ISEE

1. 关闭所有正在运行 ISEE 客户端用户界面的浏览器。
2. 以 root 身份（系统管理权限）登录受监控的系统。
3. 转至安装 HP ISEE 时创建的目录。

注释： 此目录名称列在 `/opt/hpservices/RemoteSupport/config/installDir` 中

4. 要从受监控系统中删除 HP ISEE 软件，请运行以下命令：

   `bash uninstall.sh`

3.1.2 从 Linux ProLiant 受管系统中删除 WEBES

删除整个 WEBES 套件最简单的方法是使用交互式实用程序：

1. 要运行交互式工具，请运行以下命令：

   `/usr/sbin/webes_install_update utility`

2. 选择删除全部 WEBES 的选项
3. 按照出现的提示操作。

3.2 在受管系统上配置 SNMP

必须配置 Linux 受管系统以便与 CMS 进行通信。

参与 SNMP 通知的受管系统必须包含下列内容：

- 所有受管系统都必须具备已安装并运行 TCP/IP 的正常 Intranet 连接（例如，通过以太网适配器）。受管系统必须通过此连接与 CMS 进行双向通信。
- 受管系统需要 Insight Management Agent 软件来检测问题并生成陷阱。由 HP 发布的 IM Agents 旨在生成 SNMP 陷阱，其中包含进行更全面地分析所需的信息。
- 最后，所有受管系统都需要有 CMS 主机（已定义为陷阱目标）的 IP 地址。

3.2.1 关于 ProLiant Support Pack (PSP)

ProLiant Support Pack (PSP) 是系统的特定软件包，其中包含适用于 ProLiant 设备的驱动程序、实用程序及管理代理程序。该 PSP 在 HP SmartStart CD 中随每个 ProLiant 一起提供。也可以在 www.hp.com/servers/psp 上获得最新版本。

3.2.1.1 适用于 Linux 的 IM Agents

Insight Management Agents (IM Agents) 支持运行 Linux 的 HP ProLiant 系统，并通过 PSP 交付。Insight Remote Support 支持 SmartStart CD 和/或 ProLiant Support Pack (PSP) 7.1 版或更高版本中的 IM Agents。

注释： 在 Linux 受管系统上，`/etc/snmp/snmpd.conf` 文件包含当前 SNMP 配置。在配置 IM Agents 的安装脚本期间，请查阅此文件的相关信息。当脚本提示您从远程管理站配置 SNMP 访问时，请务必提供 CMS 的 IP 地址。否则需要在受管系统上重新配置此 IP 地址。

3.2.1.2 System Management Homepage

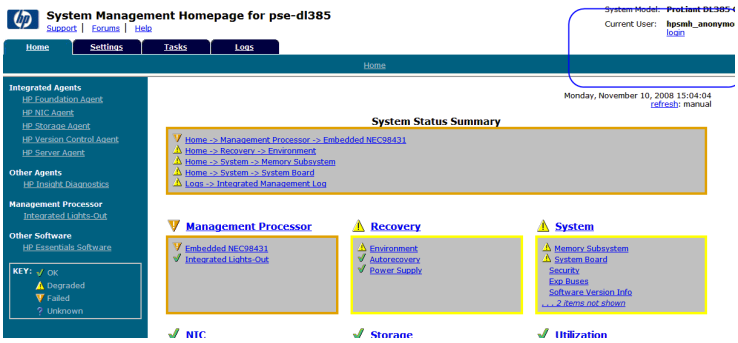
System Management Homepage (SMH) 也是 PSP 的一部分。它会在受管系统上提供其他报告功能。在 Insight Remote Support Advanced 不强制要求的情况下，如果在安装 Insight Management Agent 期间没有正确配置 SNMP 服务与 CMS 进行通信，就可以使用 SMH 重新配置这些配置。

注释： 缺省情况下，SMH 与 HP Insight Remote Support Solution 一起安装在 CMS 上。

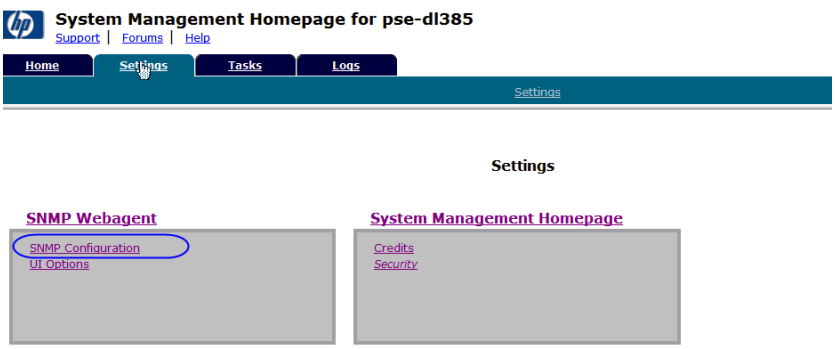
3.2.2 Linux 受管系统 SNMP 配置

如上所述，Linux 受管系统需要 Insight Management Agents。一旦将 Insight Management Agents 安装到受管系统后，就可以使用 `snmpd.conf` 文件向受管系统中的 SNMP 通信添加 CMS 的 IP 地址。您需要对每个 Linux 受管系统执行此操作。

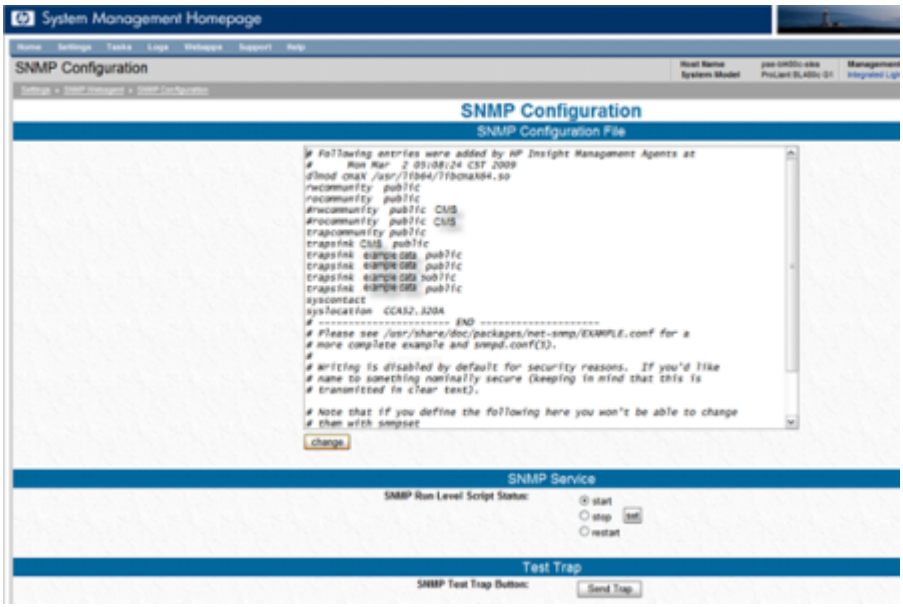
1. 在 Web 浏览器中，访问受管系统上的 System Management Homepage (SMH)：`https://ipaddress:2381`。
2. 使用受管系统的 root 用户名和密码进行登录。



3. 单击 **Settings** 选项卡。



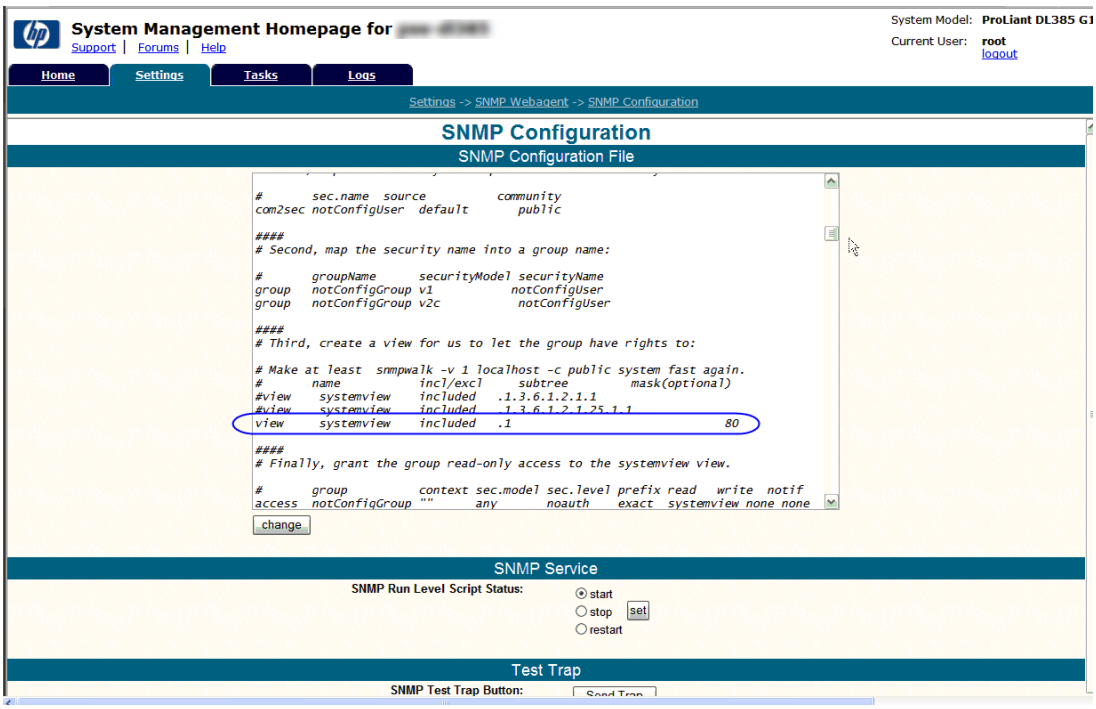
4. 单击 **SNMP Configuration** 链接。
5. 在 **SNMP Configuration File** 中添加包含 CMS IP 地址的 `trapsink` 命令（例如 `trapsink 1.2.3.4 public`），然后单击 **Change**。



注释： 对于那些支持查看语句新增安全性的 Linux 安装（例如 Red Hat 4 或 5），应对缺省值做如下调整。如果未将 trapsink 条目指定为 public，则必须为该受管系统，以及凭借 CMS 上的 HP SIM 使用相同团体字符串的任何其他系统配置新的 SNMP 协议。

6. 要使 CMS 能够收集所有关于此受管系统的信息，需要在 **SNMP Configuration File** 中向下滚动至 `view systemview included` 条目。用 # 字符对缺省条目加注释。然后添加此条目：

   `view systemview included .1 80`，接着单击 **Change**。



注释： 如果您未使用SMH，也可以通过在文本编辑器中编辑snmpd.conf文件来执行此操作。

3.3 将 SNMP 测试陷阱发送至 CMS

您可以按照“Linux 受管系统 SNMP 配置”中的说明使用 SMH 界面，也可以单击 **Settings** 选项卡上的 **Send Trap**。除此之外，还可以输入以下命令，将测试陷阱发送至 CMS。

```
snmptrap -v1 -c public CMS IP Address.1.3.6.1.4.1.232 Linux Managed
System IP Address 6 11003 1234 .1.3.6.1.2.1.1.5.0 s test
.1.3.6.1.4.1.232.11.2.11.1.0 i 0 .1.3.6.1.4.1.232.11.2.8.1.0 s "provide
your own identifiable identifier and time stamp"
```

此时将返回含有受管系统和 CMS 详细信息的结果文本。

```
Management Agents Test Trap sent -“timestamp”
```

请参阅“检查从受管系统发送的测试事件”，了解有关查看测试说明或陷阱的详细信息。

4 配置运行 VMware ESX-i 的 ProLiant 受管系统

必须执行下列操作，才能监控 ESX-i ProLiant 受管系统：

- 参阅 《A.05.40 Insight Remote Support Advanced Release Notes》 ，确认系统受支持。
- 根据制造商的说明书验证是否已配置了 ESX-i 系统。如果已正确配置，将提供所需的全部 WBEM Providers。

4.1 关于 VMware ESX-i 与 Insight Remote Support Advanced

VMware ESX-i（已正确且完整安装时）将包含所需的 WBEM Providers，以便将硬件事件发送给 CMS。在 CMS 上为此受管系统配置 WBEM 协议时，需要使用 ESX-i 系统的 root 帐户凭据。由于 ESX-i 中没有 System Management Homepage 功能，因此，目前不存在可从受管系统运行至 CMS 的 WBEM 指示测试。

5 配置运行 VMware ESX 的 ProLiant 受管系统

必须执行下列操作，才能监控 ESX ProLiant 受管系统：

- 通过查看《A.05.40 Insight Remote Support Advanced Release Notes》 验证您的受管系统是否受支持。
- 确认您的 ProLiant 受管系统上已正确配置了 SNMP

5.1 在 ESX 受管系统上配置 SNMP

必须将 Linux 受管系统配置为与 CMS 进行通信。VMware ESX 使用 SNMP 与 CMS 进行通信。缺省情况下，SNMP 与 VMware ESX 一同安装，但是您必须将受管系统 SNMP 配置为与 CMS 进行通信。

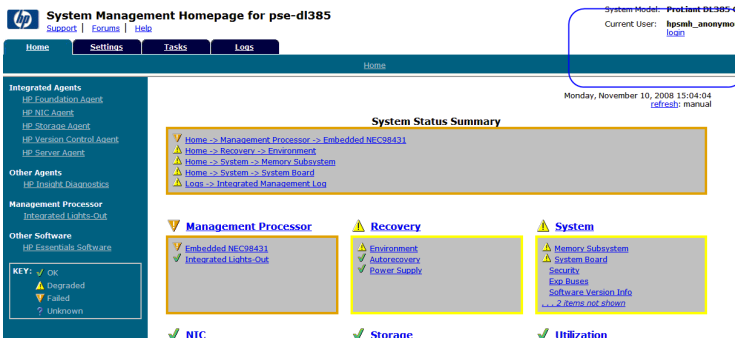
参与 SNMP 通知的受管系统必须包含下列内容：

- 所有受管系统都必须具备已安装并运行 TCP/IP 的正常 Intranet 连接（例如，通过以太网适配器）。受管系统必须通过此连接与 CMS 进行双向通信。
- 受管系统需要 Management Agent 软件来检测问题并生成陷阱。由 HP 发布的 IM Agents 旨在生成 SNMP 陷阱，其中包含进行更全面地分析所需的信息。管理代理程序与 VMware ESX 一起，是 VMware ESX 包的一部分。因此，如果已正确配置了受管系统，代理程序将会出现在系统上。
- 最后，所有受管系统都需要有 CMS 主机（已定义为陷阱目标）的 IP 地址。

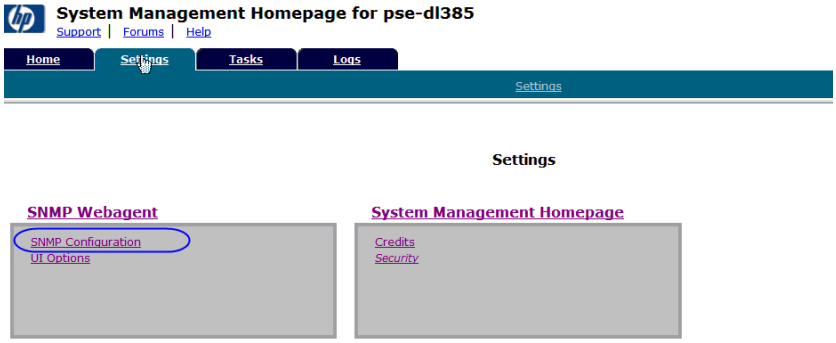
5.1.1 VMware ESX SNMP 配置

您可以在文本编辑器中访问 `snmpd.conf` 文件，向受管系统中的 SNMP 通信添加 CMS 的 IP 地址，也可以使用 System Management Homepage 来配置 SNMP。您需要对每个 VMware ESX 受管系统执行此操作。

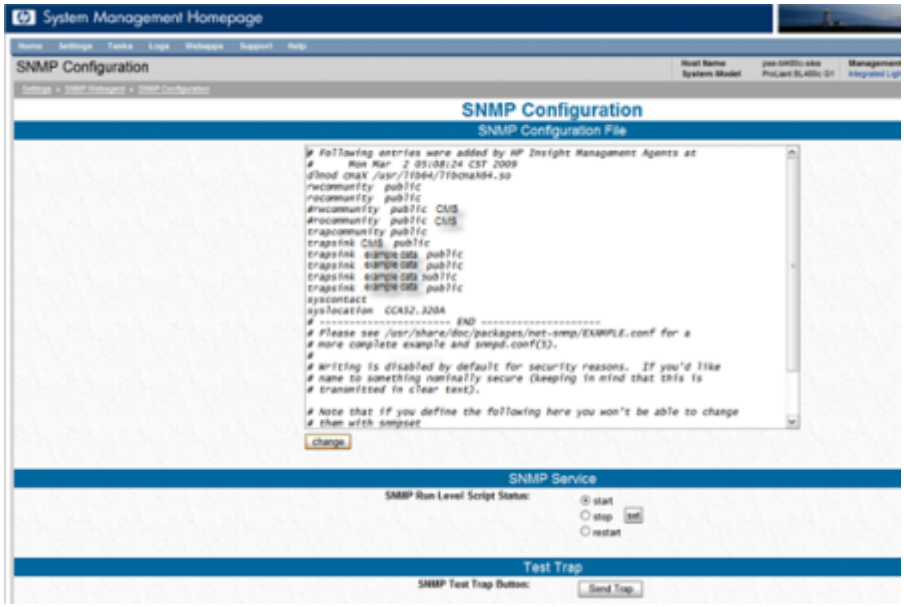
1. 在 Web 浏览器中，访问受管系统上的 System Management Homepage (SMH)：`https://ipaddress:2381`。
2. 使用受管系统的 root 用户名和密码进行登录。



3. 单击 **Settings** 选项卡。



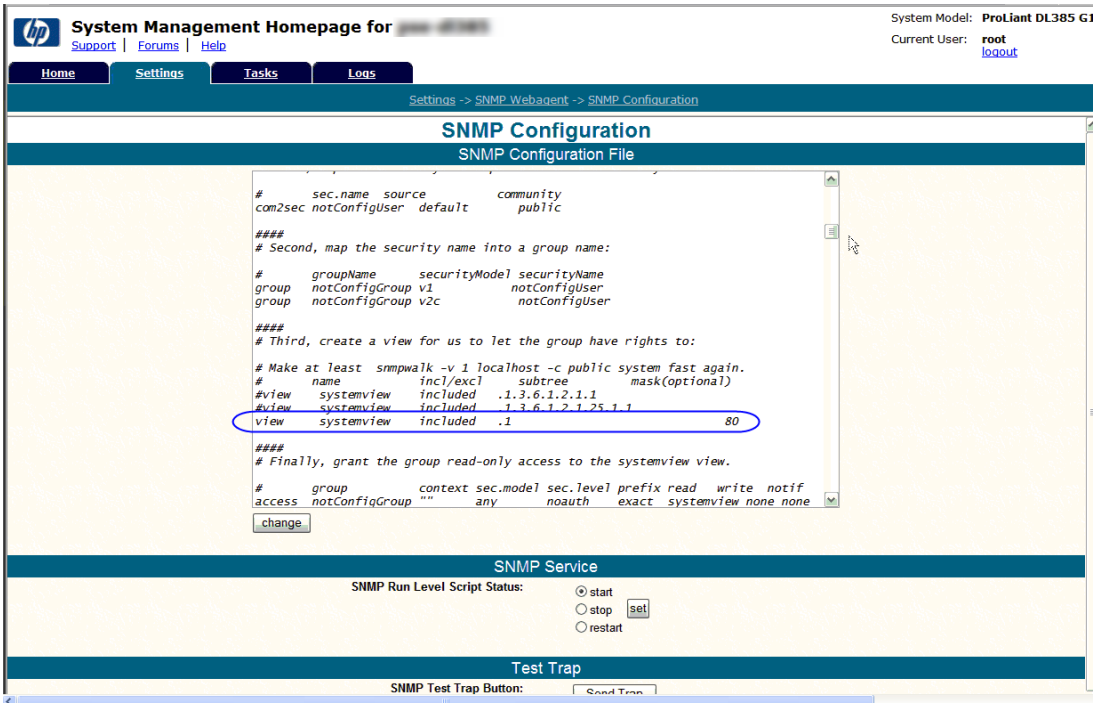
4. 单击 **SNMP Configuration** 链接。
5. 在 **SNMP Configuration File** 中添加包含 CMS IP 地址的 `trapsink` 命令（例如 `trapsink 1.2.3.4 public`），然后单击 **Change**。



注释： 对于支持查看语句新增安全性的安装，应对缺省值做如下调整。如果未将 trapsink 条目指定为 public，则必须为该受管系统，以及凭借 CMS 上的 HP SIM 使用相同团体字符串的任何其他系统配置新的 SNMP 协议。

6. 要使 CMS 能够收集所有关于此受管系统的信息，需要在 **SNMP Configuration File** 中向下滚动至 `view systemview included` 条目。用 # 字符对缺省条目加注释。然后添加此条目：

   `view systemview included .1 80`，接着单击 **Change**。



注释： 如果您未使用SMH，也可以通过在文本编辑器中编辑snmpd.conf文件来执行此操作。

5.2 将 SNMP 测试陷阱发送至 CMS

您可以按照“VMware ESX SNMP 配置”中的说明使用 SMH 界面，也可以单击 **Settings** 选项卡上的 **Send Trap**。除此之外，还可以输入以下命令，将测试陷阱发送至 CMS。

```
snmptrap -v1 -c public CMS IP Address.1.3.6.1.4.1.232 Linux Manage
System IP Address 6 11003 1234 .1.3.6.1.2.1.1.5.0 s test
.1.3.6.1.4.1.232.11.2.11.1.0 i 0 .1.3.6.1.4.1.232.11.2.8.1.0 s "provide
your own identifiable identifier and time stamp"
```

请参阅“检查从受管系统发送的测试事件”，了解有关查看测试说明或陷阱的详细信息。

6 Linux Integrity 受管系统的先决条件

6.1 从受管系统中删除冲突的旧版软件

在配置受管系统与 CMS 上安装的 Insight Remote Support Advanced A.05.40 版一起使用之前，必须删除当前可能已安装在受管系统上的所有先前版本 WEBES 或 HP ISEE 客户端。另外，还必须删除旧版 WCCProxy，但在卸载 WEBES 时通常会自动将其一并卸载。

仅当已在受管系统上安装了任意版本的 HP ISEE 客户端、WEBES 或 WCCProxy 时，才需要执行下列步骤。如果尚未安装上述任何应用程序，可跳过此节。

6.1.1 从 Linux 受管系统中删除旧版应用程序

6.1.1.1 从 Linux 受管系统中删除 HP ISEE

1. 关闭所有正在运行 ISEE 客户端用户界面的浏览器。
2. 以 root 身份（系统管理权限）登录受监控的系统。
3. 转至安装 HP ISEE 时创建的目录。

注释： 此目录名称列在 `/opt/hpservices/RemoteSupport/config/installDir` 中

4. 要从受监控系统中删除 HP ISEE 软件，请运行以下命令：

   `bash uninstall.sh`

6.1.1.2 从 Linux 受管系统中删除 WEBES

删除整个 WEBES 套件最简单的方法是使用交互式实用程序：

1. 要运行交互式工具，请运行以下命令：

   `/usr/sbin/webes_install_update utility`

2. 选择删除全部 WEBES 的选项
3. 按照出现的提示操作。

6.2 Integrity Linux 受管系统需要 HP WBEM Providers

重要信息： 在中央管理服务器 (CMS) 上配置 Insight Remote Support Advanced 时，必须在 HP SIM 界面中为 Linux Integrity 受管系统配置 WBEM 凭据。《HP Insight Remote Support Advanced CMS 配置与使用指南》 第二章详细介绍了此过程。请将这些凭据记下来，因为稍后将需要提供这些凭据。

Integrity Linux 受管系统上需要 HP WBEM Providers。HP Support Pack 提供 Integrity Linux HP WBEM Providers 及相关文档，同时它也是更大的 HP Integrity Essentials Foundation Pack for Linux 的一部分。HP SIM 也是 Foundation Pack 的一部分，但 Insight Remote Support Advanced **不需要也不支持** HP SIM，因为 Insight Remote Support Advanced 的 HP SIM/CMS 实例必须在 Windows ProLiant CMS 上。

您可以访问 http://www.hp.com/go/integritylinuxessentials 获取最新版的 HP Integrity Essentials Foundation Pack for Linux 软件，访问 http://www.docs.hp.com/en/linux.html 获取文档。请在该网页上搜索 **HP Integrity Essentials Foundation Pack for Linux**。

6.3 将测试事件发送至 CMS

要将测试事件从受管系统发送至 CMS，请从受管系统的命令行输入以下命令：

```
touch /tmp/SMX.test
```

此命令会在 tmp 目录中创建长度为零的文件 `SMX.test`。SMX 提供程序会创建向 CMS 发送测试事件的指示，并删除上一步中创建的临时文件。

7 Windows Integrity 服务器受管系统先决条件

7.1 概述

请查看 《A.05.40 Insight Remote Support Advanced Release Notes》 ，在为 Insight Remote Support Advanced 配置 Windows Integrity 系统前，确认支持该系统。然后根据需要阅读下列各节：

注释： 要支持 Windows 2008，需满足以下要求：

- Service Pack 1 版本需要 6.2 Insight Agents。
- Service Pack 2 或版本 2 需要 6.5 Insight Agents。

WBEM Providers 在与系统中的 SNMP Agents 版本编号相同时可以共存。不支持版本不匹配的 HP Insight Management WBEM Providers 与 HP Insight Management SNMP Agents。

- “从受管系统中删除冲突软件和旧版软件”；如果受管系统上已安装旧版应用程序，请参阅本节
- “运行 Windows 2003 的 Windows Integrity 受管系统 ”；要正确配置 Windows Integrity 受管系统，请参阅本节。

7.2 从受管系统中删除冲突软件和旧版软件

在配置受管系统与 CMS 上的 Insight Remote Support Advanced 一起使用之前，必须删除当前可能已安装在受管系统上的所有旧版 WEBES 或 HP ISEE 客户端。另外，还必须删除旧版 WCCProxy，但在卸载 WEBES 时通常会自动将其一并卸载。

仅当在 Windows Integrity 受管系统上已安装任意版本的 HP ISEE 客户端、WEBES 或 WCCProxy 时，才需要执行这些步骤。如果尚未安装上述任何应用程序，可跳过此节。

重要信息： 如果您的环境中有一个或多个计划要进行监控的 HP NonStop 受管系统，这些受管系统上必须有 OSM。有关 NonStop 的配置说明，请参见 第 8 章“安装并配置 NonStop 受管系统”。如果您没有 NonStop 系统，则不必参阅此章。

7.2.1 删除 ISEE

注意： 如果打算使用 ISEE 迁移工具将系统配置数据迁移至 CMS，那么在完成《HP Insight Remote Support Advanced CMS 配置与使用指南》 中规定的迁移步骤之前，**请不要**删除 ISEE。

1. 选择**开始→设置→控制面板→添加/删除程序**。
2. 从所安装程序的列表中选择 **HP Instant Support Enterprise Edition Client**，然后单击**更改/删除**。

7.2.2 删除 WEBES

仅当已在受管系统上安装任意版本的 WEBES 时，才需要执行这些步骤。如果未安装 WEBES，可以跳过本节。

1. 使用具有**管理员**权限的帐户登录 CMS。
2. 如果 WEBES 正在运行，请在命令提示符下运行以下命令来完全关闭 WEBES（如果进程已停止，某些命令可能会返回错误）：
   - `C:\> net stop desta_service`
   - `C:\> desta stop`
   - `C:\> net stop wccproxy`
   - `C:\> wccproxy kill`

3. 在 CMS 上，导航至“添加/删除程序”：

   开始 → 设置 → 控制面板 → 添加/删除

4. 从所安装程序的列表中选择**HP WEBES**条目（旧版WEBES可能简单地列示为**WEBES**）。
5. 单击**更改/删除**按钮运行安装向导。
6. 在向导中单击**下一步**，将显示**修改或删除**页面。
7. 选择**删除**选项。**不要**选择**修改**选项。
8. 单击**删除**，并按照提示继续卸载。
9. 卸载完成后，请在“添加或删除程序”对话框中按 **F5** 键刷新程序列表。

   如果列出 **WCCProxy** 程序，请选择该程序并单击**删除**将其卸载。

   如果无法卸载 WCCProxy，请与 HP 客户支持联系，以获取 WEBES 清除工具。

7.2.3 删除 OSEM

卸载时会完全删除 OSEM 目录下的所有文件。如果需要，可以手动备份配置文件，例如 `working.props`、`hosts.txt` 或 `communities.txt`。

1. 使用具有管理员权限的帐户登录。
2. 完全关闭所有正在运行的工具。
3. 在控制面板中双击**添加/删除程序**。
4. 在**添加/删除程序**对话框中，找到 OSEM 条目并单击**删除**以运行安装向导。

注意： 在安装向导中，只能通过第一个 **Cancel** 按钮完全退出卸载例程。之后，即使提供取消或退出选项，也无法取消或停止卸载。

5. 按照提示继续执行卸载过程。

7.3 运行 Windows 2003 的 Windows Integrity 受管系统

本节及其小节仅适用于 Windows 2003 Integrity 受管系统。如果 Windows 2003 不适用，请跳至“Windows 2008”一节。Event Log Monitoring Collector (ELMC) 用于在 Windows 2003 Integrity 受管系统上监控远程支持。WBEM 是远程收集数据的必要条件。这两点会在下面几个小节中介绍。

7.3.1 满足 ELMC 基本要求

受管系统必须符合下列基本要求，您才能安装 ELMC：

- 处理器架构：Integrity 服务器上的 Itanium
- 操作系统：在 Integrity Servers 上，Windows 2003 的所有支持版本
- 已在受管服务器上配置 TCP-IP
- 所需的权限与访问权：要安装、升级或卸载 WEBES 或 ELMC 组件，您必须以管理员的身份登录，或以具有管理员权限的用户身份登录。

7.3.2 在受管系统上安装 ELMC 软件包

将相应的（IA64 或 x32/x64）ELMC 客户端从 CMS 上的 RSSWM 下载文件夹复制到临时目录。双击以启动安装程序，该工具包完成安装时不提示用户。您不需要为此软件包输入任何用户配置。

7.3.3 WBEM 和 Windows 2003 Integrity 受管系统

要让您的 Windows 2003 Integrity 受管系统能被 HP SIM 发现，并且能够支持远程数据收集，您必须在受管系统上安装并完整配置 HP Integrity WBEM Providers for Windows Server 2003。因此，下面这一节适用于 Windows 2003 和 Windows 2008 Integrity 受管系统。

7.4 确认受管系统上 WBEM 和 Agent Provider 的先决条件

要让您的 Windows Integrity 受管系统能被 HP SIM 发现，并且能够支持远程数据收集，您必须按照相应软件包内 HP SmartSetup 产品文档中的说明，在受管系统上安装并完整配置 HP Integrity WBEM Providers for Windows Server。这适用于 Windows 2003 Integrity 受管系统和 Windows 2008。Windows 2008 Integrity 受管系统也使用 WBEM 进行事件提交/远程监控。

注释： WBEM Providers 与受管系统系统上的 SNMP Agents 版本编号相同时可以共存。不支持版本不匹配的 HP Insight Management WBEM Providers 与 HP Insight Management SNMP Agents。

由 HP 提供的 Windows Integrity Server 会在操作系统盘上预先加载 SmartSetup 安装文件。此外，您还可以使用 SmartSetup CD 或重装光盘进行安装。您可以通过访问 www.hp.com/go/integrity/windows，然后单击 **Simplified management** 标题下方的 **Integrity Essentials for Windows** 链接来下载 SmartSetup Agents 或提供程序。

7.5 使用 WBEM Providers

对于要与 CMS 进行通信的 WBEM Providers，您必须提供 WBEM 凭据，如同《HP Insight Remote Support Advanced CMS 配置与使用指南》 的《为支持的受管系统配置和应用 WBEM 凭据》一节中所述。配置 Insight Remote Support Advanced 时，必须在 CMS 上的 HP SIM 用户界面中执行这些操作。

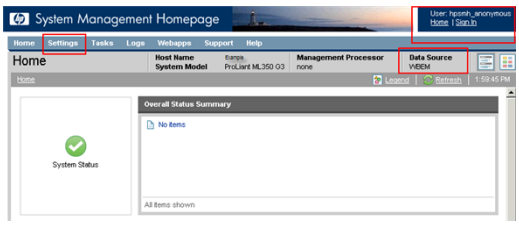
WBEM Providers 可以用来发送 WBEM 指示以确认连接，具体方法是访问 System Management Homepage，并选择 **Settings** 选项卡。然后，从 **Test Indication** 面板中，选择所显示的 3 个严重级别事件中的一个，单击 **Send**。

7.6 发送 WBEM 测试指示

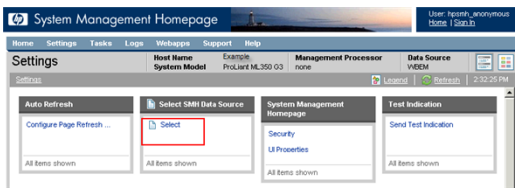
1. 在 Web 浏览器中，访问受管系统上的 System Management Homepage (SMH)：`http://ipaddress:2301`。
2. 使用受管系统的管理员用户名和密码进行登录。

注释： 如果未提示您登录，请检查 SMH 界面的右上角，并单击 **Sign In** 链接。如果不是以管理员身份登录受管系统，您将无法获得全部相关配置选项。

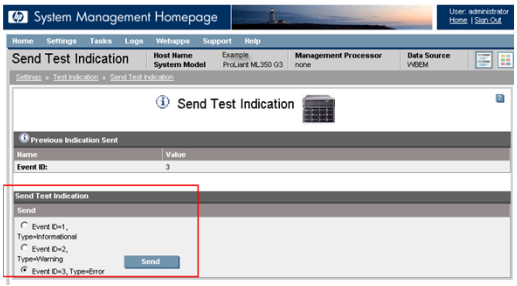
3. 单击 **Settings** 选项。



4. 如果选择用 Support Pack 安装 WBEM，会将其设置为数据源，请单击 **Send Test Indication** 选项。



在 **Send Test Indication** 窗口中，选择事件 ID 类型（任何类型都可以），然后单击 **Send** 按钮。


System Management Homepage
User: administrator
Home | Sign Out
Home Settings Tasks Logs Webapps Support Help
Send Test Indication
Host Name
System Model
Example
ProLiant ML350 G3
Management Processor
none
Data Source
WBEM
Settings » Test Indication » Send Test Indication
Send Test Indication
Previous Indication Sent
Name
Value
Event ID:
3
Send Test Indication
Send
Event ID=1, Type=Informational
Event ID=2, Type=Warning
Event ID=3, Type=Error
Send

8 安装并配置 NonStop 受管系统

注释： 独立文档《Insight Remote Support Advanced for NonStop》中也包含本章的内容，该文档位于 NonStop 技术资源库中（网址为 http://docs.hp.com/en/NSSupport.html）的 “NonStop Service Information” 下。建议您阅读该文档，以了解可能已更新的信息。

8.1 概述

HP Insight Remote Support Advanced 适用于 NonStop 系统，包括 HP Integrity NonStop BladeSystems、Integrity NonStop NS 系列系统以及 NonStop S 系列系统。Insight Remote Support Advanced 是目前适用于 NonStop 系统的最新远程支持解决方案，可取代调制解调器和 HP Instant Support Enterprise Edition (ISEE) 远程支持解决方案。

Insight Remote Support Advanced 是 HP Systems Insight Manager (SIM) 的一个插件。它采用智能事件诊断，可以将硬件事件通知（包括通知和状态）自动且安全地提交给 HP 支持，从而增强 HP SIM 的功能。

HP SIM 与 Insight Remote Support Advanced 都安装在基于 Windows 的中央管理服务器 (CMS) 上（请参阅“要求”）。理想情况下，来自客户数据中心内所有 NonStop 及其他 HP 平台的事件都会发送至该中央服务器。这样可以提供单一虚拟管理平台，从而为整个数据中心提供远程支持。

在 NonStop 系统上，OSM 会执行问题诊断并创建事件报告 (IR)。位于系统上的 OSM 软件会将这些 IR 直接发送至 Insight Remote Support Advanced（不使用 OSM Notification Director），Insight Remote Support Advanced 会将其转发给 HP 支持人员。

8.1.1 过程概述

在 NonStop 环境中使用 Insight Remote Support Advanced 需要 HP SIM 与 Insight Remote Support Advanced 文档中没有涵盖的一些 NonStop 特定详细信息。本章是标准文档的补充说明，概述了步骤顺序，提供文档链接，并说明开始使用 Insight Remote Support Advanced 需要执行其他 NonStop 特定任务的时间与方法。在 NonStop 环境中开始使用 Insight Remote Support Advanced 的过程如下：

- 确保已满足在 NonStop 环境中使用 Insight Remote Support Advanced 的所有“要求”。
- 执行“HP SIM 与 Insight Remote Support Advanced 的安装和配置”。此过程包含要在特定时间执行的一些“NonStop 特定的任务”（包括禁用 OSM Notification Director (ND)），如“Insight Remote Support Advanced 迁移方案”中所述。

8.2 要求

HP SIM 与 Insight Remote Support Advanced 都安装在称为中央管理服务器 (CMS) 的 Windows PC 上。虽然 HP 支持使用合格的 NonStop 系统控制台 (NSC) 作为 CMS，但是 HP 还是建议将 NSC 和 CMS 设定为两台不同的服务器。要将 NSC 配置为 CMS，NSC 必须运行 Windows 2003 Server，并具有至少 4 GB 的内存。目前只有运行 Windows Server 2003 的 CMS 上的 NonStop 系统才支持 Insight Remote Support Advanced。如需建议与替代配置图表的示例，请参阅“控制台配置示例”。

表 8-1 NonStop 系统软件要求：

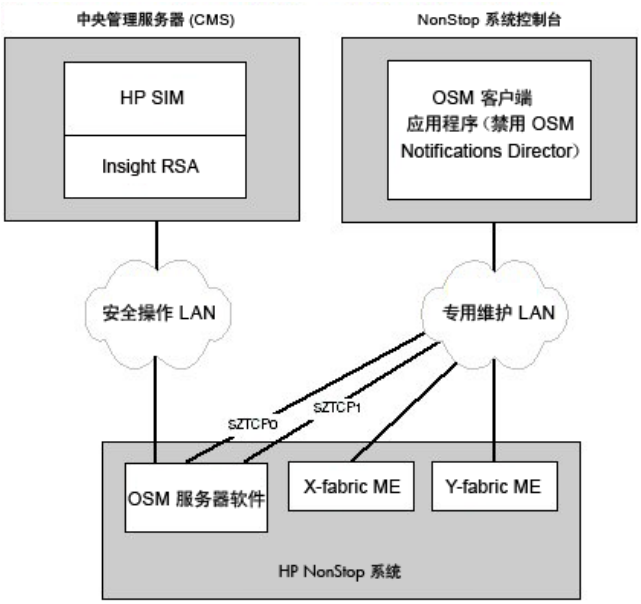
产品	最低版本
OSM（基于 Nonstop 系统的软件）	HP Integrity NonStop BladeSystems 或 Integrity NonStop NS 系列系统：T0682 ABU 或更高版本。 NonStop S 系列系统：T0682 ABY 或更高版本。
RVU	J06.03 或更高版本，H06.03 或更高版本，G06.10 或更高版本。

表 8-2 CMS 软件要求：

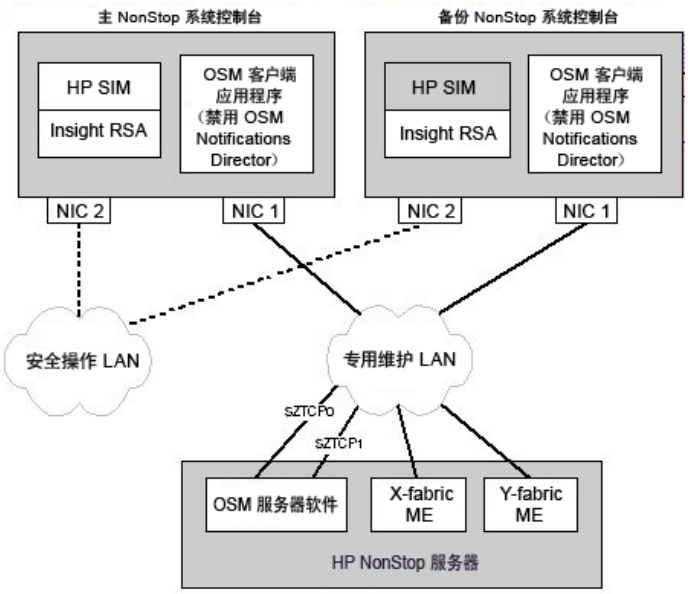
产品	最低版本	注释
HP SIM	5.3 with HotFix 或更高版本	HP SIM 包括 Remote Support Software Manager (RSSWM)，它在初始化时会安装 Insight Remote Support Advanced 和必要的组件包。
Insight Remote Support Advanced	A.05.20 或更高版本	已通过 RSSWM 下载并安装。
WEBES	G 系列：5.6 或更高版本 H/J 系列：5.5 Patch 1 或更高版本*	Insight Remote Support Advanced 的组件，通过 RSSWM 安装。
	* 如果已经安装，则也支持 WEBES 5.5 with NonStop Support Patch。如果您在早于 WEBES 5.5 with NonStop Support Patch 的版本上安装 WEBES 5.5 Patch 1，则会覆盖现有的 WEBM.jar 文件。虽然不是必要条件，但还是建议您对 H/J 系列使用 WEBES 5.6，请参阅"已知问题"了解升级到 5.6 版的好处。	
Remote Support Eligible Systems List	A.05.20.24 或更高版本	Insight Remote Support Advanced 的组件，通过 RSSWM 安装。

8.2.1 控制台配置示例

第一个示例（如下图所示）显示从 CMS（而非其中一个 NonStop 系统控制台）运行 Insight Remote Support Advanced 的推荐配置。可能会有其他的 CMS 或 NSC 设备（图中只显示其中一个），但此处的重点是 Insight Remote Support Advanced 并未在 NSC 上运行。



下面的图例显示推荐配置的替代方法，即从主和备份 NonStop 系统控制台安装和运行 Insight Remote Support Advanced。



8.3 HP SIM 与 Insight Remote Support Advanced 的安装和配置

本节包含相关说明，根据这些说明可以获取描述如何安装和配置 HP SIM 与 Insight Remote Support Advanced 的 HP SIM 和 Insight Remote Support Advanced 文档，以及在安装和配置过程中的特定时间要执行的“NonStop 特定的任务”列表。在安装和配置 HP SIM 与 Insight Remote Support Advanced 时请参阅“NonStop 特定的任务”一节，了解执行这些附加任务的合适时间。

请遵循适用于您正在安装的版本的手册说明来安装 HP SIM 与 Insight Remote Support Advanced，这些手册可在 http://docs.hp.com/en/netsys.html 中找到，标题如下：

- HP Systems Insight Manager
- Insight Remote Support
- Remote Support Pack

8.3.1 NonStop 特定的任务

1. 安装 HP SIM 5.3 之后，请下载并安装适用于 HP SIM 5.3 - MS Windows 的 HotFix 更新套件（HP SIM 5.3 with SP1 也需要此更新套件）。您可以从以下网址获取此套件：http://h18013.www1.hp.com/products/servers/management/hpsim/dl_windows.html。

注释： 安装该套件后，将会停止 HP SIM 服务，添加修补程序，然后重新启动 HP SIM。当系统在 HP SIM 中发现您的 NonStop 系统时，请等待，直到此过程提出要求为止。

2. WEBES `DESTA.REG` 文件中有两个设置必须要适当地设置，才能确保与 NonStop 兼容。从 CMS 上的 DOS 提示符执行下列命令，以指定 `wbem.useip` 和 `wbem.destname` 参数所需的值：
   - `desta dri set wbem.useip t`
   - `desta dri set wbem.destname`

   然后执行下列命令，让 DESTA.REG 文件的更改生效：
   - `net stop desta_service`
   - `net start desta_service`

3. 如果不用于监控 CMS 上的任意 NonStop 系统，请禁用该 CMS 上的 OSM Notification Director (ND)，–或者–如"Insight Remote Support Advanced 迁移方案"中所述，将 NonStop 系统配置为"非拨出点"。
4. 在要监控的各个 NonStop 系统上配置 OSM – 必须在您的 OSMCONF 文件中配置各种配置，这些配置根据您的硬件平台和 LAN 配置而有所不同。

   禁用 OSM ND 之后，在您的 OSMCONF 文件中添加适当的标志（具体取决于 NonStop 系统类型），使每个 NonStop 系统都由 Insight Remote Support Advanced 监控，并启用拨叫 Insight Remote Support Advanced/WEBES 的功能。

   - 如果是 NonStop BladeSystems，请添加：

     ```
     IR_Alert=YES
     Schema#NSK_DialoutConfiguration#Method#IrCalloutPathTest#OSMDisplayable
     = {"OSM_SC"}
     ```

     （Schema 参数必须在同一行，这样所使用的编辑方法就不会被截断。）

     ```
     EnableNDData=OFF
     ```

   - 如果是 NonStop NS 系列系统，请添加：

     ```
     IR_Alert=YES
     Schema#NSK_DialoutConfiguration#Method#IrCalloutPathTest#OSMDisplayable
     = {"OSM_SC"}
     ```

     （Schema 参数必须在同一行，这样所使用的编辑方法就不会被截断。）

     ```
     EnableNDData=OFF
     UseSSL=ON
     ```

   - 如果是 NonStop S 系列系统，请添加：

     ```
     IR_Alert=YES
     UseSSL=ON
     ```

   如果用于 Insight Remote Support Advanced 的 CMS 在专用的维护 LAN 之外，您必须在 OSMCONF 中为 OSM 指定堆栈参数，如下所述：

   ```
   stack = <TCPIP 过程名称>
   ```

   例如：

   ```
   stack = $ZTC00 stack = $ZTC01
   ```

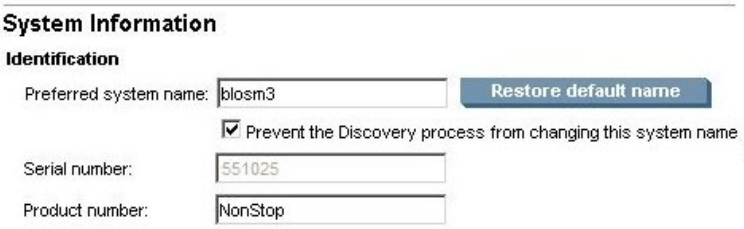
注释： 编辑 OSMCONF 文件后，必须重新启动下列 OSM 服务器过程（如果是在 NonStop 系统上运行），使更改生效：

- $ZZKRN.#OSM-CIMOM
- $ZZKRN.#OSM-APPSRVR
- $ZZKRN.#OSM-OEV

---

5. 使用所用版本的 HP SIM 联机帮助中所述的系统发现方法来发现 HP SIM 中的每个 NonStop 系统（而不是 CMS）。发现各个系统后，可通过 HP SIM 中的 **Edit System Properties** 页来输入下列 NonStop 权限值，为 Insight Remote Support Advanced 启用各个系统。您可以从每个 NonStop 系统主页上的 **Tools & Links** 选项卡访问该页（如下图所示）：

- 在 System Information > Identification 下：在 Product number 字段中输入 **`NonStop`**。



- 在 Contract and Warranty Information > Entitlement Information 下：
  - — System Country code：从下拉菜单中选择相应的国家/地区：
  - — Entitlement type：输入 **`System Handle`**
  - — Entitlement ID：输入 **`NSKSUPPORT`**

单击 **OK** 保存更改。

6. 对要由 Insight Remote Support Advanced 监控的每个 NonStop 系统重复执行步骤 3-5。
7. 完成后，每个 NonStop 系统都应该由 Insight Remote Support Advanced 监控。您可以使用 **Test Incident Report Delivery Paths** 操作（位于 OSM Service Connection 中的 System 对象下），在每个系统上测试此功能。此操作会触发定期事件报告。如果系统已经由 Insight Remote Support Advanced 监控，HP SIM 会在 Event 选项卡上显示事件，指出已报告 NonStop 系统事件。就 OSM 事件和警报而言：
   - 如果是 NonStop BladeSystems 和 NS 系列系统，始终会生成 OSM 事件 1103，显示 “Incident report delivery path not configured”，即使已成功传递 IR 也一样。您可以忽略此事件（如需详细信息，请参阅“已知问题”）。
   - 如果是 NonStop S 系列系统，OSM 会发出下列事件之一，指出尝试传递 IR 是成功还是失败：
     - — 事件 1102 (An Incident Report has been dialed out to the Support Center) – 至少在一个路径上成功传递 IR 时生成。如果第二个路径失败，会在 System 对象上生成警报，提供失败路径的详细信息。
     - — 事件 1103 (An Incident Report has failed to be delivered) – 两个路径上的 IR 传递都失败时生成。系统会在 System 对象上生成警报，提供失败路径的详细信息。

注释： 如果只有 NonStop S 系列系统（此时），为实现容错功能，您可以在多个 CMS 上安装和使用 Insight Remote Support Advanced。要使用此配置，请在其他的 CMS 上重复执行步骤 1-7。

如果您在用于管理 NonStop BladeSystems 或 NS 系列系统的多个 CMS 上安装和配置 Insight Remote Support Advanced，请确定只在一个 CMS 上的 HP SIM 中执行这些系统的发现过程，以避免重复拨出。

8.4 Insight Remote Support Advanced 迁移方案

本节说明从使用 OSM Notification Director 迁移到 Insight Remote Support Advanced 的四个方案。当指向上述四个方案时，在"NonStop 特定的任务"的步骤 3 中，执行与您现有控制台环境和配置相应的方案中所列的步骤。

注释： 必须配置 Insight Remote Support Advanced 或 OSM Notification Director（但不能同时配置）以监控 NonStop 系统。HP 不支持配置为同时支持 Insight Remote Support Advanced 和 OSM Notification Director 的 NonStop 系统。

此时，NonStop NS 系列系统和 NonStop BladeSystems 一次只能由一个 CMS 上的 Insight Remote Support Advanced 监控（请参阅"已知问题"）。

8.4.1 方案 1：使用 OSM ND 只监控单一 NSC 中的一个 Nonstop 系统

1. 依次选择 **开始→控制面板→管理工具→服务→service_name**，禁用下列服务。不仅要停止服务，还要将其"启动类型"更改为**已禁用**。
   - Remote Proxy Service
   - OSM Notification Director Monitor
2. 重命名下列可执行文件（位于`C:\OSM\bin`中），防止这些文件意外启动。例如，在".exe"后加上".txt"扩展名，使其不能再执行。
   - `NDMonSvr.exe`
   - `OsmNd32.exe`
3. （**可选**）要从控制台删除 OSM Notification Director 和 Remote Proxy Service 的开始菜单快捷方式，请从`C:\Documents and Settings\All Users\Start Menu\Programs\HP OSM`中删除下列文件夹：
   - `OSM Notification Director`
   - `Remote Proxy`
4. 返回到"NonStop 特定的任务"的步骤 4，以完成启用 Insight Remote Support Advanced 的过程。

8.4.2 方案 2：使用 OSM ND 只监控两个 NSC（主 NSC 和备份 NSC）中的一个 Nonstop 系统

1. 遵循方案 1下的步骤 1–3，以禁用并删除主 NSC 上的 OSM ND。
2. 遵循方案 1下的步骤 1–3，以禁用并删除备份 NSC 上的 OSM ND。
3. 返回到"NonStop 特定的任务"的步骤 4，以完成启用 Insight Remote Support Advanced 的过程。

8.4.3 方案 3：使用 OSM ND 监控单一 NSC 中的多个 Nonstop 系统

一次选择一个 Nonstop 系统，在该系统中执行这些 Insight Remote Support Advanced 迁移步骤：

1. 启动 OSM ND 并从 Systems 菜单中选择 **Configure \system_name**。

2. 登录。在 Preferences 选项卡的 Dial-out Definition 中，选择 **Not a Dial-out Point**，然后单击 **OK**
3. 返回到"NonStop 特定的任务"的步骤 4，以完成在每个 NonStop 系统上启用 Insight Remote Support Advanced 的过程。但是，请务必返回到方案 3 的过程，并对要迁移至 Insight Remote Support Advanced 的每个 NonStop 系统重复执行步骤 1-3。
4. 如果所有的 NonStop 系统都已迁移至 Insight Remote Support Advanced，请执行方案 1下的步骤 1–3 来禁用 OSM ND。但是，如果有些 NonStop 系统要继续由 ND 监控，请勿执行这些步骤，否则会禁用并删除 ND。

8.4.4 方案 4：使用 OSM ND 监控两个 NSC（主 NSC 和备份 NSC）中的多个 NonStop 系统

一次选择一个 Nonstop 系统，在该系统中执行这些 Insight Remote Support Advanced 迁移步骤。从备份 NSC 开始：

1. 启动 OSM ND 并从 Systems 菜单中选择 **Configure \system_name**。
2. 登录。在 Preferences 选项卡的 Dial-out Definition 中，选择 **Not a Dial-out Point**，然后单击 **OK**
3. 移至主 NSC 并重复执行上述步骤 1 和 2（在方案 4 中）。
4. 返回到"NonStop 特定的任务"的步骤 4，以完成在每个 NonStop 系统上启用 Insight Remote Support Advanced 的过程。但是，请务必返回到方案 4 的过程，并对要迁移至 Insight Remote Support Advanced 的每个 NonStop 系统重复执行步骤 1-4。
5. 在备份 NSC 上：如果由此控制台监控的所有 NonStop 系统都已迁移至 Insight Remote Support Advanced，请执行方案 1下的步骤 1-3 来禁用 OSM ND。但是，如果有些 NonStop 系统要继续由 ND 监控，请勿执行这些步骤，否则会禁用并删除 ND。
6. 在主 NSC 上：如果由此控制台监控的所有 NonStop 系统都已迁移至 Insight Remote Support Advanced，请执行方案 1下的步骤 1-3 来禁用 OSM ND。但是，如果有些 NonStop 系统要继续由 ND 监控，请勿执行这些步骤，否则会禁用并删除 ND。

8.5 已知问题

这些问题仅适用于 NonStop NS 系列系统与 NonStop BladeSystems，不适用于 NonStop S 系列系统：

- Insight Remote Support Advanced 目前不适用于这些系统的容错 CMS 配置。如果您在用于管理 NonStop BladeSystems 或 NS 系列系统的多个 CMS 上安装和配置 Insight Remote Support Advanced，请确定只在一个 CMS 上的 HP SIM 中执行这些系统的发现过程，以避免重复拨出。
- 始终会创建下列 OSM 子系统事件，即使事件报告已成功传递至 CMS 也一样。您可以忽略此事件，因为它代表 IR 路径的容错本质，这是当前版本中的一个已知限制：

  ```
  OSM 子系统事件 1103: An Incident Report has failed to be delivered。
  原因：尚未配置事件报告传递路径。
  ```

  要了解事件报告的传递状态，请查看 HP SIM 内的 Events 选项卡。

注释： 升级至 WEBES 5.6 后会提供更多信息，指出尝试传递 IR 是成功还是失败。使用 WEBES 5.6 时，不论 IR 是否已传递，您都会收到该事件（如上所述）。但是，您也会收到下列事件之一，指出尝试传递 IR 是成功还是失败：

```
1102. An Incident Report has been dialed out to the Support Center for IR id#.
```

或

```
1103. An Incident Report has failed to be delivered.IR id#
```

（这种情况下，事件 1103 可能会列出除 “Incident report delivery path not configured” 以外的其他原因，或者不列出任何原因。）

如果您收到事件 1102 以及最初的 1103 事件，则表示 IR 已成功传递。如果您没有收到事件 1102，而是再次收到 1103 事件，则表示 IR 未成功传递。

8.6 回退

如果您希望使用 OSM Notification Director 从 Insight Remote Support Advanced 进行回退，请根据需要执行下列任务（具体取决于您在迁移至 Insight Remote Support Advanced 期间是删除了 ND 还是只将其禁用）：

- 如果您不会再使用 HP SIM，请停止 HP Systems Insight Manager 服务（**开始→控制面板→管理工具→服务**）；如果您要继续使用 HP SIM 来监控其他系统，则只需从 HP SIM 删除个别 NonStop 系统。
- 删除在执行 OSMCONF 配置任务期间插入的 OSMCONF 标志，然后重新启动 OSM 服务器过程，使这些更改生效。
- 根据需要撤消所执行的步骤，以便在 Insight Remote Support Advanced 迁移的方案 1期间，禁用 OSM Notification Director 和 Remote Proxy Service。如果您已删除 OSM Notification Director 和 Remote Proxy Service 的开始菜单快捷方式，则需要重新安装这些产品。若未删除，则只需将文件重命名为其原始名称，并重新启动服务即可。
- 如果已从 OSM Notification Director 中删除个别系统（如方案 3和方案 4中所要求），请在 OSM Notification Director 内重新配置各个 NonStop 系统。

9 Insight Remote Support 对 HP-UX 受管系统的要求

9.1 概述

本文说明了 HP-UX 受管系统要符合 Insight Remote Support Advanced 的要求而必须具备的条件。在尝试将 HP Insight Remote Support 与 HP-UX 受管系统一起使用之前，请通读本文。

1. **验证硬件支持**

   由于产品支持可能会更改主要软件版本的范围，请务必检查《A.05.40 Insight Remote Support Advanced Release Notes》，确认硬件目前仍受支持。

2. **删除发生冲突的软件**

   如果 ISEE 或 Insight Remote Support 完全不支持此 HP-UX 受管系统，请跳过此步骤。如果正在将现有的 Instant Support Enterprise Edition (ISEE) 客户端从 ISEE 迁移至 Insight Remote Support，则必须删除以下软件应用程序：

   - 所有旧版 WEBES
   - 所有版本的 HP Instant Support Enterprise Edition (ISEE)

   如果 Insight Remote Support（以前称为 RSP）A.05.05 版支持此 HP-UX 受管系统，则必须删除 A.05.05 ACC 组件（如果已安装）。

   有关删除这些组件（ISEE、WEBES 或 A.05.05 ACC）的说明和注意事项，请参阅“删除发生冲突的软件”。

3. **确认符合操作系统、软件及补丁要求。**

   欲详细了解 HP-UX 操作系统要求，请参阅“满足 HP-UX 操作系统、软件及补丁要求”。

4. **建立通信并配置协议**

   System Fault Manager (SFM) 是在 HP-UX 所有支持版本上进行 HP Insight Remote Support 通信所必需的。“满足 HP-UX 操作系统、软件及补丁要求” 会对 SFM 许多补丁先决条件进行详细说明。如果系统已符合本节指出的最低要求，则不需要删除或重新安装那些组件。如果系统不符合最低要求，请依照 “深入了解 WBEM 和 SFM 及 Insight Remote Support” 中的指示进行升级。

注释： 您可能已熟悉不同 SFM 产品提供的各种 SFM 提供程序。Insight Remote Support 仅需要 “满足 HP-UX 操作系统、软件及补丁要求” 中指定的标准 SFM 包中的提供程序。

5. **安装和配置 Advanced Configuration Collector**

   Advanced Configuration Collector (ACC) 组件用于生成主动式服务配置集合并发送给 HP。如果您没有关键业务支持合同，则不需要安装或配置 ACC 组件。如果您有权享受关键业务支持，请按照“删除 B.05.05 Advanced Configuration Collector (ACC) 软件包”中的说明进行操作。

6. **完成 CMS 配置**

   这个简短文档仅说明 HP-UX 受管系统的要求。当受管系统确实符合所有必要条件后，就需要配置 CMS 来与受管系统进行通信。《HP Insight Remote Support Advanced CMS 配置与使用指南》 中会说明这些过程。

重要信息： 当您在中央管理服务器 (CMS) 上配置 Insight Remote Support Advanced 时，必须在 HP SIM 界面中为 HP-UX 受管系统配置 WBEM 凭据。《HP Insight Remote Support Advanced CMS 配置与使用指南》 的第二章详细说明此过程。请将这些凭据记下来，因为稍后将需要提供这些凭据。

9.2 删除发生冲突的软件

仅当已在 HP-UX 受管系统上安装了任意版本的 HP ISEE 客户端或 WEBES 时，才需要执行这些步骤

注意： 如果打算使用 ISEE 迁移工具将系统配置数据迁移至 CMS，那么在完成《HP Insight Remote Support Advanced CMS 配置与使用指南》 中规定的迁移步骤之前，**请不要**删除 ISEE。

9.2.1 从 HP-UX 受管系统中删除 HP ISEE

仅当已在受管系统上安装了 HP Instant Support Enterprise Edition 时，才需要执行这些步骤。如果尚未在受管系统上安装 ISEE，可以跳过本节。

重要信息： Instant Support Enterprise Edition (ISEE) A.03.95 及之前版本与 Insight Remote Support Advanced 不是相同的应用程序，不应安装在任何受管系统上。

要删除 ISEE，请完成下列步骤：

1. 以 **`root`** 身份（系统管理权限）登录受监控的系统。
2. 在每个受管系统上运行以下命令：

   ```
   /usr/sbin/swremove ISEEPlatform
   ```

   如果 `swremove` 过程执行成功，则会显示已移除软件的确认消息。请检查日志文件，确认没有任何错误。

   如果 `swremove` 过程未成功完成，请参阅生成的日志文件。其中可能指出导致失败的 ISEE 平台依赖性。VAEH、Availability Measure 或 CCMon 等组件都是可选的业务支持软件组件，但必须先删除这些组件，ISEE 平台才能完成卸载。

   请为日志文件中列出的每一个业务支持软件组件运行 `swremove`。有关这些组件的详细信息，请参阅 A.03.95.500 的《**HP Instant Support Enterprise Edition Client 安装和升级指南**》中的**业务支持软件**组件章节，地址为：http://sstwww.fc.hp.com/ISEE/client/A.03.95.500client.pdf

9.2.2 从 HP-UX 受管系统中删除 WEBES

运行交互式 `webes_install_update utility`，选择删除所有 WEBES 的选项，并按照出现的提示操作。

9.2.3 删除 B.05.05 Advanced Configuration Collector (ACC) 软件包

在安装 A.05.40 版 ACC 软件包之前删除 B.05.05 版。要删除此包，请在每一个 HP-UX 受管系统上运行以下命令：

```
swremove RS-ACC
```

在 CMS 上，使用 HP SIM 发现 HP-UX 受管系统，且在 CMS 上安装 WEBES **之前**，请按照第 4 章所述来配置系统信息。根据 HP SIM 的具体配置，可能会自动执行发现过程。

9.3 满足 HP-UX 操作系统、软件及补丁要求

请参阅下表，确认 HP-UX 受管系统已正确配置为接受 Insight Remote Support。

9.3.1 HP-UX 11.11 的软件和补丁要求

重要信息： 虽然并非 HP-UX 11.11 必需，但还是强烈建议使用

`GOLDBASE11i - B.11.11.0612.459 Base Patches for HP-UX (December 2006)`。

安装 GOLDBASE11i 可满足所有系统补丁要求，也能为客户提供稳定的支持环境。下表列出了**最低**要求的补丁（未安装 GOLDBASE11i 时需要）。

注释： 有关下表的注意事项

- 操作环境 (OE) 光盘中包含 WBEM Services、Online Diagnostics、SysMgmtWeb 及 HP SIM，在 SFM 安装期间可选择安装。Insight Remote Support 不支持 HP-UX 上的 HP SIM。
- 列出的软件版本是最低的支持要求。除非另外注明，否则较新的版本都可兼容。
- SysMgmtWeb 中捆绑的 System Management Homepage (SMH) 为可选项目。但是，如果没有安装，则无法访问 Event Viewer (EvWEB) 用户界面。
- 如果存在旧版 SFM（A.01.00.01 或 A.03.00.xx），必须先将其卸载，才能安装 SFM A.04.00.04 版。
- 此表中项目的顺序取决于在缺少且需要升级或安装项目时应该遵循的安装顺序。

表 9-1 HP-UX 11.11 必需的软件组件

需要的软件	需要的版本
HP-UX 操作环境	11i V1
如何下载或获取软件： http://h20338.www2.hp.com/hpux11i/cache/324916-0-0-0-121.html	
操作系统补丁要求	支持任意 11.11 OE，但 2003 年 6 月以前的所有 11.11 OE 还必须安装补丁包 B.11.11.0306.1。
如何下载 HP-UX 的补丁： 转至 http://itrc.hp.com/service/patch/hpuxPatchBundlePage.do?bundleId=BUNDLE11i:B.11.11.0306.1	
OpenSSL	**A.00.09.07i.012 产品包（2006 年 12 月）或更高版本**
如何下载或获取软件： • 自 2006 年 12 月起通过应用程序软件光盘提供 • 或者，也可以从以下 HP 软件库位置获取最新版本： https://h20392.www2.hp.com/portal/swdepot/try.do?productNumber=OPENSSL11I	
WBEMServices（WBEM Services 核心产品）	**A.02.05 产品包（2006 年 12 月）**
如何下载或获取软件： • 自 2006 年 12 月起通过应用程序软件光盘提供 • 或者，也可以从以下 HP 软件库位置获取最新版本： https://h20392.www2.hp.com/portal/swdepot/try.do?productNumber=WBEMSvcs	
Online Diagnostics	**B.11.11.18.05 产品包（2006 年 12 月）**

表 9-1 HP-UX 11.11 必需的软件组件 (续)

需要的软件	需要的版本
如何下载或获取软件： • 通过 HWE0612 光盘提供 • 或者，也可以从以下 HP 软件库位置获取最新版本： https://h20392.www2.hp.com/portal/swdepot/try.do?productNumber=B6191AAE	
System Management Web（推荐用于事件监控，收集配置数据时也需要此组件）	**A2.2.5 产品包（2006 年 12 月）**
System Management Web 为可选组件，但可让您充分利用系统故障管理的 EVWEB GUI 组件，以查看 SFM 在主机上所处理的事件。 如果系统上只有 SysMgmtHomepage 2.2.6.2 版，则还必须应用以下补丁： 如果是 HP-UX 11iv1 (11.11) OE，则必须应用补丁 `PHSS_36869` 可从位于以下 URL 的 IT 资源中心获取该补丁： ftp://ftp.itrc.hp.com/hp-ux_patches/s700_800/11.X/'patch number' 这是“sharfile”，必须以脚本的形式运行来解压缩 (“sh PHSS_36869)。请务必查看随附的文本文件 (`PHSS_36869.text`) 中的补丁安装说明	
如何下载或获取软件： • 自 2007 年 12 月起通过应用程序软件光盘提供 • 或者，也可以从以下 HP 软件库位置获取最新版本： https://h20392.www2.hp.com/portal/swdepot/try.do?productNumber=SysMgmtWeb	
hpuxwsApache	**A.2.0.49**
只有 Advanced Configuration Collector 组件（作为远程支持的 HP Remote Support Configuration Collection 项目的代理程序）才一定需要 hpuxwsApache。对远程支持**监控**来说它不是必需的组件。	
安装 `hpuxwsAPACHE` 产品时，推荐安装整个 `hpuxwsApache` 包。对于已下载的软件库，则不需要 `hpuxTomcat` 和 `hpuxWebmin` 包。	
如何下载或获取软件： • 通过 11.11 Jun04 OE/AR 或更高版本的光盘提供 • 或者，也可以从以下 HP 软件库位置获取最新版本： https://h20392.www2.hp.com/portal/swdepot/try.do?productNumber=HPUXWSATW218	
系统故障管理 (SFM)	**A.04.00.04 产品包（2006 年 12 月）**
SFM **必须**是从这份列表中安装或升级的最后一个必要软件组件。	
如何下载或获取软件： • 通过 HWE0612 光盘提供 • 或者，也可以从以下 HP 软件库位置获取最新版本： https://h20392.www2.hp.com/portal/swdepot/try.do?productNumber=SysFaultMgmt	

9.3.2 HP-UX 11.23 的软件和补丁要求

重要信息： 虽然并非 HP-UX 11.23 必需，但还是强烈建议使用

`QPKBASE B.11.23.0712.070 Base Quality Pack Bundle for HP-UX 11i v2 (December 2007)`。

安装 QPKBASE B.11.23.0712.070 可满足所有系统补丁要求，也能为客户提供稳定的支持环境。下表列出了**最低**要求的补丁（未安装 QPKBASE B.11.23.0712.070 时需要）。

重要信息： 在 CMS 上，使用 HP SIM 发现 HP-UX 受管系统，并在安装 WEBES **之前**，按照第 4 章所述来配置系统信息。根据 HP SIM 的具体配置，可能会自动执行发现过程。

注释： **有关下表的注意事项**

- 操作环境 (OE) 光盘中包含 WBEM Services、Online Diagnostics、SysMgmtWeb 及 HP SIM，在 SFM 安装期间可选择安装。Insight Remote Support 不支持 HP-UX 上的 HP SIM。
- 列出的软件版本是最低的支持要求。除非另外注明，否则较新的版本都可兼容。
- SysMgmtWeb 中捆绑的 System Management Homepage (SMH) 为可选项目。但是，如果没有安装，则无法访问 Event Viewer (EvWEB) 用户界面。
- 如果存在旧版 SFM（A.01.00.01 或 A.03.00.xx），必须先将其卸载，才能安装 SFM A.04.00.04 版。
- 此表中项目的顺序取决于在缺少且需要升级或安装项目时应该遵循的安装顺序。

注释： 对于 HP-UX 端点系统上的 ELMC 软件没有要求，因为在 HP-UX 系统上，WEBES 直接与 CIM Object Manager (CIMOM) 进行通信。另外还必须删除 WCCProxy，但在卸载 WEBES 时会自动将它一并卸载。

重要信息： 在 CMS 上，使用 HP SIM 发现 HP-UX 受管系统，并在安装 WEBES **之前**，按照第 4 章所述来配置系统信息。根据 HP SIM 的具体配置，可能会自动执行发现过程。

表 9-2 HP-UX 11.23 必需的软件组件

需要的软件	需要的版本
HP-UX 操作环境	• 2004 年 9 月 11i v2 OE（最低 OE 版本） • 2005 年 5 月 11i V2 OE（启用 vPars 时需要）。
如何下载或获取软件： http://h20338.www2.hp.com/hpux11i/cache/324923-0-0-0-121.html	
操作系统补丁要求 **注释：** HP-UX 11i v2 的这六个额外补丁不是 Bundle11i 的一部分，必须另外安装。	BUNDLE 11i 补丁包 B.11.23.0409.3（2004 年 9 月）： • PHKL_36288 - 11.23 累加 diag2 驱动程序及 vPars 启用（用来取代 PHKL_32653），需要重新启动 • PHKL_34795 - 11.23 累加 IPMI 驱动程序补丁，需要重新启动 • PHSS_37552 1.0 Aries 累加补丁 • PHSS_37947 1.0 链接程序 + fdp 累加补丁 • PHSS_35055 - aC++ Runtime (IA：A.06.10，PA：A.03.71) • PHSS_36345 - 11.23 Integrity Unwind Library
如何下载或获取软件： 转至 www.hp.com，选择 **Support and Drivers** 选项卡。然后，单击网页右边的 **Download patches for HP-UX, Open VMS, Tru64 and MPE** 按钮。这时会连结到 ITRC，以便搜索适当的补丁。	

表 9-2 HP-UX 11.23 必需的软件组件 (续)

需要的软件	需要的版本
OpenSSL	**A.00.09.07i.012 产品包（2006 年 12 月）或更高版本**
如何下载或获取软件： • 自 2006 年 12 月起通过应用程序软件光盘提供 • 或者，也可以从以下 HP 软件库位置获取最新版本： https://h20392.www2.hp.com/portal/swdepot/try.do?productNumber=OPENSSL11I	
Online Diagnostics	**B.11.23.10.05 产品包（2007 年 12 月）**
如何下载或获取软件： • 通过 HWE0706 光盘提供 • 或者，也可以从以下 HP 软件库位置获取最新版本： https://h20392.www2.hp.com/portal/swdepot/try.do?productNumber=B6191AAE	
WBEMServices（WBEM Services 核心产品）	**A.02.05.08 产品包（2007 年 12 月）**
如何下载或获取软件： • 自 2007 年 12 月起通过应用程序软件光盘提供 • 或者，也可以从以下 HP 软件库位置获取最新版本： https://h20392.www2.hp.com/portal/swdepot/try.do?productNumber=WBEMSvcs	
System Management Web（推荐用于事件监控，收集配置数据时也需要此组件）	**A.2.2.7 产品包（2007 年 12 月）**
推荐安装 System Management Web，以充分利用系统故障管理的 EVWEB GUI 组件，以查看 SFM 在主机上所处理的事件。 如果系统上只有 SysMgmtHomepage 2.2.6.2 版，则还必须应用以下补丁： 如果是 HP-UX 11iv2 (11.23) OE，则必须应用补丁 `PHSS_36870` 可从位于以下 URL 的 IT 资源中心获取该补丁： ftp://ftp.itrc.hp.com/hp-ux_patches/s700_800/11.X/'patch number' 这是“sharfile”，必须以脚本的形式运行来解压缩 (“sh PHSS_36870)。请务必查看随附的文本文件 (`PHSS_36870.text`) 中的补丁安装说明	
如何下载或获取软件： • 自 2007 年 9 月起通过应用程序软件光盘提供 • 或者，也可以从以下 HP 软件库位置获取最新版本： https://h20392.www2.hp.com/portal/swdepot/try.do?productNumber=SysMgmtWeb	
hpuxwsApache	**A.2.0.49**
只有 Advanced Configuration Collector 组件（作为远程支持的 HP Remote Support Configuration Collection 项目的代理程序）才一定需要 hpuxwsApache。对远程支持**监控**来说它不是必需的组件。	
安装 `hpuxwsAPACHE` 产品时，推荐安装整个 `hpuxwsApache` 包。对于已下载的软件库，则不需要 `hpuxTomcat` 和 `hpuxWebmin` 包。	
如何下载或获取软件： • 通过 11.23 Sep04 OE/AR 或更高版本的光盘提供 • 或者，也可以从以下 HP 软件库位置获取最新版本： https://h20392.www2.hp.com/portal/swdepot/try.do?productNumber=HPUXWSATW218	

表 9-2 HP-UX 11.23 必需的软件组件 (续)

需要的软件	需要的版本
HPUXBaseAux.SysMgmtBase 或 **SysMgmtBASE.SysMgmtBase**	**A.2.0.49**
只有 Advanced Configuration Collector 组件（作为远程支持的 HP Remote Support Configuration Collection 项目的代理程序）才一定需要此组件。对远程支持**监控**来说它不是必需的组件。	
从 `HPUXBaseAux` 包中安装产品 `SysMgmtBase` 时，不需要安装整个包。	
如何下载或获取软件： • 11.23 Sep06 OE 或更高版本（例如 `HPUXBaseAux.SysMgmtBase`），或者 11.23 Sep06 AR 或更高版本（例如 `SysMgmtBASE.SysMgmtBase`） • 或者，也可以从以下 HP 软件库位置获取最新版本： https://h20392.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=SysMgmtBASE	
系统故障管理 (SFM)	**B.05.00.05 产品包（2007 年 12 月）**
SFM **必须**是从这份列表中安装或升级的最后一个必要软件组件。	
如何下载或获取软件： • 通过 HWE0712 光盘提供 • 或者，也可以从以下 HP 软件库位置获取最新版本： https://h20392.www2.hp.com/portal/swdepot/try.do?productNumber=SysFaultMgmt	

9.3.3 HP-UX 11.31 的软件和补丁要求

注释：　有关下表中的注意事项

- 操作环境 (OE) 光盘中包含 WBEM Services、Online Diagnostics、SysMgmtWeb 及 HP SIM，在 SFM 安装期间可选择安装。Insight Remote Support 不支持 HP-UX 上的 HP SIM。
- 列出的软件版本是最低的支持要求。除非另外注明，否则较新的版本都可兼容。
- SysMgmtWeb 中捆绑的 System Management Homepage (SMH) 为可选项目。但是，如果没有安装，则无法访问 Event Viewer (EvWEB) 用户界面。
- 如果存在旧版 SFM（A.01.00.01 或 A.03.00.xx），必须先将其卸载，才能安装 SFM A.04.00.04 版。
- 此表中项目的顺序取决于在缺少且需要升级或安装项目时应该遵循的安装顺序。

表 9-3 HP-UX 11.31 必需的软件组件

需要的软件	需要的版本
HP-UX 操作环境	HP-UX 11i V3
如何下载或获取软件： http://h20338.www2.hp.com/hpux11i/cache/458092-0-0-0-121.html	
操作系统补丁要求	• EVM-Event Mgr B.11.31 • Baseboard Management Controller (BMC) 固件 70.59 版或更高版本 • Sys MgmtBase B.00.02.03
如何下载或获取软件： 转至 www.hp.com，选择 **Support and Drivers** 选项卡。然后，单击网页右边的 **Download patches for HP-UX, Open VMS, Tru64 and MPE** 按钮。这时会连结到 ITRC，以便搜索适当的补丁。	

表 9-3 HP-UX 11.31 必需的软件组件 (续)

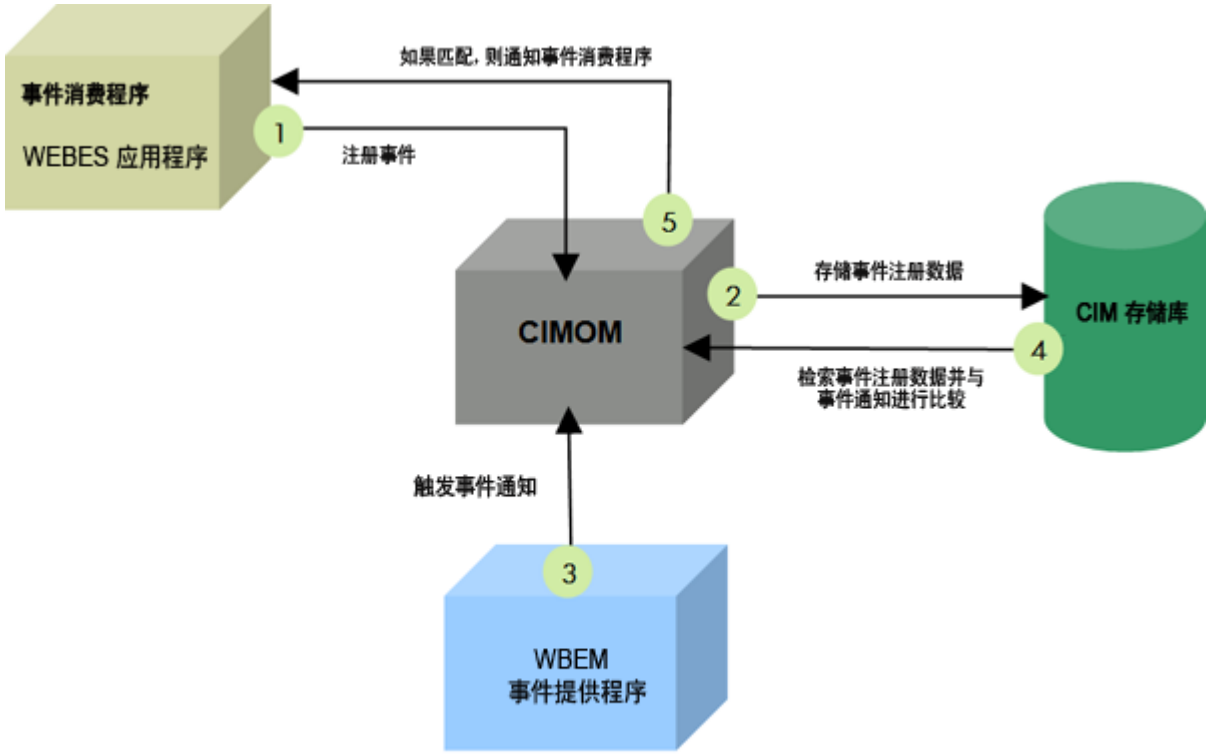
需要的软件	需要的版本
OpenSSL	**A.00.09.07e.013 或更高版本**
如何下载或获取软件： • 自 2007 年 9 月起通过应用程序软件光盘提供 • 或者，也可以从以下 HP 软件库位置获取最新版本： https://h20392.www2.hp.com/portal/swdepot/try.do?productNumber=OPENSSL11I	
HP-UX 诊断和支持工具；包括 STM A.49.10 版或更高版本及 EMS A.04.20 版或更高版本	**B.11.31.01.yy**
如何下载或获取软件： • 通过 HP-UX 11i v3 - 2007 年 2 月光盘提供 • 或者，也可以从以下 HP 软件库位置获取最新版本： https://h20392.www2.hp.com/portal/swdepot/try.do?productNumber=B6191AAE	
WBEMServices（WBEM Services 核心产品）	**A.02.05 或更高版本**
如何下载或获取软件： • 自 2007 年 9 月起通过应用程序软件光盘提供 • 或者，也可以从以下 HP 软件库位置获取最新版本： https://h20392.www2.hp.com/portal/swdepot/try.do?productNumber=WBEMSvcs	
System Management Web（推荐的，但非必需的）	**A.2.2.4**
推荐安装 System Management Web，以充分利用系统故障管理的 EVWEB GUI 组件，以查看 SFM 在主机上所处理的事件。 如果系统上只有 SysMgmtHomepage 2.2.6.2 版，则还必须应用以下补丁： 如果是 HP-UX 11iv3 (11.31) OE，则必须应用补丁 `PHSS_36871` 可从位于以下 URL 的 IT 资源中心获取该补丁： ftp://ftp.itrc.hp.com/hp-ux_patches/s700_800/11.X/'patch number' 这是“sharfile”，必须以脚本的形式运行来解压缩 (“sh PHSS_36871)。请务必查看随附的文本文件 (`PHSS_36871.text`) 中的补丁安装说明	
如何下载或获取软件： • 自 2007 年 9 月起通过应用程序软件光盘提供 • 或者，也可以从以下 HP 软件库位置获取最新版本： https://h20392.www2.hp.com/portal/swdepot/try.do?productNumber=SysMgmtWeb	
系统故障管理	**C.01.00.29.yy**
SFM **必须**是从这份列表中安装或升级的最后一个必要软件组件。	
如何下载或获取软件： 也可以从以下 HP 软件库位置获取最新版本： https://h20392.www2.hp.com/portal/swdepot/try.do?productNumber=SysFaultMgmt	

9.4 深入了解 WBEM 和 SFM 及 Insight Remote Support

Web-Based Enterprise Management (WBEM) 是一项业界倡议，用来将不同平台间的管理信息进行标准化。系统故障管理（SysFaultMgmt 或 SFM）是实施 WBEM 标准的 HP-UX 故障管理解决方案。SysFaultMgmt 与其他易于管理的应用程序（如 HP SIM 和 HP SMH）以及其他任何基于 WBEM 的客户端（如 WEBES）集成在一起。SFM 要求 HP-UX 必须安装 **WBEM Services for HP-UX** 和其他软件。

WBEM 中的事件称为指示。客户端系统（例如 CMS）必须先订阅事件，才能向客户端系统报告指示。事件订阅可以让受管系统的 **Common Information Model Object Manager** (CIMOM) 知道客户端 (CMS) 想要接收来自该受管系统（端点）的指示。当 CIMOM 收到来自指示提供程序的指示时，它会将指示发送到先前已订阅要接收这些指示的客户端。

CMS 上的 WEBES 会订阅这些指示。完成订阅后，指示发生时就会传递到 CMS 上的 WEBES。下图简要概况了事件（指示）订阅和传递过程。



事件订阅与交付

有关 SFM 的详细信息，请参阅 《HP-UX WBEM Providers 的 OE/AR 软件库信息》中关于这些提供程序的概述，地址为 http://h10018.www1.hp.com/wwsolutions/misc/hpsim-helpfiles/OEARInformation.pdf。

9.5 确认系统故障管理组件可以正常运行

要确认系统故障管理组件 (SFM) 可以在 HP-UX 受管系统上正常运行，请执行以下步骤：

1. 运行以下命令，检查是否已安装 **HP WBEM Services for HP-UX** 组件：

   ```
   # swlist | grep -i WBEM
   ```

   输出内容如下所示：

```
# swlist | grep -i WBEM
  LVMProvider              R11.23.008      CIM/WBEM Provider for LVM
  ProviderDefault          B.11.23.0706    Select WBEM Providers
  VMProvider               A.03.00.76      WBEM Provider for Integrity VM
```

2. 要列出已注册的CIM提供程序及其当前状态，以确保它们全部都已启用，请运行以下命令：

   ```
   # cimprovider -l -s
   ```

   这时会显示一个较长的提供程序模块列表，以便检查它们是否全部都已启用。

3. 运行以下命令，检查是否已安装 **OnlineDiag**，并确定版本为 B.11.11.16xx 或更高版本。

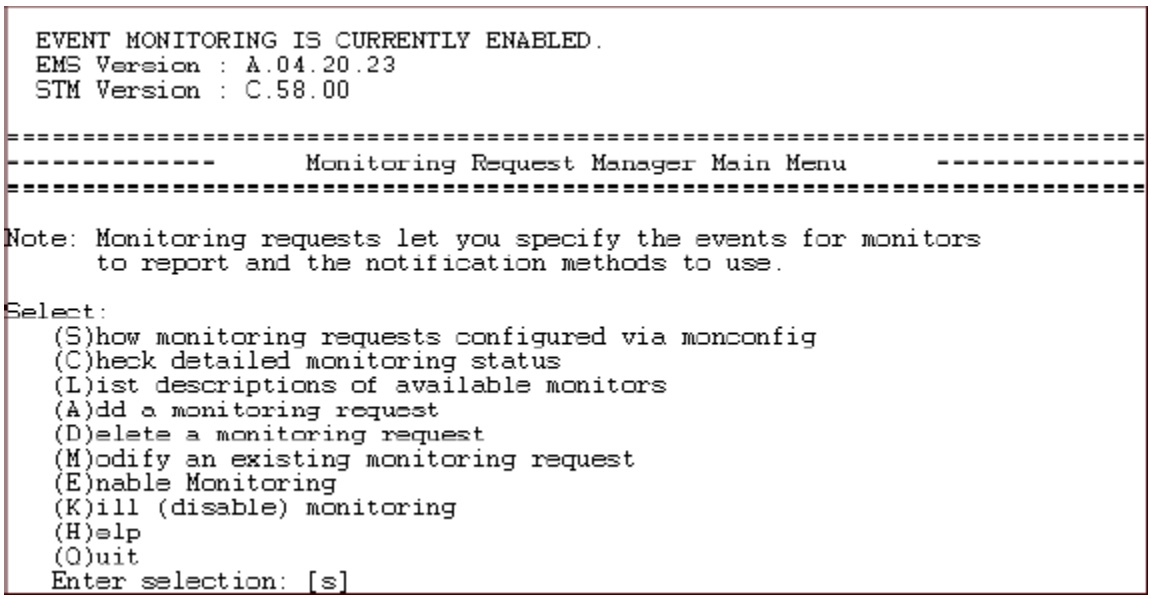
   ```
   # swlist | grep -i OnlineDiag
   ```

   输出内容如下所示：

4. 运行以下命令，检查 OnlineDiag 是否报告 **Event Monitoring is Currently Enabled**，且 EMS 版本为 A.04.20 或更高版本，STM 为 A.49.10 或更高版本：

   ```
   # /etc/opt/resmon/lbin/monconfig
   ```

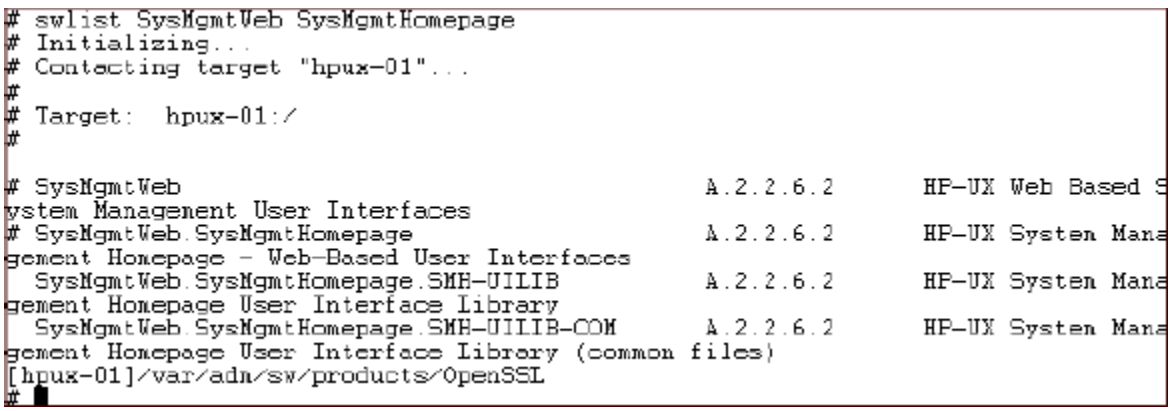
   输出内容如下所示：



5. 选择'Q'退出 **EMS Monitoring Request Manager Main Menu**。
6. 可选择运行以下命令，确定（可选用，但推荐）System Management Homepage (SMH) 组件至少为 A.2.2.6.2 版：

   ```
   # swlist SysMgmtWeb SysMgmtHomepage
   ```

   输出内容如下所示：



9.6 在 CMS 上配置 WEBES 以支持 HP-UX 系统上的 WBEM 指示

完成以下步骤，将 WEBES 配置为接收 WBEM 通信：

1. 确认 HP-UX 系统已安装所有必需的软件（如上所列）。
2. 确定中央管理服务器 (CMS) 已安装 WEBES，且正在 Insight Remote Support Advanced A.05.40 环境中运行。
3. WEBES 会根据 HP SIM 所发现的信息，自动为 HP-UX 受管系统创建 **WBEM 服务器**类型的受管实体。
4. WEBES 从 HP SIM 获取与受管系统上的 HP-UX CIMOM 进行通信时所需的信息，并将这些数据存储在受管实体中。当 WEBES 从 HP SIM 收到 WBEM 用户名和密码后，便会向 HP-UX 服务器订阅指示。

要将 HP-UX 系统与 WBEM 一起添加到 HP SIM：

对所有的 HP SIM 安装来说，此过程都一样，都是使用 Internet Explorer 或 Mozilla 连接到 HP SIM。

1. 通过浏览器登录 HP SIM。您必须具有系统管理权限才能添加系统。
2. 将 WBEM 凭据添加至全局协议设置。选择 **Options→Security→Global Protocol Settings**，在 WBEM 设置部分下添加 root/密码凭据。

注释： HP SIM 会请求对每一个 HP-UX 受管系统，可将 root/密码添加到 WBEM 通信协议登录，但 WBEM 通信也可以使用无权限的帐户。

要在 HP-UX 受管系统上设置适当的无权限帐户，请执行以下步骤：

1. 创建用户或使用现有的无权限用户。指定的用户名必须代表本地主机上有效的 HP-UX 用户。在本例中，将创建一个名为**sam**的用户，将该用户分配到用户组，然后设置用户密码：

   ```
   #useradd -g users sam
   #passwd sam（出现提示时，提供密码并确认）
   ```

   这是在 HP-SIM 中要针对此受管系统的 WBEM 通信而提供的用户和密码。

2. 查看当前的 CIM 配置，如下所示：

   ```
   #cimconfig -l -p
   ```

   输出示例：

   ```
   sslClientVerificationMode=disabled
   enableSubscriptionsForNonprivilegedUsers=false
   shutdownTimeout=30
   authorizedUserGroups=
   enableRemotePrivilegedUserAccess=false
   enableHttpsConnection=true
   enableHttpConnection=true
   ```

3. 根据以上的输出，在 CIM 计划配置中确定/设置以下变量：

   ```
   #cimconfig -s enableSubscriptionsForNonprivilegedUsers=true -p
   #cimconfig -s enableNamespaceAuthorization=true -p
   ```

4. 停止后启动 CIM 服务器，以在 CIM 当前配置中更改配置

   ```
   #cimserver -s
   #cimserver
   ```

5. 确认 CIM 当前配置中的设置：

   ```
   #cimconfig -l -c
   ```

   输出示例：

   ```
   sslClientVerificationMode=disabled
   enableSubscriptionsForNonprivilegedUsers=true
   shutdownTimeout=30
   authorizedUserGroups=
   enableRemoteprivilegedUserAccess=true
   enableHttpsConnection=true
   enableNamespaceAuthroization=true
   enablehttpConnection=false
   ```

6. 将用户 sam 的读取和写入授权添加到每一个名称空间，包括 root/cimv2、root/PG_InterOp 及 root/PG_Internal：

   ```
   #cimauth -a -u sam -n root/cimv2 -R -W
   #cimauth -a -u sam -n root/PG_InterOp -R -W
   #cimauth -a -u sam -n root/PG_Internal -R -W
   ```

```
#cimauth -a -u sam -n root/cimv2/npar -R -W
#cimauth -a -u sam -n root/cimv2/vpar -R -W
```

7. 确认用户的授权：

   输出示例：

```
sam, root/PG_InterOp, "rw"
sam, root/PG_Internal, "rw"
sam, root/cimv2, "rw"
```

---

3. 发现系统。选择 **Options→Discovery**，再选择 **Manual Discovery**。
4. 添加系统名称（最好是标准 DNS 名称）。
5. （可选）确认 HP SIM 已正确发现系统。一种简单的方法是在搜索面板中输入系统的名称，然后单击Search。搜索完成后，选择系统，然后从菜单中选择Properties（选择Tools→System Information→Properties），然后单击 **Run Now**。产生的页包含只通过 WBEM 检索的数据。
6. 在 HP-SIM 系统页面中配置受管系统时，请确认 Identification 选项卡部分包含系统序列号和产品编号的值。如果这些字段中没有填入值，请单击页面顶部的 **Tools & Links** 选项卡，然后选择并打开 **Edit System Properties** 链接，接着在 Contract and Warranty Information 部分、Entitlement Information 子部分及 Customer Entered Serial Number 和 Customer Entered Product Number 字段中输入这些值。选择 **OK**，完成此更新。

   要确定 HP-UX 受管系统的序列号和产品号码，可以访问服务器的 MP，选择 Command Menu，然后使用 ID 命令（如果是移动服务器）或 PS 命令（如果是非移动服务器），以显示此信息。服务器前方面板的系统识别外拉选项卡上也印有此信息。

7. 订阅 WBEM 事件。从 All Systems 集合中，对于您要从中检索指示的系统，勾选每个系统左边的复选框。选择 Options→Events→Subscribe to WBEM events，然后单击 **Run Now**。任务随即开始执行且应该会顺利完成，没有任何错误。
8. 发送测试指示：您可以在受管系统上生成测试事件，以确认一切都已正确设置。在受管系统上执行以下命令：`# etc/opt/resmon/lbin/send_test_event disk_em`
9. 要确认 HP SIM 已收到事件，您必须立即访问 HP SIM GUI。通过浏览器登入 HP SIM 来查看 WBEM 指示。在 Systems and Events 面板中选择 All Events。Events→Event Type 之下有一个信息事件，称为 HP-UX EMS Disk Event。单击此事件类型以查看详细信息。
10. 在 HP-UX 服务器上发出测试事件来测试安装，并确定 WEBES 已收到并显示这些事件。

有关SysFaultMgmt的详细信息，包括在HP-UX上定义WBEM用户/密码帐户并发出测试事件，请参考以下文档：

- 《HPUX System Fault Management Administration Guide》 (http://docs.hp.com/en/diag/sfm/5992-1318.pdf)
- 《EVA CommandView Installation Guide》 (http://h20000.www2.hp.com/bc/docs/support/SupportManual/c01080985/c01080985.pdf)

9.7 HP-UX 系统的 Firewall/DMZ 端口要求

表 9-4 HP-UX 系统的 Firewall/DMZ 端口要求

服务	协议	来源 IP	目标 IP	目标端口
非 SNMP 问题讨论区	http	McData/HAFM 交换机 DecEvent	CMS	2069
SNMP 设陷传递	SNMP	受管系统	CMS	162
HP-UX 事件监控				

表 **9-4 HP-UX** 系统的 **Firewall/DMZ** 端口要求 (续)

服务	协议	来源 IP	目标 IP	目标端口
WBEM 事件接收器	http/https	受管系统	CMS	50004
HP SIM WBEM 指示设置	https	受管系统	CMS	5989
HP-SIM GUI	https	任意浏览器	CMS	50000
Remote Support Configuration Collector				
存储集合 - SSH	TCP	CMS	受管系统	22
存储集合 - Telnet	TCP	CMS	受管系统	23
存储集合 - (NSR) - http	http	CMS	受管系统	80
存储集合 - (EVA) - https	https	CMS	受管系统	2372
存储集合 - SNMP	SNMP/udp	CMS	受管系统	161
存储集合 - SMI-S	http	CMS	受管系统	5988
存储集合 - SMI-S	https	CMS	受管系统	5989
服务器数据收集 SMH“唤醒”	http	CMS	受管系统	2301
服务器数据收集启动 (SOAP)	https	CMS	受管系统	2381
服务器数据收集结果 (SOAP)	https	受管系统	CMS	50001
UC 本地通信 (SOAP) - （UC 至 WEBES sidbuilder）	https	CMS	CMS	7902
UC 本地通信 (SOAP) - (GUI、CLI、MessageReceiver)	https	CMS	CMS	20649
UC 本地通信 (SOAP) - （UC 至服务器数据收集启动的 JBoss）	https	CMS	CMS	50001

9.8 配置用于主动式收集服务的 HP-UX 受管系统

HP-UX 受管系统上需要有 Advanced Configuration Collector (ACC)，才能为授权客户启用配置、可用性及性能数据收集。本节说明安装 ACC 以及其他必要配置所需的过程，以便备妥 HP-UX 受管系统来启用主动式支持服务。

9.8.1 下载并安装服务器数据收集客户端

注释： 此时应该已安装 System Management Homepage 先决条件。

ACC 组件作为本地代理程序使用，让 Remote Support Configuration Collector 能够从合格的 HP-UX 受管系统收集配置数据。HP-UX 服务器的 Advanced Configuration Collector (ACC) 组件可在 CMS 上通过 HP Software Manager (RSSWM) 取得。必须分送此组件并安装到 HP-UX 受管系统。 .

ACC 软件压缩在 GZIP 文件中，以 SD-UX 系列软件库的形式来发布。RSSWM 会将文件传送至 CMS 上的以下其中一个缺省位置：

```
c:\Hewlett-Packard\BusinessSupport\UC\ACC-HPUX\
```

或

```
c:\Program Files"(x86)"\SWMAgent\Installers\UC\ACC-HPUX
```

或

```
c:\Program Files\HP\SWMAgent\Installers\UC\ACC\HPUX
```

注释： 在 HP SIM 5.3 中，当安装 HP Remote Support Software Manager 时，可配置此目录。

如果是 Insight Remote Support Advanced A.05.40，则可用的文件如下：

- PA-RISC 软件库：

  ```
  rs-acc-hpux 11.x-PA-A.05.40.xxx.depot.gz
  ```

- Itanium 软件库：

  ```
  rs-acc-hpux 11.x-IA-A.05.40.xxx.depot.gz
  ```

针对这两种 A.05.40 文件，应该根据受管系统的处理器类型来选择并传送适当的文件。

由于每一个客户的环境都不相同，可将此文件分送至 HP-UX 受管系统的方法众多，本指南将不详列所有可能的方法。不过，最简单的作法是登录中央管理服务器 (CMS)，并使用 FTP 将文件传送至受管系统上的临时位置。

依照指示安装 RS-ACC 包：

注释： 下面的 `filename` 实例代表变量。实际文件名取决于所下载的软件库以及是否重命名文件。

- 将从 CMS 复制的软件文件解压缩：

  ```
  gunzip filename.depot.gz
  ```

- 使用已解压缩的软件库文件来安装软件：`swinstall -s $PWD/filename.depot RS-ACC`

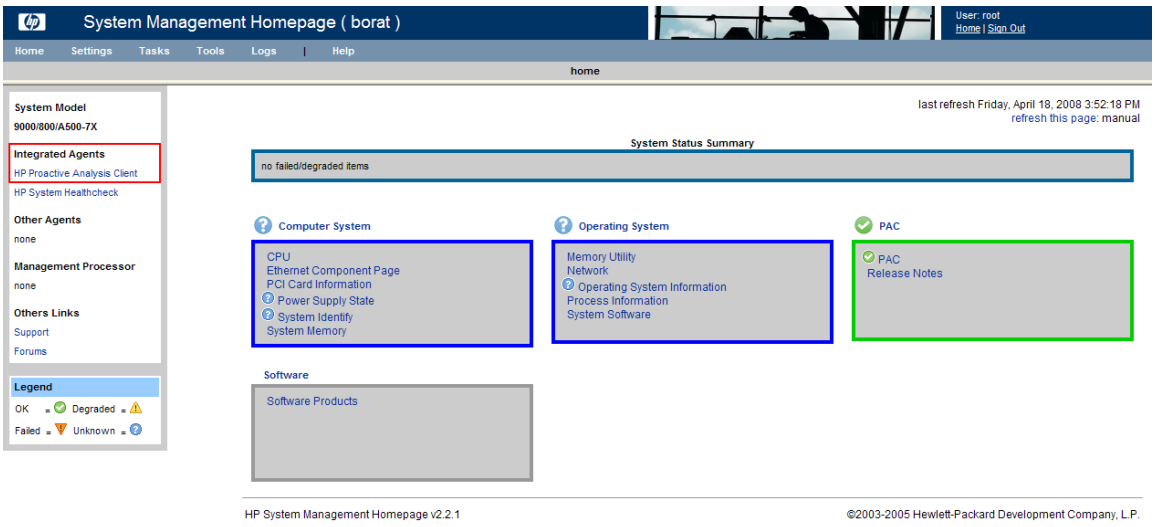
以下是已安装包的 swlist 示例（版本号码不是最新的）：

```
# RS-ACC                A.05.10.15.047 HP Remote Support Advanced Configuration Collector
  RS-ACC.UC-ACC         A.05.10.15.047 HP Remote Support Advanced Configuration Collector
  RS-ACC.MCPS-PAC       A.01.00.00.183 Proactive Client
  RS-ACC.MCPS-AVC       A.02.03.00.00213 HP Availability Collector
  RS-ACC.MCPS-COMMON    A.01.04.00     HP Service Mission Critical Common Component
```

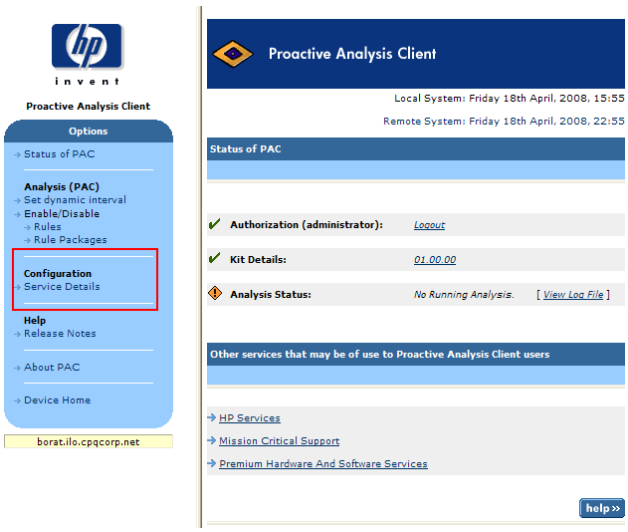
9.8.2 将 System Management Homepage (SMH) 配置为支持自定义的性能集合

如果您是客户的 HP 客户服务团队成员，并且要修改对性能集合执行的分析类型或时间长度以自定义报告，则需要通过 HP-UX 受管系统上的 System Management Homepage (SMH) 来更新 **Specialist E-mail**。要更改密码，请执行以下步骤：

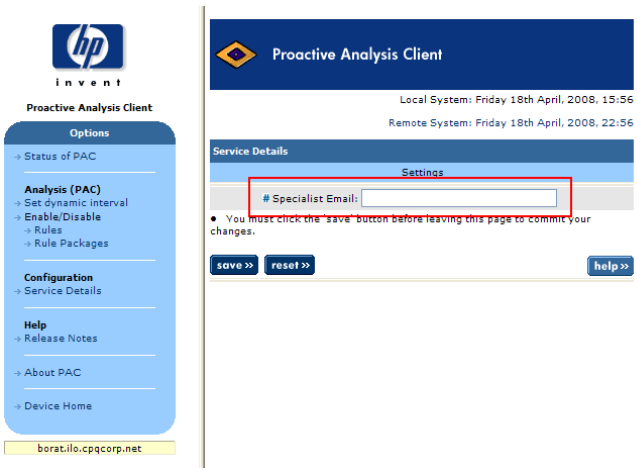
1. 访问 HP-UX 受管系统上的 System Management Homepage
2. 在 SMH 窗口的 **Integrated Agents** 部分下，单击 **HP Proactive Analysis Client** 选项。



3. 在窗口的 **Configuration** 部分下，单击 **Service Details** 选项。



4. 在字段中输入正确的 Specialist 电子邮件地址，然后单击 **Save**。



5. 关闭 System Management Homepage 和 HP Proactive Analysis Client 窗口。

现在，按照《HP Insight Remote Support Advanced CMS 配置与使用指南》 中的指示完成 CMS 配置。

10 OpenVMS 受管系统支持 Insight Remote Support Advanced 的先决条件

10.1 安装或升级必需软件前受管系统需要具备的条件

在升级受管系统以便与 CMS 上安装的 Insight Remote Support Advanced A.05.40 版一起使用之前，必须删除当前可能已安装的 WEBES 或 HP ISEE 客户端的所有先前版本。另外还必须删除 Event Log Monitoring Collector (ELMC)（以前称为 WCCProxy），但在卸载 WEBES 时通常会自动将其一并卸载。

10.1.1 准备 OpenVMS 受管系统

仅当已在受管系统上安装了任意版本的 HP ISEE 客户端、WEBES 或 ELMC 时，才需要执行这些步骤。

10.1.1.1 从 OpenVMS 受管系统中删除 HP ISEE

仅当已在受管系统上安装了 HP Instant Support Enterprise Edition (ISEE) 时，才需要执行这些步骤。如果尚未在受管系统上安装 ISEE，可以跳过本节。

重要信息： Instant Support Enterprise Edition (ISEE) A.03.95 及早期版本与 Insight Remote Support Advanced 不是相同的应用程序，不应安装在任何受管系统上。

要删除 ISEE，请完成下列步骤：

1. 关闭所有正在运行 ISEE 客户端用户界面的浏览器。
2. 登录受管系统。
3. 要从系统中删除 HP ISEE 软件，请运行以下命令：

   ```
   $ PRODUCT REMOVE ISEE
   ```

4. ELMC (WCCProxy) 由 ISEE 与其他工具（如 WEBES）共享。为了确保使用 WCCProxy 的工具计数保持正确，删除 ISEE 后，请在受监控系统上运行以下命令：

   ```
   $ @WCCPROXY_COMMON:[COMMON.WCCPROXY.BIN]WCCPROXY_INSTALL UNINSTALL
   MASTERISEE
   ```

   如果还有任何其他工具仍在使用 WEBES，WCCProxy 会减小使用工具的参考计数。此计数存储在 `WCCPROXY_COMMON:[COMMON.WCCPROXY]REF.CNT` 文件中。

   然后会显示以下文本：

   ```
   WCCProxy is still in use by other applications on this system.

   Uninstallation of the last using application will also remove the
   WCCProxy.

   This Kit will decline deletion.
   ```

   这是 WCCProxy 的正常操作。即使 WCCProxy 不会将自身删除，您也需要执行此命令，向 WCCProxy 通知，ISEE 将不再使用它，这一点很重要。如果 ISEE 是（或曾经是）唯一使用 WCCProxy 的工具，WCCProxy 会将自身删除，并显示如下文本：

   ```
   WCCProxy is being uninstalled.

   The following product has been selected:

      DEC AXPVMS WCCPROXY V1.x-x Layered Product

   The following product will be removed from destination:

   DEC AXPVMS WCCPROXY V1.x-x DISK$ALPHASYS:[SYS0.SYSCOMMON.]
   ```

```
Portion done:
0%...20%...30%...40%...50%...60%...70%...80%...90%...100%


The following product has been removed:
   DEC AXPVMS WCCPROXY V1.x-x Layered Product
```

10.1.1.2 从 OpenVMS 受管系统中删除 WEBES

要从 OpenVMS 受管系统中卸载 WEBES，请执行以下操作：

1. 重新运行安装命令，如下所示：

```
$ @svctools_home:"common.bin"webes_install

WEBES UPDATE - MAIN MENU
========================

 1. SEA Menu
 2. CCAT Menu
 3. Start At Boot Time
 4. Customer Information
 5. System Information
 6. Service Obligation
 7. Start DESTA Director
 8. Stop DESTA Director
 9. Uninstall Webes
    - Fully uninstalls Webes and all installed dependent components
      such as SEA and CCAT
10. Exit
========================
```

2. 从更新菜单中选择"Uninstall WEBES"选项，并按照出现的提示操作。

10.1.2 OpenVMS 受管系统支持 Insight Remote Support Advanced 的先决条件

System Event Analyzer (SEA) 是一种远程系统事件监控工具，也是在 CMS 上运行的 WEBES 组件。

错误日志：安装后，CMS 上的 WEBES 会开始分析当前存储在错误日志中的所有事件，并使用 OpenVMS 系统上安装的 ELMC 来收集事件，这会导致 CPU 使用率长时间偏高。要控制此操作，建议您在安装前按照以下说明归档并清除错误日志。这样可以缩小日志，并缩短初始扫描需要的时间。

请按照以下准则清除错误日志。清除日志时，如果 ELMC 已安装且正在运行，则无需先停止再重新启动 Director 进程。另外，请勿先停止再重新启动 ERRFMT 系统事件日志记录过程。

缺省错误日志（通常是 SYS$SYSROOT:[SYSERR]ERRLOG.SYS）会不断增大并保留在系统磁盘上，直到用户明确将其重命名或删除为止。如果重命名或删除日志文件，约 15 分钟后系统会创建一个全新的错误日志文件。

△ **注意：** 重命名或删除现有日志后，请勿安装 ELMC，除非新的缺省日志出现。

如果重命名日志，稍后就可以对保存的日志进行分析。

定期维护：除了在安装 SEA 前开始使用全新的日志，您可能还希望对错误日志执行定期维护。一种方法是每天重命名 ERRLOG.SYS。例如，可以在每天早上 9:00 将 ERRLOG.SYS 重命名为 ERRLOG.OLD。为了释放系统磁盘上的空间，您可以将重命名的版本备份到不同的卷，然后从系统磁盘中删除该文件。

10.1.2.1 满足 OpenVMS 受管系统的 ELMC 基本要求

安装 ELMC 之前，受管系统必须满足以下基本要求。在群集内，群集的每个节点都需满足以下最低要求：

10.1.2.1.1 系统要求

- 处理器架构：HP AlphaServer 或 Integrity (Itanium) 服务器
- 操作系统 OpenVMS Alpha - 7.3 - 2 或更高版本
- 操作系统 OpenVMS Itanium (Integrity) - 8.2–1 或更高版本
- 可用磁盘空间至少包含 20,000 个块。

10.1.2.1.2 安装条件和要求

- 连接性：必须安装并运行 TCP/IP。

  即使已停止向其他机器传送 TCP/IP 流量，也必须启用将本地主机名解析成 IP 地址的功能。否则，Director 将无法正确处理 ELMC 消息流量，也无法启动。

  ELMC 只正式支持两个用于 OpenVMS 的 TCP/IP 产品：

  — HP TCP/IP Services for OpenVMS 5.4 版或更高版本

  — 处理软件 MultiNet（非 TCPware）

  注释： 其他 TCP/IP 产品可以照常工作，因此无论安装何种 TCP/IP 产品（如果有），WEBES 安装工具包总能完成安装。

- LOCALHOST 条目：为了使 ELMC 正常运转，必须在 OpenVMS TCP/IP HOSTS 数据库中定义 LOCALHOST 条目。缺省情况下该条目已正确定义，但可以将其删除，不过删除会导致 WEBES 失败。

  输入以下命令：

  ```
  $ TCPIP SHOW HOST /LOCAL
  ```

  查找 LOCALHOST，其 IP 地址应该是 127.0.0.1。如果列表中未显示 LOCALHOST，请输入以下命令：

  ```
  $ TCPIP SET HOST LOCALHOST /ADDRESS=127.0.0.1 /ALIAS=LOCALHOST
  ```

  输入 ping 命令确认已添加 LOCALHOST：

  ```
  $ TCPIP PING LOCALHOST
  PING LOCALHOST (127.0.0.1):56 data bytes
  64 bytes from 127.0.0.1:icmp_seq=0 ttl=64 time=0 ms
  64 bytes from 127.0.0.1:icmp_seq=1 ttl=64 time=0 ms
  64 bytes from 127.0.0.1:icmp_seq=1 ttl=64 time=0 ms
  ```

  确认 LOCALHOST 会对 ping 命令做出响应后，可以使用 Ctrl-C 或 Ctrl-Y 停止 ping。

- 系统固件：必备的系统固件支持按照 FRU 表版本 5 规范记录事件，这是处理 WEBES FRU 配置树的必要条件。

  所有 DSxx 和 ES40 系统必须具备固件 V5.7–4 版或更高版本。

  System Event Analyzer 支持的所有其他产品（请参阅 WEBES 发行说明）都附带与 WEBES/SEA 处理兼容的固件版本。

  一般情况下，用户应该获取可用于自己平台的最新固件版本，以充分利用最新的改进功能。

- 验证序列号（仅某些有 SEA 组件的 GS80、GS160 及 GS320 系统才需要）

  某些 GS80、GS160 及 GS320 系统在出厂时并未正确设置系统序列号，而 CMS 上的 SEA 规则必须在序列号已正确设置的情况下才有效。

  涉及的序列号将以字母“G”开头。

  在 SRM 控制台固件提示中（首次启动系统时出现的提示），使用以下命令检查序列号：

  ```
  show sys_serial_num
  ```

  显示的序列号应该与电源柜中机型/序列号标签上的实际序列号一致。如有必要，请使用以下命令更改序列号：

```
set sys_serial_num
```

输入电源柜标签上所显示的六位序列号。

多台 AlphaServer

订购多台 AlphaServer 时，也可能会发生这种问题，因为工厂可能将相同的序列号分配给每个系统。在这种情况下，SEA 规则无效，因为它们要求每台 AlphaServer 有一个唯一的序列号。如果发生这种情况，在使用 set sys_serial_num 命令时，请在序列号后面加上 –1、–2、–3 等，依此类推，以便唯一标识每台 AlphaServer。

分区

请注意，同一台 AlphaServer 上多个分区的序列号必须相同，因为它们都在同一台机器上。这种情况下不存在 SEA 冲突问题，因此请不要尝试为同一台机器上的不同分区分配唯一的序列号。

10.1.2.1.3 必需的权限和访问权

- 要安装或卸载 ELMC，用户需要具备以下 OpenVMS 权限：
  - ALTPRI
  - BUGCHK
  - BYPASS
  - CMKRNL
  - DIAGNOSE
  - IMPERSONATE
  - NETMBX
  - OPER
  - SYSLCK
  - SYSPRV
  - TMPMBX

  卸载 WEBES 时，执行卸载的用户名必须与原来安装 WEBES 时的用户名相同。

  仅当群集是由单个系统磁盘提供服务时，SET PROCESS 命令才能对所有群集节点设置权限。但在具有多个系统磁盘的群集上，您可能会选择在由其他系统磁盘提供服务的节点上安装 WEBES，而不在由正在安装的系统磁盘提供服务的节点上安装。在这种情况下，SET PROCESS 不会在这些节点（由其他系统磁盘提供服务的节点）上设置权限，WEBES 也无法在这些节点上正确安装。

  要在具有多个系统磁盘的群集上正确安装，请在想要安装 ELMC 的所有节点上将必需的权限设为缺省值（登录时获得的权限），而不需要使用 SET PROCESS 命令。

  有关一对多系统磁盘的其他注意事项，请参阅“共享的非系统磁盘安装”一节。

  运行 ELMC

  要执行任意 ELMC 命令，用户需要具备以下 OpenVMS 权限。请注意，这些只是安装、升级或卸载 ELMC 所需的部分权限：

  - ALTPRI
  - BUGCHK
  - CMKRNL
  - DIAGNOSE
  - IMPERSONATE
  - NETMBX
  - SYSPRV
  - TMPMBX

- 安装目录所需的群集节点访问权限

  群集节点必须能够访问用来安装ELMC的目标目录，安装包才能安装在群集节点上。也就是说，这些节点必须安装包含目标目录的磁盘。这意味着可能无法在所有群集节点上安装 ELMC，因为并非所有节点都能识别将安装 ELMC 的位置。

  下面举例说明了这个问题：

  — 群集：所有节点共享同一个系统磁盘。

    安装节点：任意节点

    安装目标：缺省位置 SYS$COMMON:[HP...]

    结果：ELMC 会自行安装在所有节点上。

  — 群集：除两个节点外，其他所有节点都共享系统磁盘 A。这两个节点共享系统磁盘 B。

    安装节点：使用系统磁盘 A 的节点。

    安装目标：缺省位置 SYS$COMMON:[HP...]

    结果：其他两个节点都不会安装 ELMC。

    在上例中，从其余两个节点中的任意一个运行安装程序，并再次选择缺省位置 SYS$COMMON:[HP...]，即可在其余两个节点上再次安装 ELMC。请注意，这是完全独立的 ELMC 安装，与第一次在大多数节点上的安装不同。

  — 群集：除两个节点外，其他所有节点都共享系统磁盘 A。这两个节点共享系统磁盘 B。所有节点也都装入了非系统磁盘 C。

    安装节点：任意节点

    安装目标：磁盘 C 上的目录，由您在安装期间指定。

    结果：ELMC 会自行安装在所有节点上。

注释： 在所有情况下，安装包都允许您选择只在部分节点上可以看见安装位置。

10.1.2.2 在 OpenVMS 受管系统上安装 ELMC 软件包

共享的非系统磁盘安装

OpenVMS 群集可以包含由单个通用系统磁盘提供服务的节点，也可以包含由多个系统磁盘提供服务的节点。任何给定的节点都仅由一个系统磁盘提供服务，但一个系统磁盘可以为一或多个节点提供服务。每个系统磁盘都包含自己的 PCSI 数据库（产品注册表）。

ELMC可以安装在系统磁盘上，也可以安装在共享的非系统磁盘上。但是，由不同系统磁盘提供服务的多个节点可以访问共享的非系统磁盘。这表示ELMC并非只能安装在由给定系统磁盘提供服务的节点上。但 PCSI 数据库只能属于一个系统磁盘。

这种情况可能会在 PRODUCT SHOW PRODUCT WEBES 命令中造成矛盾。从某一节点（该节点与最初安装 WEBES 的节点（即安装节点）由同一系统磁盘提供支持）运行此命令时，始终会显示已安装 ELMC。这是因为 ELMC 安装程序只会将 ELMC 注册到为安装节点提供服务的系统磁盘的PCSI数据库中，而不会注册到任何其他PCSI数据库中。可能会产生两种误导信息，如下图所示。

- 如果某个节点与安装节点都由同一个系统磁盘提供服务，但用户并没有将ELMC添加至该节点，则该命令会显示已安装 ELMC，但实际并未安装。
- 反之，如果某个节点与安装节点分别由不同的系统磁盘提供服务，且用户已将 WEBES 添加至该节点，则该命令将不显示已安装 WEBES，但实际已安装。

解压缩安装软件包

要解压缩 ELMC 安装包，请将 .EXE 可执行文件放在符合以下条件的某个目录中：

- 该目录中不存在其他工具包，尤其是其他版本的 WEBES 工具包。
- 该目录中不存在先前操作留下的WEBES或WCC旧文件。（最可靠的方法是使用空目录。）

然后输入以下命令：

```
$ run ELMC_{version}.EXE
```

此命令会解压缩 ELMC 安装文件。

执行 ELMC OpenVMS 安装

符合上面说明的所有条件后，请运行安装命令并按照提示进行操作。

注释： 此命令会在当前目录中执行 DCL 脚本 WCCPROXY_INSTALL.COM。请勿执行 PRODUCT INSTALL WCCPROXY 命令，此命令通常用来安装基于 PCSI 的产品。此命令会中止并提示您改为运行 WCCPROXY_INSTALL 脚本。将缺省目录设置为包含 wccproxy_install.com 文件的目录，在上一步解压缩 ELMC .exe 文件时已创建此文件。

执行 DCL 脚本：

```
$ @wccproxy_install install
```

工具包的安装和完成没有用户提示。当返回 DCL 提示符 ($) 时，说明安装已完成，ELMC (WCCProxy) 进程将开始运行。

10.2 在 WEBES 用户界面中更新 ELMC 协议

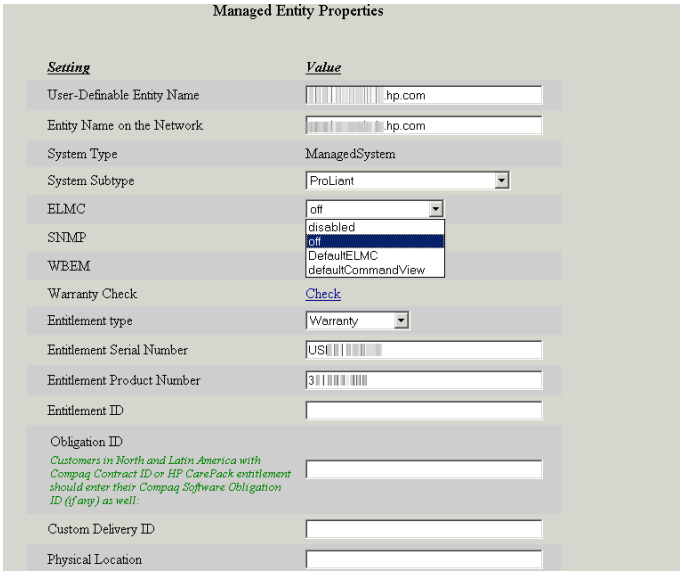
因为 WEBES 会自动安装在 CMS 上，**之后** ELMC 软件库包才能分发并安装在受管系统上，所以您需要登录 CMS 上的 WEBES 界面并修改通信协议来包含 ELMC。 请在 CMS 上完成以下步骤：

1. 打开 System Event Analyzer 界面：

   开始→程序→ Hewlett-Packard Service Tools → Service Event Analyzer → Service Event Analyzer

2. 在屏幕顶部的工具栏上，单击 **Configure Webes Managed Entities** 图标。

3. 从列表中选择您的受管系统，然后单击主机名链接。
4. 在 Managed Entity Properties 屏幕上，从下拉菜单中选择启用 ELMC。



5. 应用所做更改并关闭 System Event Analyzer。

11 Tru64 Unix 受管系统支持 Insight Remote Support Advanced 的要求

11.1 安装或升级必需软件前受管系统需要具备的条件

在 CMS 上升级受管系统以便与 Insight Remote Support Advanced A.05.40 版一起使用时，必须删除所有当前可能已安装的旧版 WEBES 或 HP ISEE 客户端。另外还必须删除 Event Log Monitoring Collector (ELMC)（以前称为 WCCProxy），但在卸载 WEBES 时通常会自动将其一并卸载。

11.1.1 从 Tru64 UNIX 受管系统中删除 HP ISEE

仅当已在受管系统上安装了 HP Instant Support Enterprise Edition 时，才需要执行这些步骤。如果尚未在受管系统上安装 ISEE，可以跳过本节。

重要信息： Instant Support Enterprise Edition (ISEE) A.03.95 及早期版本与 Insight Remote Support Advanced 不是相同的应用程序，不应安装在任何受管系统上。

要删除 ISEE，请完成下列步骤：

1. 以 **root** 身份（系统管理权限）登录受监控的系统。
2. 将目录转至安装 HP ISEE 时创建的目录 `/usr/ISEEInstall`。
3. 要从系统中删除 HP ISEE 软件，请运行以下命令：

   ```
   ./ISEEuninstall.sh
   ```

11.1.2 从 Tru64 UNIX 受管系统中删除 WEBES

要从 Tru64 UNIX 受管系统中卸载 WEBES，请运行交互式 `/usr/sbin/webes_install_update` 实用程序，选择删除所有 WEBES，并根据出现的提示进行操作。在群集中，卸载时会从群集中的所有节点删除 WEBES。

11.2 满足 Tru64 受管系统的 ELMC 基本要求

安装 ELMC 之前，受管系统必须满足以下基本要求。在群集内，群集的每个节点都需满足以下最低要求：

11.2.1 系统要求

- 处理器架构：HP AlphaServer
- 操作系统 Tru64 UNIX 4.0F、4.0G、5.1A 版或更高版本

注释： 请注意，HP Sustaining Engineering 会维护 Tru64 UNIX 操作系统的支持日程。对于已超过支持有效期的操作系统版本上安装的 WEBES，HP 不承诺支持。请访问以下 URL：http://www.hp.com/hps/os/os_pvs_amap.htm

- 至少需要 20 MB 的可用磁盘空间，才能安装所有组件。

11.2.2 Tru64 Unix 受管系统支持 Insight Remote Support Advanced 的要求

在 Tru64 Unix 受管系统上安装 ELMC 软件前，请先阅读下列各节：

11.2.2.1 归档并清除错误日志

System Event Analyzer (SEA) 是一种远程系统事件监控工具，也是在 CMS 上运行的 WEBES 组件。如果希望 SEA 自动分析系统的本地错误日志，您必须在支持的 HP 硬件平台或包含支持的 HP I/O 设备的机器上安装 SEA。要查看所支持产品的列表，请参阅《WEBES 发行说明》。

安装后，CMS 上的 WEBES 会开始分析当前存储在错误日志中的所有事件，并使用 Tru64 UNIX 系统上安装的 ELMC 来收集事件，这会导致 CPU 使用率长时间偏高。要控制这项操作，建议您在安装 ELMC 前（如本节中所述）归档并清除错误日志。这样可以缩小日志，从而节省初始扫描的成本。

如果您决定清除日志时 WEBES 已安装且正在运行，请先停止 Director 进程，再进行此操作（有关停止 Director 的详细信息，请参阅 《SEA User Guide》）。在归档并清除错误日志后，按照 http://h18023.www1.hp.com/support/svctools/webes/index.html 上 《SEA User Guide》 的步骤说明，重新启动 Director。

11.2.2.1.1 4.0F

1. 停止 binlogd 进程：`# /sbin/init.d/binlog stop`
2. 如果需要，请将原始错误日志移动到任意适当的名称，例如：

   ```
   # mv /var/adm/binary.errlog /var/adm/binary.errlog.2002_06_11
   ```

   稍后将对保存的日志进行分析。
3. 如果跳过了步骤 2，请删除原始错误日志：`# rm /var/adm/binary.errlog`
4. 重新启动系统。重新启动时，系统会创建新的 binary.errlog 文件，其中包含新的配置事件。系统还会重新启动 binlogd 进程。

11.2.2.1.2 4.0G

1. 停止 binlogd 进程：`# /sbin/init.d/binlog stop`
2. 如果需要，请将原始错误日志移动到任意适当的名称，例如：

   ```
   # mv /var/adm/binary.errlog /var/adm/binary.errlog.2002_06_11
   ```

   稍后将对保存的日志进行分析。
3. 如果跳过了步骤 2，请删除原始错误日志：`# rm /var/adm/binary.errlog`
4. 重新启动 binlogd 进程：`# /sbin/init.d/binlog start`

11.2.2.1.3 5.A 或更高版本

新功能可将信号发送至 binlogd 以保存当前日志并创建新日志，而无需停止此进程。请执行“**确认 binary.errlog CDSL**”和“**在运行 binlogd 期间清除日志**”这两节中的步骤。

11.2.2.1.3.1 确认 binary.errlog CDSL

在 5.1A 版或更高版本中，二进制错误日志 /var/adm/binary.errlog 应该是指向每个群集节点专属文件的上下文独立符号链接 (CDSL)。这样可确保每个节点上的 binlogd 进程将该节点的事件存储至该节点的专属错误日志 /var/cluster/members/{memb}/adm/binary.errlog。

如果 CDSL 被删除，binlogd 将其重新创建为群集通用文件，但无法正常运行。要检查您的文件，请发出以下命令：

```
# ls -l /var/adm/binary.errlog
```

正确的输出如下所示：

```
>lrwxrwxrwx 1 root adm 43 Jun 11 12:54 /var/adm/binary.errlog -> ../
cluster/members/{memb}/adm/binary.errlog
```

错误的输出不会显示 -> 链接指示符：

```
-rw-r----- 1 root adm 560 Jun 11 12:59 /var/adm/binary.errlog
```

如果需要，请执行下列步骤来更正文件：

1. 通过在每个节点上发出以下命令，停止所有群集节点上的 binlogd 进程：

   ```
   # /sbin/init.d/binlog stop
   ```

2. 稍后将对保存的日志进行分析。如果需要，请将原始错误日志移动到任意适当的名称，例如：

   ```
   # cd /var/adm
   # mv binary.errlog binary.errlog.2002_06_11
   ```

3. 对要保存的任意节点专属错误日志发出类似的移动命令，例如：

   ```
   # mv /var/cluster/members/{memb}/adm/binary.errlog
   /var/cluster/members/{memb}/adm/binary.errlog.2002_06_11
   # mv /var/cluster/members/{memb}/adm/binlog.saved/binary.errlog.saved
   /var/cluster/members/{memb}/adm/binlog.saved/
   binary.errlog.saved.2002_06_11
   ```

4. 删除现有的错误日志，忽略所有 **No such file or directory** 错误：

   ```
   # rm /var/adm/binary.errlog
   # rm /var/cluster/members/{memb}/adm/binary.errlog
   # rm /var/cluster/members/{memb}/adm/binlog.saved/binary.errlog.saved
   ```

5. 创建 CDSL：

   ```
   # mkcdsl /var/adm/binary.errlog
   ```

6. 通过在每个节点上发出以下命令，重新启动所有群集节点上的 binlogd 进程：

   ```
   # /sbin/init.d/binlog start
   ```

11.2.2.1.3.2 在 binlogd 运行期间清除日志

对于 5.1A 版或更高版本，请在要清除的每个群集节点上执行下列步骤：

1. 确认已如上所述完成 binary.errlog CDSL 部分。
2. 如果需要，请保留先前保存的所有副本，以免因将其移动至适当的名称后被覆盖，例如：

   ```
   # cd /var/cluster/members/member/adm/binlog.saved
   # mv binary.errlog.saved binary.errlog.2002_06_11
   ```

3. 导致 binlogd 复制并清除原始错误日志：

   ```
   # kill -USR1 `cat /var/run/binlogd.pid`
   ```

   先前的命令不会结束 binlogd 进程。而是向 binlogd 发送信号，让它将 /var/adm/binary.errlog 复制到 /var/cluster/members/member/adm/binlog.saved。然后只使用配置事件重新创建原始 /var/adm/binary.errlog 文件。请注意，/var/adm/binary.errlog 是一个指向 /var/cluster/members/{memb}/adm/binary.errlog 的 CDSL。

有关详细信息（包括如何自动管理这类错误日志），请参阅 binlogd 手册的“管理二进制错误日志文件”这一节。

11.2.2.2 序列号验证

在 GS80、GS160 及 GS320 系统上，确认序列号与在受管系统上安装 ELMC 前指示的序列号相同。

某些 GS80、GS160 及 GS320 系统在出厂时并未正确设置系统序列号，而 CMS 上的 SEA 规则必须在序列号已正确设置的情况下才有效。涉及的序列号将以字母“G”开头。

在 SRM 控制台固件提示中（首次启动系统时出现的提示），使用以下命令检查序列号：

```
show sys_serial_num
```

显示的序列号应该与电源柜中机型/序列号标签上的实际序列号一致。如有必要，请使用以下命令更改序列号：

```
set sys_serial_num
```

输入电源柜标签上所显示的六位序列号。

- **多台 AlphaServer：**在订购多台 AlphaServer 时，也可能会发生这种问题，因为工厂可能将相同的序列号分配给每个系统。在这种情况下，SEA 规则无效，因为它们要求每台 AlphaServer 有一个唯一的序列号。如果发生这种情况，在使用 set sys_serial_num 命令时，请在序列号后面加上 –1、–2、–3 等，依此类推，以便唯一标识每台 AlphaServer。
- **分区** 在同一台 AlphaServer 上，多个分区有相同的序列号，因为它们都在同一台机器上。这种情况下不存在 SEA 冲突问题，因此请不要尝试为同一台机器上的不同分区分配唯一的序列号。

11.2.2.3 满足 Tru64 Unix 受管系统的 ELMC 基本要求

系统必须符合下列基本要求，才能安装 ELMC。在群集内，群集的每个节点都需满足以下最低要求：

11.2.2.3.1 系统要求

- 处理器架构：HP AlphaServer
- 操作系统：Tru64 UNIX 4.0F、4.0G、5.1A 版或更高版本

  请注意，HP Sustaining Engineering 会维护 Tru64 UNIX 操作系统的支持日程。对于已超过支持有效期的操作系统版本上安装的 WEBES，HP 不承诺支持。请访问以下 URL：http://www.hp.com/hps/os/os_pvs_amap.htm
- 至少需要 20 MB 的可用磁盘空间，才能安装所有组件
- 必须安装并运行 TCP/IP 服务。

11.2.2.3.2 安装条件要求

- 如果您有使用 SLI2 编程接口的 EMX LP6000、LP7000 或 LP8000 适配器 (KGPSA–xx)，请升级至 Emulex (EMX) 驱动程序的 1.22 版或更高版本。使用 1.22 版以前的 EMX 驱动程序可能会导致无法正确处理数据。
- 系统固件：必备的系统固件支持按照 FRU 表版本 5 规范记录事件，这是处理 WEBES FRU 配置树的必要条件。
  - 所有 DSxx 和 ES40 系统必须具备固件 V5.7–4 版或更高版本。
  - 其他所有系统（当前为 ES45、GSxx 及 TS202c）均附带可与 WEBES 处理兼容的固件版本。

  一般情况下，用户应该获取可用于自己平台的最新固件版本，以充分利用最新的改进功能。

11.2.2.3.3 必需的权限和访问权

要安装、升级或卸载 WEBES，您必须以 root 用户的身份登录。/usr/opt/hp/svctools 目录归 root 所有，且 root（所有者）拥有 rwx（读取、写入及执行）权限，而其他用户（组或通用组）则没有权限。

11.2.2.4 在受管系统上安装 ELMC Tru64 Unix 软件包

首先解压缩 ELMC 软件包，然后进行安装。

11.2.2.4.1 解压缩 ELMC 软件包

要解压缩 ELMC 安装包，请将安装包 .gz 文件放在临时目录中并解压缩：

```
# gunzip WEBES{version}.tar.gz
```

然后解压缩文件。如果在执行此命令时已经有“kit”子目录，请先确定此子目录中没有先前的 WEBES 安装包文件，然后再执行命令。

```
# tar -xvf ELMC_{version}.tar
```

此命令会创建一个 kit 目录（如果该目录事先不存在），并解压缩 ELMC 安装文件。

11.2.2.4.2 安装 ELMC 软件包

注释： 如果在 TruCluster 环境中进行安装，请在确定所有节点都已启动且正在运行后再继续操作。

当前目录是安装包的解压缩目录时，请输入以下命令来安装 ELMC WCCProxy 的文件。

```
# setld -l kit
```

请勿运行 setld -D 将 ELMC 安装到非缺省目录。ELMC 需要缺省目录才能正常运行。

工具包的安装和完成没有用户提示。当返回 shell 提示符 (#) 时，说明安装已完成，wccproxy 进程将会运行。

11.3 在 WEBES 用户界面中更新 ELMC 协议

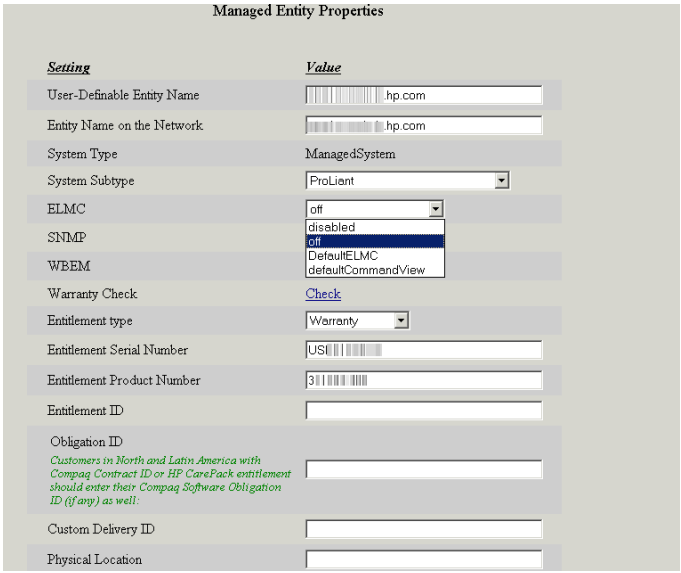
因为 WEBES 会自动安装在 CMS 上，**之后** ELMC 软件库包才能分发并安装在受管系统上，所以您需要登录 CMS 上的 WEBES 界面并修改通信协议来包含 ELMC。请在 CMS 上完成以下步骤：

1. 打开 System Event Analyzer 界面：

   Start → Programs → Hewlett-Packard Service Tools → Service Event Analyzer → Service Event Analyzer

2. 在屏幕顶部的工具栏上，单击 **Configure Webes Managed Entities** 图标。

3. 从列表中选择您的受管系统，然后单击主机名链接。
4. 在 Managed Entity Properties 屏幕上，从下拉菜单中选择启用 ELMC。



5. 应用所做更改并关闭 System Event Analyzer。

12 HP Insight Remote Support Advanced 支持 EVA 的要求

12.1 了解不同的服务器类型和软件应用程序

需要一台或多台 Windows ProLiant 服务器来托管环境中必需的远程支持和 EVA 监控软件应用程序；实际设备数量取决于用来支持 EVA 的 CommandView 版本。

- Insight Remote Support Advanced 和 HP Systems Insight Manager (HP SIM) **始终**需要中央管理系统 (CMS)，但 CMS 上可以同时安装 CommandView 8.0.1 及更高版本，因此不需要单独的 SMS。
- 所有版本的 CommandView 8.0 及更早版本都需要单独的存储管理服务器 (SMS)。

警告！ CommandView 8.0 及更早版本**不能**安装在 CMS 上，而对于那些 CommandView 版本，则需要单独的 SMS 或 SMA 以及单独的 CMS。要安装 CommandView 8.0.1，必须先安装 CommandView 8.0。在 CMS 上，**请勿安装** StorageWorks CommandView EVA 的早期版本。请勿在 SMS（运行 CommandView 8.0 或更早版本的系统）上安装 WEBES、HP SIM 或 Insight Remote Support Advanced Client。

12.1.1 中央管理系统 (CMS)

HP Insight Remote Support Advanced 是 HP Systems Insight Manager (HP SIM) 的一个插件。Insight Remote Support Advanced 与 HP SIM 软件应用程序都位于中央管理服务器 (CMS) 上，依靠其他软件组件来管理客户环境，并将配置集合和事件数据提交给 HP 支持中心进行分析和响应。

必须具有《HP Insight Remote Support Advanced CMS Configuration and Usage Guide》中定义的基本 CMS 配置。满足了 CMS 系统先决条件后，按照《HP Insight Remote Support Advanced A.05.40 配置与使用指南》注册并配置 CMS。可以从以下 URL 获取 Insight Remote Support Advanced 技术文档：http://docs.hp.com/en/netsys.html#Remote%20Support%20Pack

12.1.2 存储管理服务器

CommandView V8.0.1 可以安装在 CMS 上，而不需要安装在单独的 SMS 或 SMA 上。但是，只有存储管理服务器 (SMS) 或存储管理设备 (SMA) 才支持 CommandView 的所有早期版本。CommandView EVA 将事件写入 SMS/SMA 上的 Windows 应用程序日志中。SMA 实际上相当于 Windows 2000 平台上的 SMS。

为方便起见，除非有必要强调这两种存储管理类型之间的差异，否则本文档始终使用 SMS 一词。

本章其余部分会根据您选择使用的机型分成几个较大的节：

- “CMS 上的 CommandView 8.0.1 及更高版本”
- “单独 SMS/SMA 上运行的 CommandView”
- “在 ABM 上使用 CommandView 支持 EVA4400 的要求”
- “EVA 受管系统故障排除”

12.2 CMS 上的 CommandView 8.0.1 及更高版本

如果您选择在中央管理系统 (CMS) 上运行 CommandView 8.0.1 软件，请阅读本节。如果要在**单独的** SMS 服务器上运行当前的 CommandView 软件，或者要使用 CommandView 8.0 或更早版本，则必须将 CommandView 安装在这台单独的 SMS 设备上，并跳至“单独 SMS/SMA 上运行的 CommandView”。

重要信息： 以下内容摘自 HP StorageWorks CommandView EVA 和 HP Systems Insight Manager 安装说明。要在同一台服务器上安装 HP CommandView EVA 8.0.1 和 HP Systems Insight Manager 5.3.1，请按照以下说明操作。

在执行这些安装过程之前，请确保满足管理服务器的下列要求：

- 已安装支持的 Microsoft Windows 版本。
- 先前未安装 HP CommandView EVA。
- 已安装 Windows SP2 的安全补丁。

12.2.1 重要的端口设置信息

WBEM/WMI 和 SMI-S 缺省分配的端口 5989 与 CMS 上的 HP-SIM 冲突。WEBES 子组件与 WBEM 指示的交互、WMI Mapper 以及将 HP-UX 系统纳入环境，都使得环境的配置更加复杂。HP-UX 硬编码为使用端口 5989。下面几节说明了可解决端口分配问题的更改，并提供了使用 CommandView SMI-S 配置 Insight Remote Support Advanced 的新解决方案。

注释： 如果已经配置了 Insight Remote Support Advanced 环境并且其运行正常，那么可以选择不做任何更改，并计划仅在发现相关问题时再执行以下步骤。

在 CMS 上安装 HP SIM 和 CommandView SMI-S 的顺序会影响缺省端口设置。当前的最佳做法是建议**先安装 HP SIM**，并允许 WMI Mapper 使用缺省端口 5989。CommandView 安装会检测此端口是否正在使用，如果正在使用则重定向到其他端口。

请从命令窗口中执行以下命令，评估环境中当前的端口分配情况：

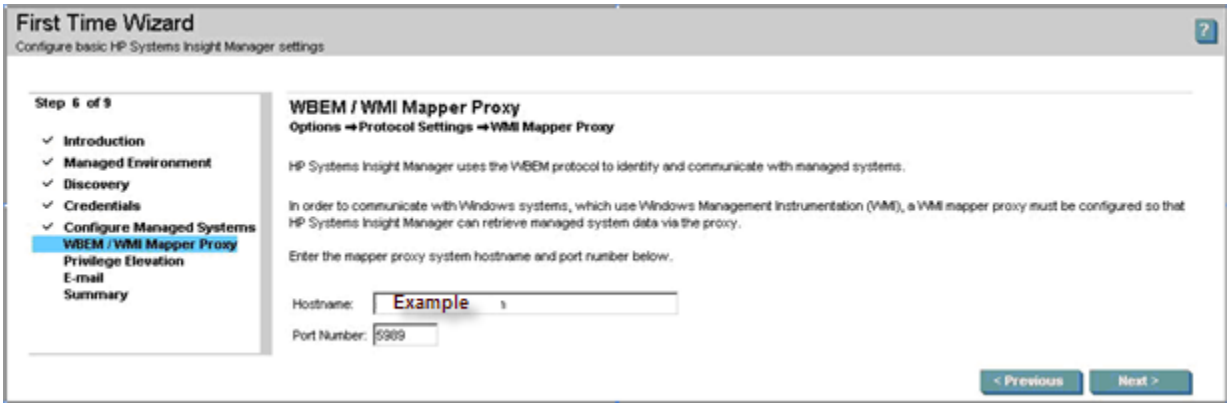
```
C:\ netstat -anb >netstat.txt
```

12.2.2 关于新 HP SIM 安装的重要信息

如上所述，最佳做法是在安装 CommandView EVA **之前**先安装 HP SIM。本节及其各小节仅适用于 CMS 上全新的 HP SIM 安装。

1. 在安装 HP SIM 期间，First Time Wizard 会提示您配置 WBEM / WMI Mapper Proxy。

图 12-1 HP SIM First Time Wizard



保持缺省端口设置 5989。安装好 HP SIM 后，将 CommandView SMI-S 将使用的端口添加至以下步骤示例中显示的 xml 文件。

2. 确定 HP SIM 将用于连接 SMI-S 的端口。以下示例使用端口 60000 建立到 **namespace interop** 的 SMI-S https 连接。
3. 在文本编辑器中打开以下文件：

   ```
   C:\Program Files\HP\Systems Insight Manager\config\identification\
   wbemportlist.xml
   ```

4. 将以下文本行添加至文件结尾处。

注释： 示例中显示了完整的文件，红色的行表示将添加到文件的新行。

图 **12-2 XML** 文件示例

```
<?xml version="1.0" encoding="UTF-8"?>
<wbemportlist>
  <port id="5989" protocol="https">
    <cimnamespacelist>
      <cimnamespace name="root/cimv2"/>
      <cimnamespace name="vmware/esxv2"/>
      <cimnamespace name="root/hpq"/>
    </cimnamespacelist>
    <interopnamespacelist>
      <interopnamespace name="root/pg_interop"/>
      <interopnamespace name="root"/>
      <interopnamespace name="root/emulex"/>
      <interopnamespace name="root/qlogic"/>
      <interopnamespace name="root/ibm"/>
      <interopnamespace name="root/emc"/>
      <interopnamespace name="root/smis/current"/>
      <interopnamespace name="root/hitachi/dm51"/>
      <interopnamespace name="interop"/>
      <interopnamespace name="root/interop"/>
      <interopnamespace name="root/switch"/>
      <interopnamespace name="root/cimv2"/>
    </interopnamespacelist>
  </port>
  <port id="60000" protocol="https">
    <interopnamespacelist>
      <interopnamespace name="interop"/>
    </interopnamespacelist>
  </port>
</wbemportlist>
```

5. 保存 `wbemportlist.xml` 文件。
6. 重新启动 HP SIM 服务。

   右键单击 Windows Services API 中的 HP Systems Insight Manager 服务，然后从下拉菜单中选择 **restart**。

12.2.3 更正现有的 HP SIM 安装

重要信息： 如果是第一次安装 HP SIM，请勿执行以下步骤。仅当已经安装了 HP SIM 并且已将 WMI Mapper 端口重新配置为缺省端口 5989 以外的设置时，才执行这些步骤。

EVA 的旧版 Insight Remote Support Advanced 受管系统文档中以使用 6989 为例，说明如何更改 WMI Mapper 的端口设置。仅当已安装了 HP SIM 并且已将 WMI Mapper 端口更改为缺省值 5989 以外的值时，才执行以下更正步骤。

请执行以下步骤，将 WMI Mapper 端口还原为缺省端口。

注释： 重新启动服务之后，在文件 `cimserver_planned.conf` 中所做的更改会移至文件 `cimserver_current.conf` 中。

1. 使用 Windows Services API 停止 Pegasus WMI Mapper Service。

1. 选择**开始**和**运行**，在运行字段中输入 **services.msc**。
2. 单击**确定**。

2. 在文本编辑器中打开文件：`C:\Program Files\The Open Group\WMI Mapper\cimserver_planned.conf`
3. 将引用 `httpsPort=6989` 的行中的端口号更改为 `5989`。

注释： 端口号可能已设为其他值，而不是示例中显示的 6989。

4. 保存文件。
5. 重新启动 Pegasus WMI Mapper Service。
6. 运行 netstat 命令并确认已应用更改。

   ```
   C:\ netstat -anb >netstat.txt
   ```

   下面是 `cimserver_planned.conf` 文件中文本的示例。

图 12-3 cimservr 文本示例

```
enableRemotePrivilegedUserAccess=true
enableHttpsConnection=true
enableHttpConnection=false
sslCertificateFilePath=C:\hp\sslshare\cert.pem
sslKeyFilePath=C:\hp\sslshare\file.pem
httpsPort=5989
```

12.2.4 在 CMS 的 HP SIM 用户界面中更改 WMI Mapper Proxy 端口

1. 以管理权限访问 HP SIM 用户界面。
2. 确认 CMS 的现有凭据正确无误：
   a. 访问 **All Systems List**，从列表中选择作为 HP SIM CMS 的设备。
   b. 单击 **Tools & Links** 选项卡。
   c. 单击 **System Credentials** 链接。
   d. 确认登录凭据存在且适合 CMS（首选），或者，如果存在 **Advanced** WBEM 设置，请确认已经为 SMI-S 使用的端口正确配置了 WBEM 协议，并且提供了正确的用户名/密码凭据。
3. 从上部导航栏中选择 **Options - Protocol Settings - WMI Mapper Proxy**。
4. 为 localhost 上运行的 WMI Mapper 的 CMS 实例选择单选按钮。
5. 单击 **Edit** 按钮。
6. 在 **port number** 字段中输入 **5989**。
7. 单击 **OK** 保存设置。

12.2.5 将缺省值还原至 wbemportlist.xml 文件

1. 在文本编辑器中打开文件：`C:\Program Files\HP\Systems Insight Manager\config\identification\wbemportlist.xml`

   下面是关于先前如何修改文本的示例（红色文本）。请在您的文件中将这些文本删除。

图 **12-4 wbemportlist** 文件示例

```
<!-- WMI Mapper httpsPort=6989  -->
    <port id="6989" protocol="https">
        <cimnamespacelist>
            <cimnamespace name="root/cimv2"/>
        </cimnamespacelist>
   </port>
```

2. 将以下文本行添加至文件结尾处。

注释： 示例中显示了完整的文件，红色的行表示将添加到文件的新行。

图 **12-5 XML** 文件示例

```
<?xml version="1.0" encoding="UTF-8"?>
<wbemportlist>
   <port id="5989" protocol="https">
      <cimnamespacelist>
         <cimnamespace name="root/cimv2"/>
         <cimnamespace name="vmware/esxv2"/>
         <cimnamespace name="root/hpq"/>
      </cimnamespacelist>
      <interopnamespacelist>
         <interopnamespace name="root/pg_interop"/>
         <interopnamespace name="root"/>
         <interopnamespace name="root/emulex"/>
         <interopnamespace name="root/qlogic"/>
         <interopnamespace name="root/ibm"/>
         <interopnamespace name="root/emc"/>
         <interopnamespace name="root/smis/current"/>
         <interopnamespace name="root/hitachi/dm51"/>
         <interopnamespace name="interop"/>
         <interopnamespace name="root/interop"/>
         <interopnamespace name="root/switch"/>
         <interopnamespace name="root/cimv2"/>
      </interopnamespacelist>
   </port>
   <port id="60000" protocol="https">
      <interopnamespacelist>
         <interopnamespace name="interop"/>
      </interopnamespacelist>
   </port>
</wbemportlist>
```

3. 保存文件。
4. 重新启动 HP SIM 服务。
   - 通过选择 **Options - Identify Systems**，重新识别 HP SIM 中的所有 WBEM/WMI 系统以更正端口引用

12.2.6 安装和配置 CommandView AFTER HP SIM

CommandView EVA 安装工具包内有 SMI-S 组件。只有在安装时，SMI-S 才会分配两个端口。SMI-S 分配的缺省端口如下（如果可用）：

- http port=5988

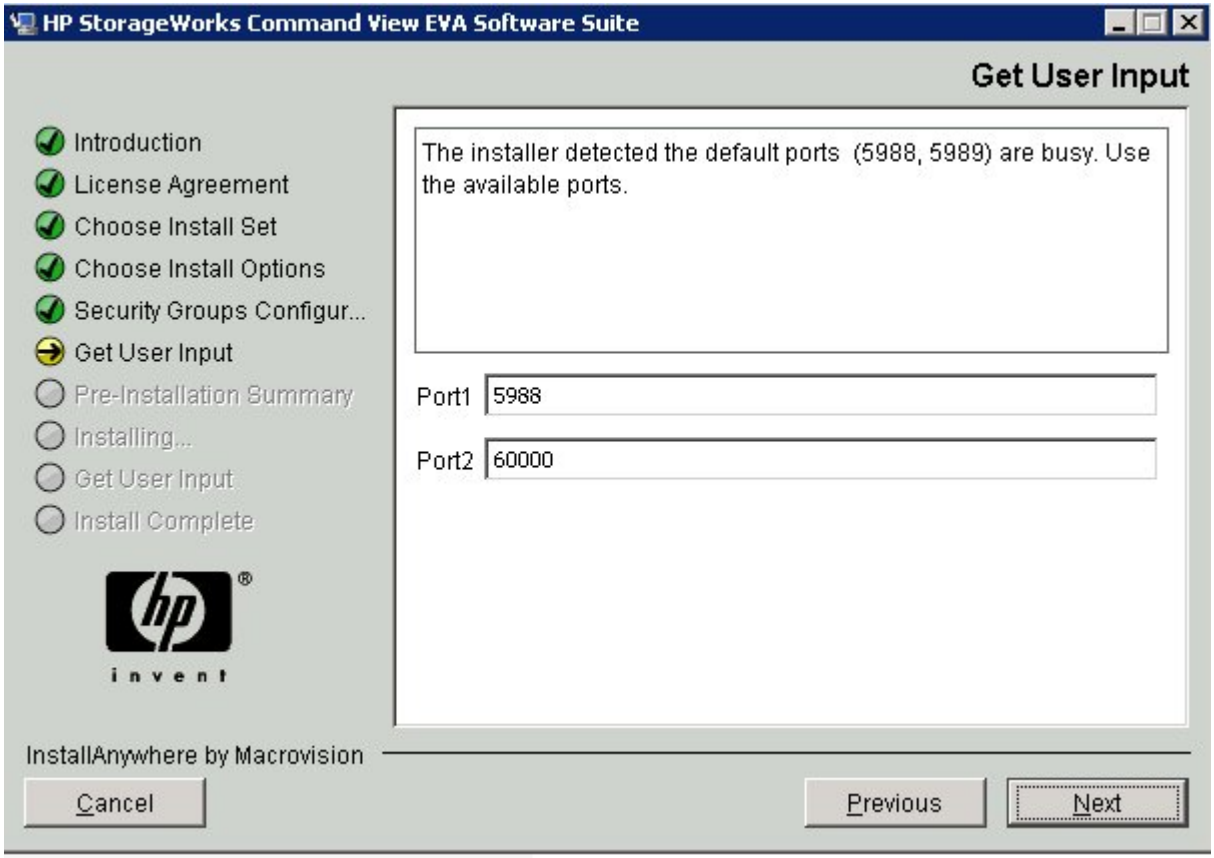
- https port=5989

如果正在使用其中一个端口或两个端口都在使用，安装程序会提供其他配置屏幕，以便您更改端口号。SMI-S 安装程序会建议使用端口 60000（如果此端口未被使用）。SMI-S 会保留端口 5988（如果没有冲突）。启动 HP StorageWorks CIM Object Manager 程序时，SMI-S 会使用这些端口。

注释：　只有在检测到端口冲突时才会显示此屏幕。这就是强烈推荐安装 CommandView 之前先安装 HP SIM 的原因。

下图是在已安装了 WMI Mapper 和 HP SIM 的 Insight Remote Support Advanced CMS 上安装 SMI-S 的示例：

图 12-6 SMI-S 安装补充屏幕



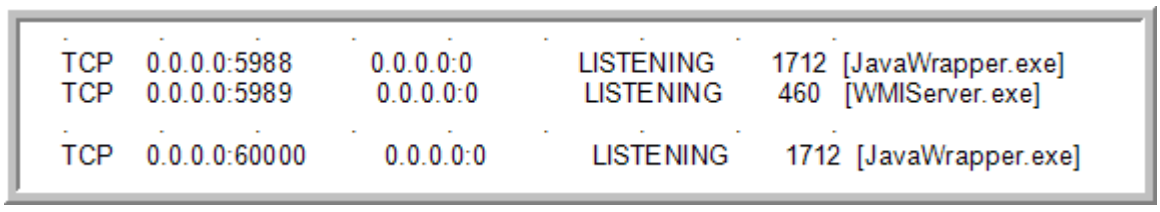
有关端口设置的详细信息以及配置 Windows 帐户进行 CommandView 访问的相关信息，请参阅《HP StorageWorks CommandView EVA 安装指南》。HP SIM 和 WEBES 需要这些凭据。

使用 `netstat` 命令验证这些端口后，

```
C:\ netstat -anb >netstat.txt
```

您将看到以下输出：

图 12-7 netstat 结果



注释： 在上例中，SMI-S 配置为使用端口 5988 和 60000。

12.2.7 当 CommandView 先于 HP SIM 安装时，请重置端口号

1. 编辑文件：

   ```
   C:\Program Files\Hewlett-Packard\SMI-S\CXWSCimom\config\
   cxws.properties
   ```

2. 找到 `cxws.http.port and cxws.https.port` 条目并将其重置为以下值：

   ```
   cxws.http.port=5988
   cxws.https.port=60000
   ```

3. 重新启动 HP StorageWorks CIM Object Manager

注释： 任何需要通过此 SMI-S 与阵列进行通信的 API，也必须更新目标端口。在独立的 SMS 配置中，只要不与 SMS 上的其他端口发生冲突，CommandView 就应该使用缺省端口 5988 和 5989 与 Insight Remote Support Advanced 通信。

12.3 单独 SMS/SMA 上运行的 CommandView

在 CMS 之外单独配置 SMS 时，请使用本节及其各小节作为指导。

以下软件应用程序在 SMS 上运行，且与 (Insight Remote Support Advanced) 解决方案有关或属于此解决方案：

- CommandView
- Event Log Monitoring Collector (ELMC)，以前称为 WCC Proxy
- MC3 组件

注释： SMS 和 SMA 的文件夹路径有一定差异。具体的路径差异不在本文讨论范围之内。在此提出只是为了让您了解 CommandView EVA 文件位于 SMA 上的不同文件夹内。

从 CommandView V8.0 开始，**添加/删除程序**窗口中已看不到软件组件 HP StorageWorks SMI-S CIMOM 和 HP StorageWorks SMI-S EVA。请检查是否存在名为 HP StorageWorks CIM Object Manager 的服务以及该服务的状态，验证组件是否已安装并且正在运行。确认 SMS/SMA 是否已安装 CommandView EVA 7.0.1 或更高版本，以及 SMI-S EVA 和 SMI-S CIM 组件（即构成 SMI-S 的两个组件）。转至 SMS 上的 Windows 控制面板，并确保“添加/删除程序”对话框中列出了以下组件：

- HP StorageWorks CommandView EVA
- HP StorageWorks SMI-S CIMOM
- HP StorageWorks SMI-S EVA

注意： 从托管系统中删除 SMI-S 时也会强制删除 Command View Tape Library (CV TL)。CV TL 的版本必须与磁带库中使用的固件相匹配。

如果 CV TL 所安装的 SMI-S 版本比 CommandView 使用的版本更旧，请在 CV TL **之后**安装或升级 CommandView，以免发生冲突。

此外，安装时会彼此覆盖每个软件应用程序所用的凭据。因此，建议使用相同的帐户信息以免信息丢失。

注释： 安装 CommandView EVA STANDARD 是支持 Insight Remote Support Advanced 的优先条件。

如果**未**安装必需的 CommandView 组件，有关详细信息，请参阅“在 SMS 上配置 CommandView for EVA 的要求和文档”

注释： 您可以在《HP StorageWorks EVA Software Compatibility Reference》中找到 SMS 系统和硬件要求，网址为：

http://h20000.www2.hp.com/bc/docs/support/SupportManual/c01525950/c01525950.pdf?jumpid=reg_R1002_USEN（请参考 PDF 中下面两张表；《表 4.1 管理服务器类型支持的软件》和《表 4.2 支持的 EVA 软件操作系统》）。

有关详细信息，请参阅《HP StorageWorks CommandView EVA Software Suite QuickSpec Overview》，网址为：http://h18004.www1.hp.com/products/quickspecs/12239_div/12239_div.html

12.3.1 在 SMS 上配置 CommandView for EVA 的要求和文档

您可以通过下面的 URL 获取 CommandView for EVA 文档：http://h18006.www1.hp.com/products/storage/software/cmdvieweva/index.html（单击 **Support for your product** 链接，查看 CommandView EVA 手册列表）

安装和配置 CommandView 时需要以下文档：

- 《HP StorageWorks CommandView EVA Installation Guide》
- 《HP StorageWorks CommandView EVA 版本号 发行说明》
- 《HP StorageWorks EVA Software Compatibility Reference》

12.3.2 CommandView 7.0.1 至 8.0.1(具有 SMI-S）要求概述

本文适用于 CommandView EVA 7.0.1 至 8.0.1。请务必查阅 CommandView EVA 文档，了解基本要求。另外，CommandView 8.0 版和更早版本无法在 CMS 上运行。从 CommandView 8.0.1 版开始，现在支持在 CMS 上运行 CommandView。为实现容错或负载平衡功能，一个环境中可以有多个 SMS；但在任何时候都只能有一台 CommandView 服务器主动管理给定的 EVA 阵列。

要成为有效的 SMS，服务器上必须安装 CommandView EVA（7.0.1 版或更高版本），且至少管理一个阵列。SMI-S 随 CommandView EVA 一起安装并且必须安装，因为它是 HP SIM 与阵列之间的通信路径（使用 CIMOM 进行 WBEM 通信）。

注释： EVA 的事件数据只会传递给主动管理阵列的 CommandView。但在任何运行 CommandView 的服务器上，只要能够成为 EVA 设备阵列的主动管理者，都应该安装 ELMC。当前未主动管理 EVA 的所有 CommandView 实例均称为被动 CommandView 实例。

12.3.3 SMS 或 SMA 系统和访问要求

存储管理服务器 (SMS) 访问要求：

- Microsoft Windows 帐户必须具有访问 CommandView EVA 所需的正确组权限。

安装 CommandView for EVA 时会在系统中添加两个新的组权限，即 HP Storage Admins（写入权限）和 HP Storage Users（读取权限）。

12.3.4 WEBES – EVA 通信

CMS 上的 WEBES 要求凭据帐户至少有读取权限。此用户名和密码是在 SMS 的 WEBES Managed Entity 页面中输入。这样 WEBES 就能够与阵列进行通信。有关此过程的详细信息，请参阅 “CommandView EVA 密码配置”。

12.3.5 HP SIM – EVA 通信

通过 SMI-S，HP SIM 与 EVA 阵列之间可以使用 WBEM 协议进行通信。CommandView 8.0 版之前的版本所附带的 SMI-S 采用了 CIMOM，它定义了单独的用户凭据来支持此 WBEM 通信路径。从 CommandView 8.0 版和更高版本开始，SMI-S 已建立了证书信任并使用 CommandView 凭据（如“SMS 或 SMA 系统和访问要求”中所述）。

在 CommandView 8.0 版之前，安装 CommandView EVA 时会在 SMS 上为帐户创建 cimuser 凭据，用户名和密码均为 administrator。SMS 上必须先存在权限级别至少为读取权限的 Windows 系统管理员帐户（例如，“SMS 或 SMA 系统和访问要求”中所述的 HP Storage Users），才能成功地自动创建此 cimuser 身份。

重要信息： HP SIM 要求必须在 System Protocol Settings 页面中输入这组用户凭据（请参阅“HP SIM 中 WEBES 的设置”），SMS CIMOM 才能与 EVA 进行 WBEM 通信。

在 CommandView 8.x 版中，这种情况已经发生了变化。SMI-S 已不再有单独的用户名/密码。现在利用 CommandView 和 SMI-S 之间的信任关系，采用单点登录 (SSO) 设计。CommandView 用户名和密码将用于 SMI-S 连接。

CommandView for EVA 文档包含有关设置自定义管理员帐户的其他信息。在设置 WBEM 凭据后，如果无法使 HP SIM 找到 EVA 阵列，或者不确定密码设置，请参阅“SMI-S 凭据故障排除”，了解如何修改或重置这些凭据。另请参阅“WBEMDISCO 故障排除”，其中介绍了 WBEMDISCO 实用程序的使用，此实用程序可用于测试用户名和密码。

注释： 可能有其他应用程序将 HP SIM 用作连接 EVA 的接口（例如 Storage Essentials）。如果这类应用程序执行主动管理功能，则可能需要具有写入权限。在这种情况下，应确保 cimuser 帐户与具有 HP Storage Admins 组权限的 Windows 帐户相关联。

12.3.6 SMS 上需要的软件

SMS 上需要具备以下软件应用程序，SMS 和 EVA 才能支持 Insight Remote Support Advanced：

- 支持的 HP StorageWorks CommandView EVA 版本，其中包括 SMI-S（获取 EVA 远程支持的必要条件）。
- 缺省安装 SMI-S 的 CommandView for EVA 工具包。SMI-S 由两个组件组成（SMI-S CIMOM 和 SMI-S EVA），而 SMS 上需要这两个组件。

重要信息： 虽然 SMI-S 在安装 CommandView 时是可选组件（缺省情况下，标准安装会将其一并安装），但在 SMS 上这是获得 EVA 设备远程支持的必要条件，如果选择执行 CommandView EVA 自定义安装，请勿取消选择 SMI-S。

警告！ 如果 SMS 安装过多个版本的 CommandView EVA，可能会存在一些永久文件和/或注册表条目，而这些将对 SMI-S 的运行带来不利影响。有关详细信息，请参考以下建议：《HP StorageWorks CommandView EVA v6.x to v7.0 Upgrade Issue with the v5.0.3 Patch Installed》.

- Windows ELMC（又称为 WCCProxy）只会下载到 CMS 上，为支持 EVA 设备而安装到 SMS 上。
- HP SIM 和 Insight Remote Support Advanced 需要有 ProLiant Insight Management Agents，才能将 SMS 视为受管系统。HP SIM 支持 IM Agent 6.30 版或更高版本，但除非 SMS 是 SMA，否则建议您升级至最新可用的版本。

警告！ 如果您的存储管理设备是 SMA，则建议不要升级至最新版的 ProLiant Management Agents，因为 SMA 上仅支持特定版本的 Insight Management Agents。HP SIM 和 Insight Remote Support Advanced 还需要有 SNMP 服务，才能支持 SMS 作为受管系统。

- HP SIM 和 Insight Remote Support Advanced 还需要有 SNMP 服务，才能支持 SMS 作为受管系统。

12.3.7 满足 Windows SMS 的 ELMC 一般要求

除上面列出的 SMS 要求外，受管系统 (SMS) 还必须符合以下基本要求，才能安装 ELMC。

磁盘空间：安装时，已安装 Windows 操作系统的驱动器上必须有 40MB 的总可用空间（%SystemDrive%，缺省情况下，通常是 C:）。安装完成后总共会使用 30MB 空间。

12.3.7.1 安装条件和要求

ELMC 软件的位置：必须将从 RSSWM 下载至 CMS 的 ELMC for Windows 组件复制到受管系统上的本地驱动器。如果映射到属于其他系统的驱动器盘符，安装将会出现错误。

重要信息： 必须从 SMS 的本地驱动器安装 ELMC，不支持从远程映射共享进行安装。

12.3.7.2 必需的权限和访问权

要安装、删除或更新 ELMC，用户 ID 必须为下列之一：

- 计算机上 Administrators 组的成员
- 某个组的成员，而该组又是计算机上 Administrators 组的成员。例如，如果用户 ID 是 Domain Admin，且已将 Domain Admins 添加至本地计算机上的 Administrator 组，则您已具有必要的权限。要将 Domain Administrators 添加至本地 Administrator 组，请根据操作系统执行相应的操作。

ELMC 提供通信路径，以便 WEBES 监控 CommandView 写入的事件数据。建立此通信路径后，WEBES 会对 Windows 应用程序事件日志中找到的事件数据进行分析。如果尚未清除应用程序事件日志，此初始分析可能需要很长时间才能完成，并且会消耗 SMS 和 CMS 的带宽。另外，在完成初次清除之前，安装结束时所发送的 SEA 测试事件以及所有新事件均无法传递。

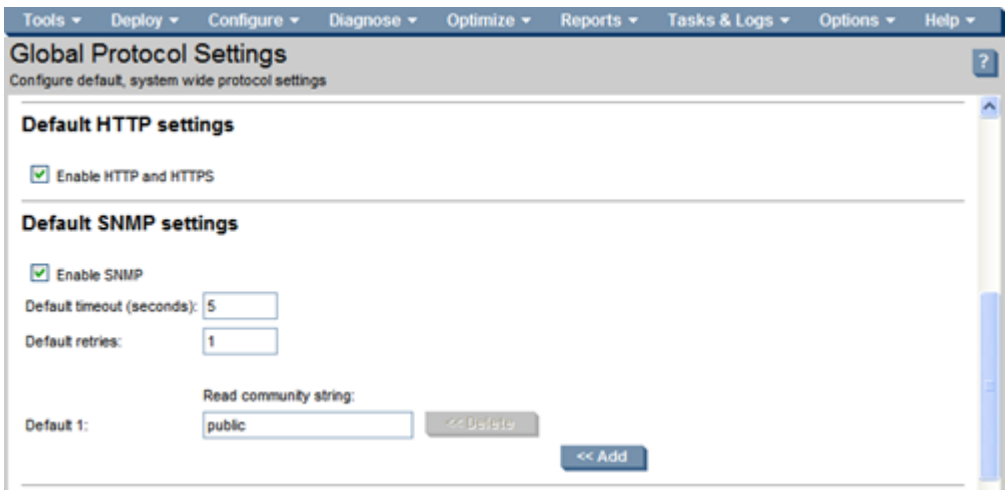
最佳作法是在安装之前归档旧的事件数据并清除应用程序事件日志，以减少这种开销。WEBES 建议将应用程序事件日志属性大小设为至少 10MB，并且覆盖时间视需要而定。可能需要根据环境条件调整这些设置。有关详细信息，请参阅“清除 SMS 上的事件日志”。

12.3.7.3 配置 SNMP 服务

必须在 SNMP 服务器属性中设置 CMS 的团体和 IP 地址，才能使 ProLiant SMS 成为向 CMS 发送报告的受管服务器。要配置 SNMP 服务，请执行以下步骤：

1. 从服务中，右键单击 **SNMP Service**，然后选择 **Properties**。
2. 选择 **Security** 选项卡，并输入 HP SIM 的 HP SIM Global Protocol Settings 页面中的 **Community** 名称。
3. 要检查 HP SIM 中定义的团体名称，请执行以下步骤：
   a. 转至 **Options - Protocol Settings - Global Protocol Settings**。
   b. 在 Global Protocol Settings 页面的 Default SNMP settings 区域中，检查 **Read** community string 字段中的条目。

图 12-8 Default SNMP settings 区域



4. 选择 **Traps** 选项卡。
5. 输入**团体**名称。
6. 输入**陷阱**目标。这是 CMS 的 TCP/IP 地址。localhost 或回送地址也必须作为目标包含其中；否则 HP-SIM 将无法从 SMS 检索到足够的信息，也就无法通过远程支持授权检查（RSEC）。
7. 单击**确定**。

12.3.7.4 在 SMS 上安装 ELMC 以获取 EVA 远程支持

12.3.7.4.1 准备 SMS 以进行 ELMC 安装

仅当您在 SMS 上安装了任意版本的 HP ISEE 客户端、WEBES、OSEM 或 WCCProxy 时，才需要执行这些步骤（"从 SMS 中删除 HP ISEE"至"从 SMS 中删除 OSEM"）。

12.3.7.4.1.1 从 SMS 中删除 HP ISEE

仅当您在受管系统上安装了 HP Instant Support Enterprise Edition (ISEE) 时，才需要执行这些步骤。如果尚未在受管系统上安装 ISEE，可以跳过本节。

重要信息： Instant Support Enterprise Edition (ISEE) A.03.95 及更早版本与 Insight Remote Support Advanced 不是相同的应用程序，不应将其安装在任何 SMS 上。

要删除 ISEE，请执行以下步骤：

1. 在控制面板中双击**添加/删除程序**。
2. 在**添加/删除程序**对话框中，找到 ISEE 条目（如果存在），然后单击**删除**。

12.3.7.4.1.2 从 SMS 中删除 WEBES

注释： 从 SMS 中删除 ISEE 后，删除 WEBES 时应该也会将 WCCProxy 一并删除。如果尚未删除 ISEE，则 WEBES 不会删除 WCCProxy。

提示： 在删除 WEBES 之前，建议您访问 System Event Analyzer (SEA) UI，并在 Managed Entities 页面中找到系统序列号和产品 ID。以后在 CMS 上的 HP SIM 中配置受管系统的属性时，可以使用此信息。

要从 SMS 中卸载所有的 WEBES 工具（包括 WCCProxy），请执行以下步骤：

1. 使用具有管理员权限的帐户登录 SMS。
2. 完全关闭所有正在运行的工具。
3. 在控制面板中双击**添加/删除程序**。
4. 在**添加/删除程序**对话框中，找到 WEBES 条目并单击**更改/删除**以运行安装向导。
5. 看到提示时，选择 **Remove** 选项。
6. 按照提示继续卸载。
7. 在**添加/删除程序**对话框中，确认不存在 WCCProxy 条目。如果存在此项目，可以通过选择并单击**删除**，手动将其删除。

12.3.7.4.1.3 从 SMS 中删除 OSEM

卸载时会完全删除 OSEM 目录下的所有文件。如果需要，可以手动备份配置文件，例如 `working.props`、`hosts.txt` 或 `communities.txt`。

您可能还想备份通知文件夹，以保留所有问题报告的副本。OSEM 1.3.7 或更高版本在卸载过程中会复制所有配置和状态信息。

要从 SMS 中卸载所有 OSEM 工具，请执行以下步骤：

1. 使用具有管理员权限的帐户登录。
2. 完全关闭所有正在运行的工具。

3. 在控制面板中双击**添加/删除程序**。
4. 在**添加/删除程序**对话框中，找到 OSEM 条目并单击**删除**以运行安装向导。

注意： 在安装向导中，您只能通过第一个 Cancel 按钮完全退出卸载例程。之后，即使提供取消或退出选项，也无法取消或停止卸载。

5. 按照提示继续执行卸载过程。

12.3.7.4.2 清除 SMS 上的事件日志

对于 EVA 远程支持来说，此步骤可选，但 HP 建议您在安装 ELMC 之前，先归档和清除 SMS 上的应用程序日志。

刚开始安装和启动 ELMC 时，WEBES 会处理最近记录的事件，而这可能会暂时占用资源。一般情况下，在可能有问题的系统上安装ELMC时，此功能很有用，因为应用程序日志信息在解决问题时非常有用。

在安装 ELMC 之前，请按照以下步骤归档和清除 Windows 应用程序事件日志：

1. 打开事件查看器：

   在 Windows Server 2003 上：**开始 | 程序 | 管理工具 | 事件查看器**

2. 在事件查看器窗口的左侧窗格中，单击应用程序日志。

   清除所有事件：选择 **Action | Clear all Events**。清除之前，您可以选择将现有事件保存到其他文件中。稍后将对保存的日志进行分析。除非您认为保留当前的事件列表没有意义，否则请将日志保存到您选择的目录。

3. 关闭事件查看器。

12.3.7.4.3 在 SMS 上安装 ELMC

注释： 如果正在 CMS 上安装 CommandView 8.0.1，并且 CMS 已要求一个 ELMC 实例，则无需安装第二个实例。如果正在非 CMS 的 SMS/SMA 上安装任意版本的 CommandView，并且希望远程监控服务器，则需要此 ELMC 实例。

满足第一章所述的先决条件后，要安装 ELMC 软件包，请执行以下步骤：

1. 从 CMS 中将 ELMC 安装可执行文件下载到 SMS。

   安装可执行文件位于 CMS 上的以下文件夹：

   - `%system driver%\Hewlett-Packard\Business Support\ELMC\Windows_x86_x64`

   安装可执行文件的文件名与以下文件名类似：

   - `ELMC_WCCProxy_v###_Windows_x86_x64.exe`

注释： Remote Support Software Manager 中的 Windows ELMC 软件包是 ProLiant CMS 的一个可执行文件，并且还是可以移植到 SMS 的软件库。

2. 在 SMS 上，双击 `ELMC___.exe` 文件。

   此时会显示一系列进度窗口，然后安装完成。

   不需要用户输入任何数据，也不会出现任何提示。

3. 不会出现关于 ELMC 安装完成的通知（在将来的 EMC 版本中会更正这一点）。
4. 要确认 ELMC 已完成安装且正在运行，请在 SMS 上打开命令窗口并执行以下命令：

   `wccproxy status`

   此命令将输出 `The WCCProxy service is running`。

12.3.8 在 CMS 上配置针对 EVA 的信息

12.3.8.1 CommandView EVA 密码配置

如"SMS 或 SMA 系统和访问要求"中所述，CommandView EVA V6 和更高版本均采用安全登录 (SSL) 设计，因此，只有使用 Windows 帐户用户名和密码才能访问 CommandView EVA 用户界面。CommandView for EVA UI 用户名和密码也是 WEBES 与 EVA 阵列进行通信所必需的，而且必须要在 WEBES SEA Web 界面的 Managed Entities 屏幕中手动输入，才能处理 EVA 事件。此用户名和密码没有缺省值。可由系统管理员进行设置。帐户至少需要有读取访问（**HP 存储用户**）组权限。

注释：

- CMS 上的 HP SIM 使用 SMS 上的 SMI-S 所提供的 WBEM 协议 CIMOM 与 EVA 进行通信。
- CMS 上的 WEBES 先与 SMS 上的 ELMC 进行通信，然后再使用 SMS 上的 CommandView 与 EVA 进行通信。

有关设置有效 SMS 和阵列的信息，请参阅 CommandView EVA 安装文档。您可以通过下面的 URL 获取 CommandView for EVA 文档：

- http://h20000.www2.hp.com/bc/docs/support/SupportManual/c01375105/c01375105.pdf?jumpid=reg_R1002_USEN

  （单击 **Support for your product** 链接，查看 CommandView EVA 手册列表）

  安装和配置 CommandView for EVA 时需要下列文档：

  — 《HP StorageWorks CommandView EVA Installation Guide》
  — 《HP StorageWorks CommandView EVA》
  — 《HP StorageWorks EVA Software Compatibility Reference》

12.3.8.2 设置 SMS 与 CMS 之间的信任关系

1. **设置 SMS 与 CMS 之间的信任关系：**

注释： 利用此信任关系，HP SIM 可以链接到要在 CMS 上显示的 CommandView EVA 阵列页面。

这种信任关系并非一定要设置。但有了它 SIM 就可以从 CommandView 收集大量其他信息，并通过 HP-SIM 中 SMS 页面上的链接来提供这些信息。

   a. 使用 CommandView UI，选择页面右上角的 **Server Options** 链接。这时将打开 Management Server Options 页面。
   b. 选择 **System Insight Manager/Replication Solutions Manager trust relationships** 的按钮。这时将打开 SIM/RSM Trust Relationship 页面。
   c. 选择 **Install Certificate** 的按钮。将 DNS 地址输入到 CMS。
   d. 选择 **Install Certificate**。

2. **确认已加载 SMI-S 的证书：**
   a. 使用 CommandView UI，选择页面右上角的 **Server Options** 链接。这时将打开 Management Server Options 页面。
   b. 选择 **Other Application Trust Relationships** 的按钮。
   c. 对于本地 SMS，确认已加载 **SMI_EVA_Provider** 证书。

      如果缺少 SMI_EVA_Provider 证书，请参阅"SMA 上的 CommandView SSO 证书：将 SSO 证书添加至 CommandView EVA 信任库 "，了解有关加载此证书的说明。

12.3.8.3 HP SIM 中 WEBES 的设置

1. 在 HP SIM 发现运行 CommandView 的服务器（正在管理 EVA 阵列）之后，在 HP SIM 中配置其系统属性。

   在 HP SIM 中配置受管系统的系统设置，如下所示：

   - 您可以在 HP SIM 中配置跨多个系统的系统设置 (**Options ¦ System Properties ¦ Set System Properties**)。
   - 您可以为 HP SIM 中的单个系统配置所有设置，方法是从 HP SIM 集合中选择系统，或在 HP SIM 中搜索系统。在 HP SIM 中显示服务器的详细信息后，选择 **Tools and Links** 选项卡，然后选择 **Edit System Properties** 链接。

注释： 对于 SMS（以及连接的 EVA 设备），WEBES 会从 HP SIM 中的 System Properties 页面捕获以下受管实体信息：

- 公司信息
- 联系信息
- 序列号
- 产品 ID
- 合同信息

您需要提供此信息以确保 SMS 能够通过**远程支持授权检查 (RSEC)**，并且能够将事件传送至 HP 支持中心。

EVA-LE 阵列例外。WEBES 将与 EVA-LE 阵列直接通信，获取产品型号和产品序列号。如果在 HP SIM System Properties 字段中显示此信息，它将覆盖自动检测的信息。

有关配置系统设置的详细信息，请参考《A.05.40 Insight Remote Support Advanced 配置与使用指南》，网址为：

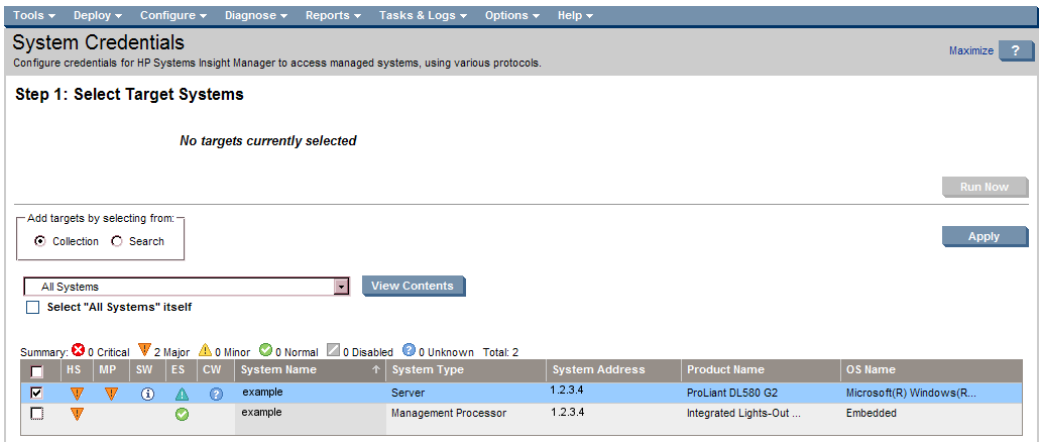
http://docs.hp.com/en/netsys.html#Remote%20Support%20Pack

要在 HP SIM 中配置系统的 WBEM 设置，请执行下列操作：

对于 HP SIM 5.3.1

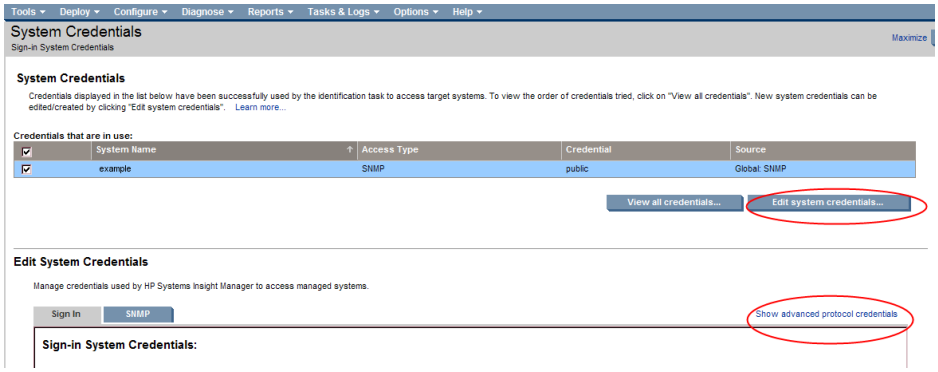
a. 选择 **Options > Security > Credentials > System Credentials**

b. 在 **Systems Credentials** 屏幕中搜索系统，或从 System Type 下拉列表中选择系统，然后单击 **Apply**。

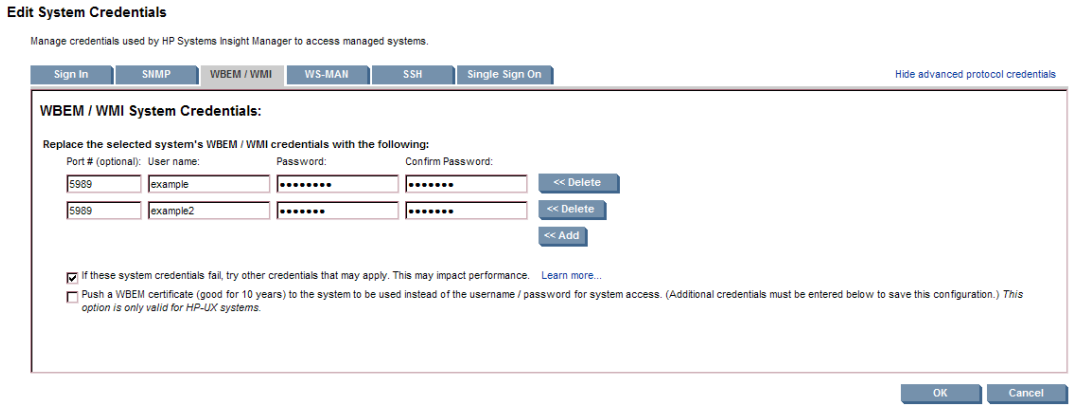


c. 单击 **Run Now**。

d. 在 **System Credentials** 屏幕中单击 **Edit system credentials** 按钮，屏幕将展开。



e. 在屏幕的 **Edit System Credentials** 部分单击 **WBEM/WMI** 选项卡。现在，您可以为此受管系统设置特定的WBEM/WMI凭据，或者使用在先前步骤中设置的全局缺省设置。确认选中 **If these system credentials fail, try other credentials that may apply...** 复选框，然后单击 **OK**。



对于 **HP SIM 5.3.1**

a. 转至 **Options ¦ Protocol Settings ¦ System Protocol Settings**。

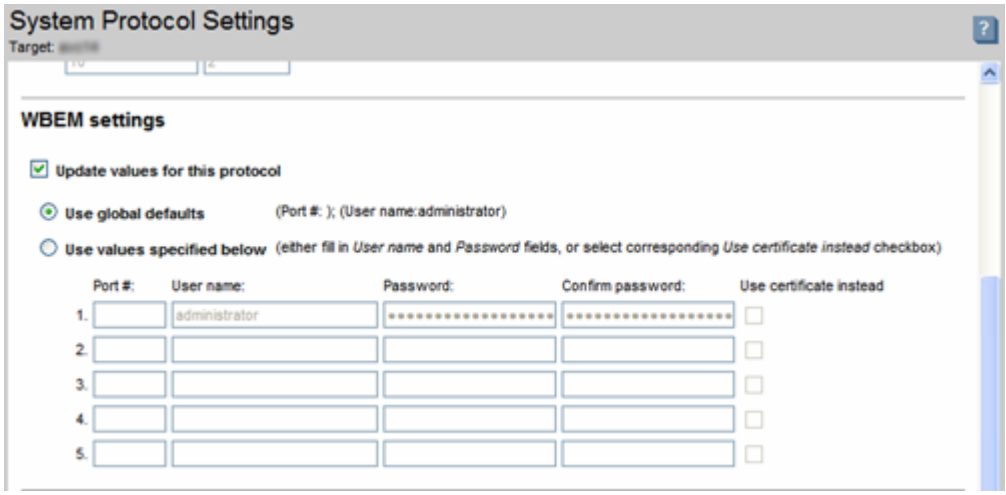
b. 在 **Step 1: Select Target Systems** 页面中，从下拉列表中选择 HP SIM 集合（包含运行 CommandView 的服务器），以显示与该集合关联的系统。

c. 从列表中选择您的系统，然后单击 **Apply**。

d. 再次选择系统，然后单击 **Next**，将显示 **Step 2: Specify the communications protocol settings for target systems** 页面。

e. 在 **WBEM settings** 部分选择 **Update values for this protocol** 复选框，并根据需要对设置进行编辑。SMI-S 使用缺省端口 5989。

图 **12-9 System Protocol Settings** 页面



注释： 还可以通过 **Options ¦ Protocol Settings ¦ Global Protocol Settings** 在 HP SIM 中配置全局通信协议。

f. 单击 **Run Now** 应用所做的更改。

2. 执行 SMS 的另一项“发现”将生成 HP SIM 系统列表中列出的 EVA。

如果 EVA 阵列没有出现，说明 HP SIM 与 SMI S 之间的通信有问题，请参阅“HP SIM 未发现 EVA”。

12.3.8.4 配置 WEBES

12.3.8.4.1 提供 WEBES 中的 SMS 受管实体信息

WEBES 会从 HP SIM 获取所有必要的受管实体信息，但不包括 CommandView 用户凭据。将受管实体视为“CommandView 服务器”是指将系统视为 SMS。

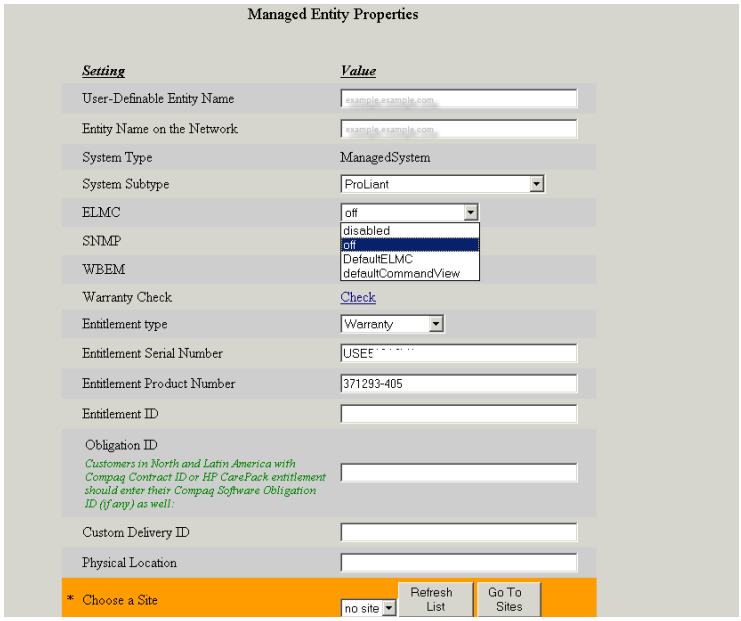
注释： 如果 WEBES 中的 Managed Entities 页面将 SMS 视为 CommandView 服务器以外的任何服务器，请确认 SMS 上已安装了 ELMC，然后重新启动 DESTA，如下所示：

1. 打开命令提示符并运行以下命令：net stop desta_service
2. 使用以下命令重新启动 DESTA：net start desta_service
3. 如果重新启动 DESTA 也无法解决问题，请从 WEBES 的 Managed Entities 页面中删除服务器，并再次重新启动 DESTA。
4. 在 Managed Entities 页面中为每个 SMS 选择 CommandView 协议。这是用于登录 CommandView EVA 的 Windows 帐户用户名和密码：
   a. 打开 System Event Analyzer 界面：

      开始 --> 程序 --> Hewlett-Packard Service Tools --> Service Event Analyzer --> Service Event Analyzer

   b. 在屏幕顶部的工具栏上，单击 **Configure Webes Managed Entities** 图标。

   c. 从列表中选择您的受管系统，然后单击主机名链接。
   d. 在 Managed Entity Properties 屏幕上，从下拉菜单中选择要启用的 CommandView 协议。



   e. 应用所做更改并关闭 System Event Analyzer。

12.3.8.4.2 测试从 SMS 传送事件

要测试从 SMS 传送事件至 CMS，请执行下列操作：

1. 在 HP-SIM 中 **Remote Support and Configuration Services** 选项的 **Entitlement** 页面内，确认 SMS 及其相关 EVA 设备都已启用远程支持。
2. 在 SMS 上打开命令窗口，并执行 `wccproxy status` 命令。此命令将输出 `The WCCProxy service is running`。

3. 执行 `wccproxy test` 命令。此命令将测试事件写入到 SMS 上的 Windows 应用程序事件日志中。接着，SMS 上的 ELMC（WCCProxy 进程）应在五分钟之内读取新事件，然后将事件数据发送至 CMS 上的 WEBES。

   CMS 上的 WEBES 将会分析测试事件，并向 CMS 上的 HP SIM 和 Remote Support Client (RSC) 发送通知。

   如果您有已打开的 Web 浏览器（连接到 CMS 上的 WEBES SEA Web 界面），那么您在 Web 浏览器中也会看到问题报告结果。同样，在 HP SIM Web 界面、RSC 用户界面及 HP 远程支持后端系统中也应该出现 WEBES 问题报告（通过应用程序管理控制台 (AMC) 进行查看）。

12.4 在 ABM 上使用 CommandView 支持 EVA4400 的要求

与在阵列中安装 CommandView 的 HSV300 控制器对相比，引进的 EVA4400 包含一个新模块。该模块被称为基于阵列的管理（简称为 ABM），它具有用于访问 LAN 的网络接口。由于 ABM 无法在阵列中托管 SMI-S，所以必须在 LAN 的其他位置上托管 SMI-S，作为到阵列的代理连接。

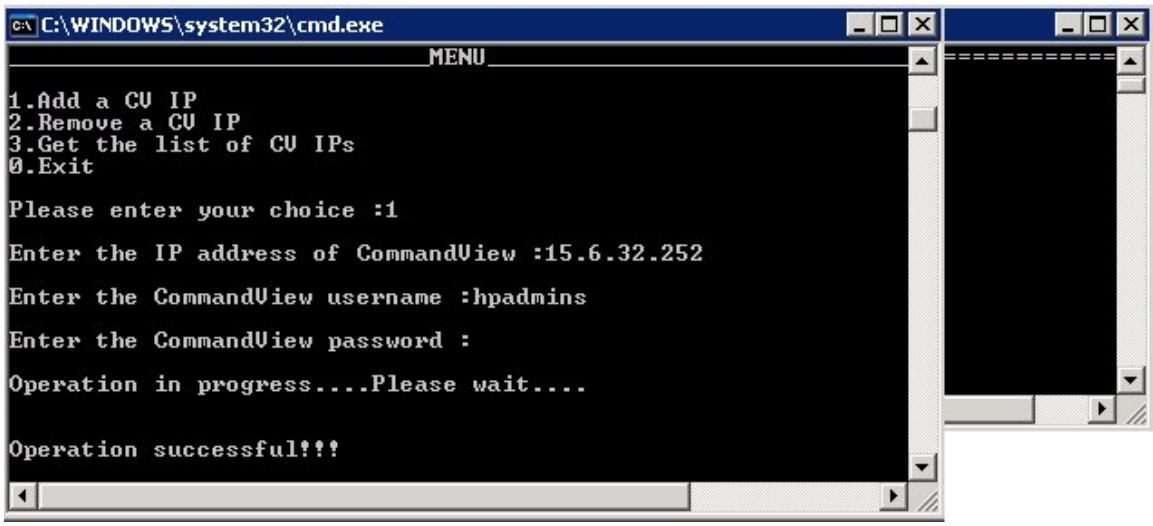
使用 CommandView 安装工具包可以将 SMI-S 独立安装到指定的服务器上。SMI-S 可以安装在 Insight Remote Support Advanced CMS 或 LAN 中另一台受支持的服务器上。本文在前面说明的端口冲突相关过程是针对在 CMS 上配置 SMI-S 这种情况，因为 HP SIM 需要通过 SMI-S 指定的端口连接到阵列。

1. SMI-S 包含一个名为 `discoverer.bat` 的实用程序，可用来配置到阵列 ABM 的连接。这样 SMI-S 就可以使用目标 ABM 的 IP 地址和凭据将连接请求发送至阵列。通过运行以下文件可调用此过程：

   ```
   C:\Program Files\Hewlett-Packard\SMI-S\EVAProvider\bin\
   discoverer.bat
   ```

   这时将打开命令窗口：

图 12-10 SMI-S ABM 配置



注释： 上例中的第一行将 `http://localhost:5988` 定义为 SMI-S 的缺省路径。如果在 CMS 上按照“端口设置”信息所述进行操作，此 http 端口可能已被更改。这是 http 端口。第二行和第三行需要为访问 HP Storage Group 而设置的帐户的凭据。输入这些项目后，就会显示菜单。

2. 选择 **1** 添加 CV IP。
3. 在 ABM 上输入 CommandView 的 IP 地址和凭据。

```
1.Add a CV IP
2.Remove a CV IP
3.Get the list of CV IPs
0.Exit

Please enter your choice :1

Enter the IP address of CommandView :15.6.32.252

Enter the CommandView username :hpadmins

Enter the CommandView password :

Operation in progress....Please wait....


Operation successful!!!
```

4. 选择 **3** 查看 CV IP 地址列表。

```
                              MENU

1.Add a CV IP
2.Remove a CV IP
3.Get the list of CV IPs
0.Exit

Please enter your choice :3

 1.2.3.4     CommandViews currently discovered by SMIS

   1.2.3.4
```

注释： 如果 CommandView 已安装到运行 discoverer 的本地主机上，您还会在此列表中看到本地主机的 IP 地址。

5. 输入 **0** 退出 discoverer 实用程序。

将 SMI-S 连接到 ABM 之后，如果在运行 SMI-S 服务的服务器上执行发现过程，HP SIM 将会发现 ABM 管理的 EVA4400 阵列。

12.4.1 WEBES 和 EVA4400

面向 ABM 的 CommandView 9.1 版包含 ABM 上运行的 ELMC (WCCProxy)。这样 WEBES 就可以成为到阵列事件数据的连接点。

当 WEBES 在 Insight Remote Support Advanced CMS 上运行时，会从 HP SIM 检索受管实体信息。需要谨记的一个关键点是：HP SIM 使用 SMI-S 提供程序并通过 WBEM 协议与阵列进行通信，而 WEBES 则使用到 ELMC (WCCProxy) 的网络连接与阵列进行通信。

请完成以下步骤，将 HP SIM 和 WEBES 设置为监控 EVA4400：

1. 首先在 WEBES UI 中设置 CommandView 协议凭据。这样可以保证在 WEBES 发现阵列和 ABM 时，能够选择正确的 ELMC 协议。
2. EVA4400 ABM 固件不包含 SNMP 或 WBEM 代理程序，所以不支持通过 HP SIM 通信来检索硬件信息。这就需要手动设置某些字段。HP SIM 系统和授权信息与 WEBES 受管实体信息密切相关。WEBES 会先检测 HP SIM 是否存在，然后将在为新添加的系统或对现有系统所做的更改而定义的 HP SIM 中检测到的信息填入受管实体。
3. 我们发现，如果缺少任何必需字段，此信息的同步会导致 WEBES 发现的实体不完整且无法恢复。这就需要从 WEBES UI 中删除受管实体，在 HP SIM 中输入所有必需信息后再重新发现受管实体。通过先停止再重新启动 DESTA_Service 可以重新发现。

12.4.2 在 HP SIM 中配置 EVA4400 和 ABM

1. 通过对运行 SMI-S 且已设置为使用 discoverer.bat 连接到 ABM 的服务器执行发现过程，或对运行 CommandView 并管理阵列的 SMS 执行发现过程，在 HP SIM 中发现 EVA4400 阵列。
2. 在 HP SIM 中编辑所发现 EVA 阵列的系统属性。包括Contract and Warranty information、Site Name 及 Primary Contact。您必须填写这些字段，HP SIM 才能在 WEBES 受管实体中显示此授权数据。EVA4400 阵列不需要 Customer-Entered Serial Number 和 Customer-Entered Model Number，因为 WEBES 会从 EVA 受管实体阵列中检索此信息。
3. 在 HP SIM 中，发现 ABM 并将 System Name 设为 ABM 的标准域名。这是 WEBES 受管实体正确检测 ABM 并将其添加为到 EVA 的连接所必需的。
4. 在 HP SIM 中编辑所发现 ABM 的系统属性。这是 HP SIM System List 中的保留位置，但 WEBES 还需要一些字段才能创建受管实体并通过远程支持授权 (RSE) 列表检查。请填写下列字段：
   - System type = Storage Device

   注释： 需要填写这些字段，WEBES 才能正确配置 ABM 实体。

   - System subtype = Storage
   - Product Model = EVA ABM

     RSE 检查需要文本 EVA。此例中已包含 ABM，以区别 HP SIM UI 中的 ABM 和阵列。

   在 CommandView 用户界面中选择 **array-name - Hardware- Controller Enclosure**，即可找到此信息。

12.5 EVA 受管系统故障排除

下面将重点说明用于支持 EVA 受管系统的故障排除解决方案。

12.5.1 HP SIM 未发现 EVA

完成下列部分：

- “确认 EVA 正由目标服务器上的 CommandView 管理”
- “SMI-S 凭据故障排除”
- “HP SIM 故障排除”

12.5.1.1 确认 EVA 正由目标服务器上的 CommandView 管理

1. 打开浏览器并转到 CommandView EVA。
2. 选择 EVA 阵列并确认您可以浏览到阵列的组件。
3. 确认 WBEM 协议已正确设置为 5989 端口，并且已根据负责管理阵列的 CommandView 的版本为 SMI-S 正确设置了用户名和密码。
   - V8 前面的 cimuser 缺省值为 administrator/administrator
   - V8 后面使用 CommandView 凭据
4. 确认 SMI-S 服务正在 SMS 上运行。
   - V8 前面的 HP StorageWorks SMI-S CIMServer。
   - V8 后面的 HP StorageWorks CIM Object Manager
5. 使用 wbemdisco.exe 测试从 CMS 到 SMI-S 的通信。请参阅“WBEMDISCO 故障排除”，了解详细信息。

12.5.1.2 SMI-S 凭据故障排除

必须将 SMI-S 和 CommandView EVA 一起安装到 SMS 上，才能在 HP SIM 和 EVA 阵列之间进行 WBEM 协议通信。CommandView EVA 工具包缺省安装 SMI-S。CommandView V8 中提供的 SMI-S 提供程序与之前 V6、V7 版本中提供的 SMI-S 提供程序有很大不同。

SMI-S 使用 CIMOM 提供程序将 WBEM 通信内容传送至 EVA 阵列。从 CommandView V8 开始，SMI-S 使用证书信任获取阵列访问权。使用相同的用户名和密码凭据登录 CommandView。在 CommandView V6 和 V7 中，SMI-S 安装时采用的用户凭据为用户名=administrator，密码=administrator。在 CommandView EVA 安装期间，如果采用自定义路径，就可以更改密码，此时会出现提示您输入密码的窗口。必须在 HP SIM System Protocol Settings WBEM Settings 中输入此用户名和密码。此通信路径会使用缺省端口 5989。

HP SIM 使用这组凭据来访问 SMI-S 的 CIMOM 接口。下列过程仅适用于 CommandView V6 或 V7 版本，不适用于 8.0.1 版或更高版本。如果此密码有问题而需要重置，或不确定 SMI-S 的用户名和密码，又或者想要添加新用户名和密码，CommandView V6 和 V7 工具包附带了一个名为 cimuser.exe 的实用程序，借助它可以列出已知的用户帐户，还可以根据需要进行添加或删除。

要使用 cimuser.exe，请执行以下操作：

1. 在 SMS 上打开命令窗口。切换至以下目录：

   ```
   C:\Program Files\Hewlett-Packard\pegasus_home\bin
   ```

2. 输入以下命令：

   ```
   cimuser -l (that is, a lower case L)
   ```

   此时将列出已知的用户。通常只会列出 administrator。

3. 使用以下命令可以删除和重新添加管理员帐户：
   - `cimuser -d -u administrator`
   - `cimuser -a -u administrator`

     系统将要求您输入并确认密码。

12.5.2 HP SIM 故障排除

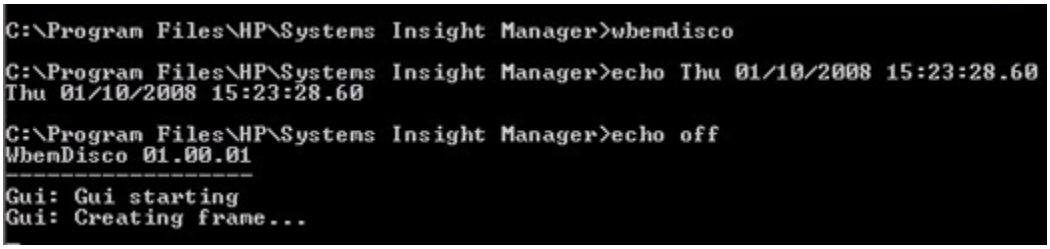
1. 配置 WEBES 受管实体（平均完成时间取决于 HP SIM 传送至 WEBES 的数据量。可能从几分钟至几小时不等）。
2. 在 WEBES SEA Web 界面中，确保 Managed Entities 列表中显示了所有 EVA 设备。
3. 在 WEBES SEA Web 界面中，确保 Managed Entities 列表中显示了所有 CommandView 服务器。如果未显示，说明未在 HP SIM 中正确发现或配置相关信息，或者该信息未从 HP SIM 正确传送至 WEBES。
4. 删除 WEBES 拥有的任何 EVA 或 CommandView 服务器受管实体，删除在 HP SIM 中发现的 SMS 系统，然后在 HP SIM 中重新开始发现和配置 SMS 信息。在 HP SIM 重新发现 SMS 系统后，或后来修改后，该信息将传送至 WEBES。
5. 开始测试。

12.5.3 WBEMDISCO 故障排除

wbemdisco.exe 工具是一个 WBEM 发现实用程序，可用于确认与 SMI-S CIMOM 组件的通信。此程序位于 CMS 上，需要从命令窗口运行。

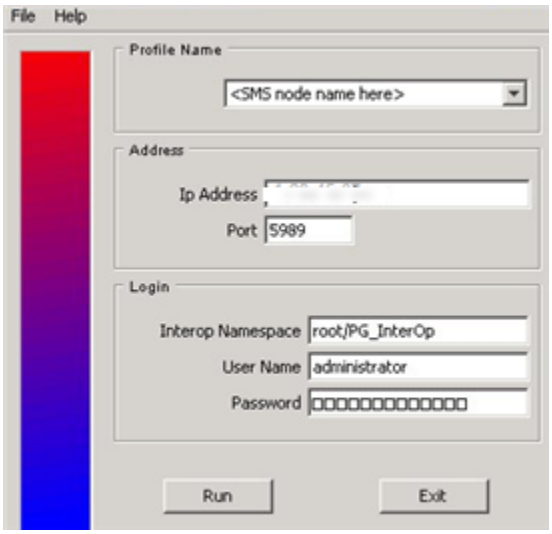
1. 在 CMS 上打开命令窗口，将目录切换至 C:\Program Files\HP\Systems Insight Manager，然后运行 wbemdisco。

图 12-11 运行 wbemdisco



2. 这时将启动其他窗口，请输入SMS节点的名称。将保留此配置文件名和设置以供将来使用。图 4-2

图 12-12 SMI-S 测试工具



3. 输入 SMS 节点的 IP 地址（SMI-S 的缺省端口是 5989）。
4. 由于 Interop Namespace 指定将 root/PG_InterOP 用作凭据管理员，所以缺省密码应该是 administrator。如果已使用 cimuser 创建了其他用户名/密码，请改用这些值。

   在 CommandView V8 中此步骤有所不同，Interop Namespace 指定为 interop，而用户名和密码凭据与 CommandView 登录中的相同。

图 12-13 SMI-S 测试工具 (CV 8)

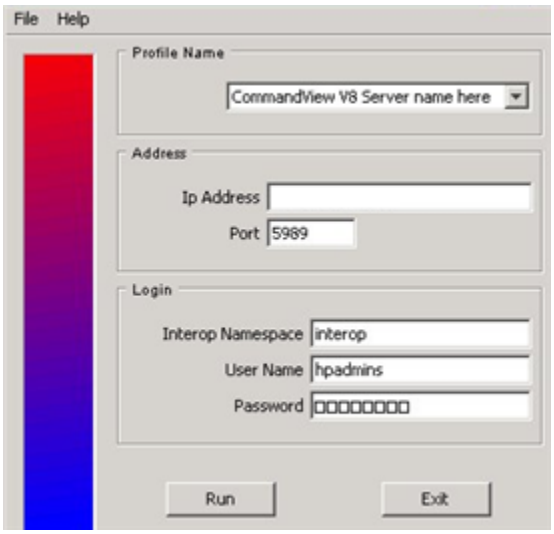
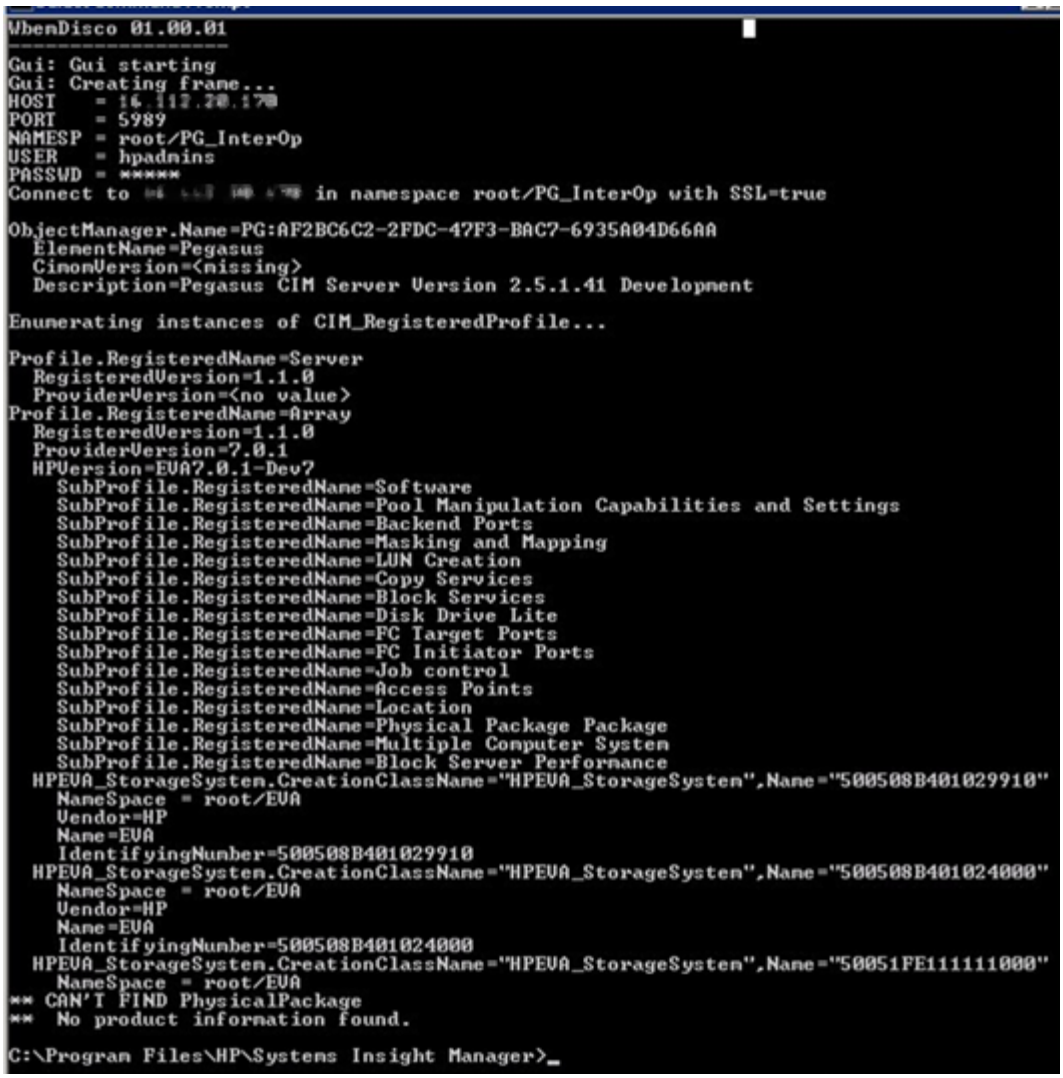


图 12-14 “wbemdisco 输出”显示执行 wbemdisco 命令的命令窗口中的成功输出：

图 12-14 wbemdisco 输出



靠近此输出顶部的 V6 和 V7 失败说明 cimuser 用户名/密码验证有问题，且不会显示此输出的大部分内容。请参阅“SMI-S 凭据故障排除”，其中介绍了 cimuser.exe 的用法。

返回的错误示例如下：

```
*** Error connecting with SSL=true - (CIM_ERR_ACCESS_DENIED) ***
```

此输出中间部分所显示的失败或错误类似于 Java 相关内存分配错误。请参阅“JAVA 内存错误”一节。

此输出结尾部分的失败（未指出 EVA 阵列 WWN 存在）表示：

- EVA 阵列目前不由此 CommandView 实例管理
- SMI-S 安装有问题，可能需要卸载/清理并重新安装 CommandView。

SMI-S 日志文件可能会显示一些失败指示，可以在以下位置查看这些指示：C:\Program Files\Hewlett-Packard\pegasus_home\logs

12.5.3.1 解决通信失败的步骤：

1. 停止并重新启动 SMI-S 服务，即 HP StorageWorks SMI-S CIMServer 或 HP StorageWorks CIM Object Manager，请参阅“停止 CIMServer”一节。
2. 停止并重新启动 CommandView 服务 HP CommandView EVA。

3. 卸载并重新安装 CommandView 套件（包括 SMI-S）。卸载后未完全删除 CommandView 和SMI-S，这是目前已知的问题。可能需要清除注册表项、文件和文件夹路径（目前正等待审核以定义这些步骤的文档）。
4. 确认 WMI Mapper 端口分配。

12.5.3.1.1 停止 CIMServer

注释： 此内容来自 CommandView 7.0 版发行说明：

停止CIMServer服务后，服务的状态在服务窗口中显示为“停止”，但服务不会停止。停止还是开始 CIMServer 服务，视您执行的 Windows 操作系统而定：

- Windows 2003:要停止 CIMServer 服务，请转至“任务管理器”，右键单击 cimserver.exe 处理程序并选择“结束进程”。要重新启动 CIMServer 服务，请打开“服务”窗口，右键单击 CIMServer，选择“所有任务”，然后选择“启动”。
- Windows 2000:要停止 CIMServer 服务，请重新启动系统。要重新启动 CIMServer 服务，请打开“服务”窗口，右键单击CIMServer，选择“所有任务”，然后选择“启动”。这是众所周知的 Windows 操作。有关详细信息，请访问：http://support.microsoft.com/kb/839174/。要避免此问题，请不要在 CIMServer 服务启动后一分钟内立即将其停止。

12.5.3.1.2 Java 内存错误：SMI-S EVA 用户的后期安装步骤

此信息记录在 CommandView 7.0.1 版和 7.0.1 版的发行说明中。

缺省情况下，会将JVMOptions.conf 文件中的 -Xmx 值设为 1024m，但这并非总是正确的值。要确定 -Xmx 的正确值，请在安装 HP StorageWorks CommandView EVA 软件套件 7.0.1 之后立即完成以下步骤：

1. 在命令行中，输入安装目录 :\Program Files\Hewlett-Packard\pegasus_home\jre\bin\java”-Xmx1024m –version。如果返回了 Java 版本号，则表示 -Xmx 的缺省值 1024m 是正确的。如果未返回 Java 版本号，请以较小的值重试命令，直到某个值返回 Java 版本为止。
2. 在位于 OS 安装目录 :\Program Files\Hewlett-Packard\pegasus_home 目录的 JVMOptions.conf 文件中，将返回 Java 版本的值添加为 -Xmx 值。

重要信息： Java 相关建议：

注意：使用旧版的 Java Runtime Environment (JRE) 时，HP StorageWorks CommandView EVA 6.X 版安装和升级不正常：

此建议的重要声明：安装机制视管理服务器上安装的最新版 JRE 而定。可以从以下 URL 下载 JRE：http://java.sun.com/javase/downloads/index.jsp

12.5.3.1.3 SMA 上的 CommandView SSO 证书：将 SSO 证书添加至 CommandView EVA 信任库

CommandView 7.0 版发行说明中记录了此信息：

1. 要在存储管理设备中将 SSO 证书添加至 CommandView EVA 信任库，请在安装 HP StorageWorks CommandView EVA 软件套件 7.0 之后完成以下步骤：导航至 \Program Files\Hewlett-Packard\pegasus_home\bin\EVAProvider 目录。执行 genEVACert.bat 文件；将会更新信任库。
2. 要确认已安装信任库，请完成以下步骤：在 CommandView EVA GUI 中，单击 Server Options。单击 Other application trust relationships。您可以查看已安装的证书。

12.5.4 SMS 上的 ELMC 安装故障排除

问题：

SMS 上的 ELMC 安装失败。此问题的可能原因是 Windows Management Instrumentation (WMI) 服务阻止访问必需的系统文件。

解决方案

具体的解决方案是使用 Windows Services Manager 实用程序停止 WMI 服务，以便解锁文件，安装 ELMC，然后重新启动 WMI 服务。

12.5.5 使用 RSCC 收集 EVA 数据前先禁用 HPCC

如果要使用 Remote Support Configuration Collector (RSCC) 来收集 EVA 数据，必须确保存储管理服务器 (SMS) 上没有运行 HP ISEE Configuration Collector (HPCC) 组件。要禁用 HPCC 组件，请执行以下操作：

1. 在 HP ISEE Configuration Collection for EVA 主机 (SMS) 上，依次选择**开始>控制面板>管理工具>服务**以显示服务列表。
2. 找到 EVA 服务的 HP ISEE Configuration Collector。右键单击并选择“属性”。
3. 从“启动类型”下拉菜单中选择**禁用**。
4. 单击**停止**，单击**确定**，再单击**关闭**。

13 Insight Remote Support Advanced 支持的 SAN 交换机与磁带库的要求

13.1 系统要求

- 在 CMS 上，必须有 WEBES 5.6 + Update 1 以及支持的虚拟和物理库才能支持光纤通道交换机和 Nearline 磁带库。利用 CMS 上的 RSSWM 应用程序，您可以下载并安装 WEBES 5.6 + Update 1（按照《Insight Remote Support Advanced CMS with WEBES 5.6 Configuration and Usage Guide》中的说明操作）。因为必须先在 CMS 上安装 WEBES 才能完成 SAN 交换机或库的配置，所以需要在完全配置 CMS 后重新阅读本节。
- 必须将所有受管系统配置为向 CMS 发送 SNMP v1 陷阱。
- 可能还需要将交换机配置为允许 CMS 与交换机之间进行 SNMP 通信。
- DCFM 所在的环境必须能够将 McData 光纤通道交换机事件转发到 CMS。

13.2 受管系统配置

CMS 上的 HP SIM 必须能够发现和识别每个光纤通道交换机或虚拟和物理库系统。

13.2.1 配置详细信息

请注意：

- 确认 HP SIM 已识别出客户环境中的每个光纤通道交换机。不要忘记将交换机应用程序配置为向 CMS 发送陷阱。
- 确认 HP SIM 已捕获交换机的正确产品编号及序列号信息。
- 对 HP SIM 中任何不正确或缺少的合同标识及客户联系信息进行修改。
- 确认已为受管设备（受管系统）选择了最合适的系统类型。

注释： 除非 HP SIM 已识别出交换机，否则将不会引发交换机事件。

13.3 SAN 交换机配置

13.3.1 Brocade SNMP 配置

请执行以下步骤配置 Brocade SNMP（包括大多数 HP StorageWorks 光纤通道交换机）：

1. 通过 Telnet 或使用 Brocade Switch Explorer 登录 CLI 界面。
2. 使用 CLI 命令 `agtcfgset` 或更新的 `snmpconfig` 进入 SNMP 配置模式。
3. 如果选择了非标准陷阱团体名称（例如，除 `public` 外的名称），请确保 CMS 上的 HP SIM 可以识别此名称。
4. 在其中一个陷阱目标设置中输入 CMS 的 IP 地址。
5. 设置 **mibCapability** 以启用 `SW-TRAP`、`FA-TRAP` 和/或 `HA-TRAP` MIB 陷阱（必须使用 CLI 执行此任务）。
6. 如果访问控制列表含有任何条目，请确保 CMS 的域也包含在此列表中。也可以通过交换机的内嵌 Web 界面完成此配置。请参阅交换机配置手册，了解如何配置陷阱严重性级别和 MIB 功能的详细信息（如果需要）。
7. 在受管系统页面中输入详细信息，并为 Brocade 品牌的交换机选择 **B series FC switch** 系统类型，或者为 HP StorageWorks 光纤通道交换机选择 **FC switch**。《HP Insight Remote Support Advanced CMS 配置与使用指南》 的第 5 章中说明了此过程。

13.3.2 Cisco 光纤通道交换机 SNMP 配置

请执行以下步骤配置 Cisco SNMP：

1. 通过 Telnet 或使用 Fabric Manager 登录 CLI 界面。

2. 使用 CLI 命令 `config t` 和 `snmp-server host <IP> traps version 1 public udp-port 162` 将 CMS IP 地址作为陷阱目标添加。
3. 选择让所有事件以陷阱的形式返回。
4. 如果选择了非标准陷阱团体名称（例如，除 `public` 外的名称），请确保 CMS 内部设置页面上已包含此名称。
5. 在其中一个陷阱目标设置中输入 CMS 的 IP 地址。也可以通过 Cisco Device Manager 完成此配置。
6. 在 CMS 的受管系统页面中输入详细信息，并为 Cisco 品牌的交换机选择 **C-series FC switch** 系统类型。

13.3.3 配置 McDATA 光纤通道交换机（M 系列）

DCFM 10.3.0 服务器是装有 DCFM 应用程序的 PC 设备。此应用程序以前称为 HAFM 或 EFCM。只有 DCFM 10.3.0 版或更高版本才能将事件发送至 CMS。此应用程序提供操作和管理 M 系列光纤通道交换机的界面，并可通过 HTTP 将交换机事件数据转发至 CMS。请按照以下步骤配置 DCFM，并将 DCFM 服务器与 CMS 连接。

1. 在 DCFM **Discover →Setup** 菜单中找到 McData 交换机。
2. 访问 Call home 配置菜单 **Monitor → Event Notification → Call home**。
3. 在产品列表下方选择 McData 交换机，然后将其添加到 Call Home 窗格的 HP LAN 部分。
4. 单击 **Edit Center**，然后将 CMS 的 IP 地址添加为 **Service Gateway**。
5. 应用设置，如果想要测试连接情况，可以单击 **Send Test** 按钮。
6. 单击 **Call Home** 对话框中的 **Apply**，或者单击 **OK**。

   无需应用任何 Call Home 过滤器。
7. 最后，转至各个 M 系列受管设备并启用 **phone home**。

13.3.3.1 HP QLogic 交换机配置

通过 Telnet 登录交换机，并发出以下 CLI 命令来配置 HP 8/20q 或 2/8q 光纤通道交换机，以便将 SNMP 陷阱发送至 CMS。

```
Admin begin
Set setup SNMP (configure the trap destinations)
“y” to save and activate the configuration
Admin end
```

13.3.3.2 HP VC-FC 虚拟连接模块配置

请执行以下步骤，配置 HP VC-FC 虚拟连接模块：

1. 登录 On-Board Administrator，然后在左侧窗格中选择 Virtual Connect manager。
2. 处于 VC 管理器中后，选择左侧的 SNMP 设置选项。
3. 在 **SNMP alert destination** 部分，输入 CMS 的 IP 地址和团体名称。请注意，只能在 VC 管理器中输入一个目标 IP 地址。相同的目标将应用于由所选 OA 控制的所有 VC-FC 模块。
4. 在 CMS Managed Systems 页面中输入详细信息，并为 HP StorageWorks 虚拟连接光纤通道交换机模块的系统类型选择 **FC switch**。

13.3.4 VLS/ETLA/MCS MSL G-3 SNMP 配置

13.3.4.1 CV-TL 和 CV-VLS SNMP 配置

1. 登录每个 VLS/ETLA 的 Command View VLS/TL Web 界面。
2. 单击 **Notifications** 选项卡。
3. 单击 **Edit SNMP settings** 任务。
4. 在 **Hostname** 字段中，输入 CMS 的 IP 地址或名称。
5. 除非已定义其他团体字符串，否则请输入 **public** 作为 Community String。

6. 陷阱版本为 1。
7. 单击 **Add**。

13.3.4.2 CV-MSL SNMP 配置

1. 以 **Administrator** 身份登录 Command View MSL Web 界面。
2. 单击 **Configurations** 选项卡。
3. 单击 **Network Management** 选项卡。
4. 确认已选择 **SNMP**。
5. 在 **IPv4 target address** 字段中输入 CMS 的 IP 地址。
6. 确认已选择版本 SNMPv1。
7. 选择 **Critical and Warnings** 作为过滤级别。
8. 单击 **Submit**。

13.3.5 测试配置

注释： 请勿提供冗余的 FRU 来测试所支持交换机或库的配置。

13.3.5.1 测试 Cisco 交换机配置

Cisco 最近引入了 CLI 测试命令，可用于验证设备的端到端事件连通性。

1. 在 CLI 提示符下发出以下命令：

   test pfm test-SNMP-trap power

2. 这会导致Cisco交换机将欺骗性的**错误**电源事件发送至CMS。如果所有项目均已正确配置，此事件将生成 HP 可以查看的事件。

注释： 您也可以使用 test pfm test-SNMP-trap fan，但如果使用的话，将会忽略 temp 类型事件。

13.3.5.2 测试 VLS 配置

使用最新版的VLS固件和Command View VLS，找到CV-VLS SNMP配置页面上的**Test SNMP**按钮以执行端到端测试。此测试事件将不会在 HP 中创建任何实例，但会创建本地电子邮件通知，以便确认 VLS SNMP 和 CMS 均已正确配置。

13.4 Nearline（磁带库）配置

磁带库 RSS 和 RSA 配置使用 HP Command View 管理工具

13.4.1 CV-TL SNMP 配置

1. 登录每个 ESL 或 EML 的 Command View TL Web 界面。
2. 单击 **Configuration** 选项卡。
3. 在左侧面板中，选择 **SNMP Alerts**。当前的 SNMP 陷阱会显示在右侧面板中。
4. 执行以下某个操作：
   - 在右侧面板中，右键单击 SNMP 陷阱，然后选择 **Add Trap Entry**。

     或者

   - 选择 **Actions → Add Trap Entry**。
5. 此时会出现 **SNMP Trap Entry** 对话框。
6. 在 **Trap Destination** 字段中，输入 WEBES 主机 IP 地址或名称。
7. 除非已定义其他团体字符串，否则请输入 **public** 作为 **Community String**。
8. 最后，请单击 **OK**。

13.4.2 CV-VLS SNMP 配置

1. 登录每个 VLS 节点的 Command View VLS Web 界面。
2. 单击 **Notifications** 选项卡。
3. 单击 **Edit SNMP settings** 任务。
4. 在 **Hostname** 字段中，输入 WEBES 主机 IP 地址或名称。
5. 如果选择了非标准陷阱团体名称（例如，除 `public` 外的名称），请确保 CMS 上的 HP SIM 可以识别此名称。
6. 陷阱版本为 `1`。
7. 最后，请单击 **Add**。

13.4.3 CV-MSL (MSL G3) SNMP 配置

1. 以 `Administrator` 身份登录 Command View MSL Web 界面。
2. 单击 **Configuration** 选项卡。
3. 单击 **Network Management** 选项卡。
4. 确保已选择 **SNMP**。
5. 在 **Ipv4 target** 地址字段中输入 WEBES 主机的 IP 地址。
6. 确保已选择版本 **SNMPv1**。
7. 选择 **Critical and Warning** 作为过滤级别。
8. 单击 **Submit**。

13.4.4 测试配置

我们不建议您提供冗余的 FRU 来测试配置。如果您已有最新版的 VLS 固件和 Command View VLS，则可以使用 CV-VLS SNMP 配置页面上的 **Test SNMP** 按钮执行端到端测试。此测试事件将不会在 HP 中创建任何实例，但会创建本地电子邮件通知，以便确认 VLS SNMP 和 WEBES 均已正确配置。

14 配置 MSA 受管系统，使其支持基于目标的 SNMP

必须执行下列操作，才能监控模块化智能阵列 (MSA)：

- 参阅 《A.05.40 Insight Remote Support Advanced Release Notes》 ，确认系统受支持。
- 确认已在受管系统上正确配置了 SNMP。

14.1 关于 MSA 基于目标的 SNMP 支持

下列几种模块化智能阵列 (MSA) 使用基于目标的 SNMP 支持来监控 Insight Remote Support Advanced。

- 1510i
- 2012 和 2112
- 23xx

MSA 的每种受管系统应在出厂时就安装了 SNMP。要获取基于目标的支持，需要在支持的 Web 浏览器中使用单独的界面配置 SNMP，以支持上述系统类型。

14.2 关于 MSA 基于目标的 SNMP 支持

下列几种模块化智能阵列 (MSA) 使用基于目标的 SNMP 支持来监控 Insight Remote Support Advanced。

- 1510i
- 2012 和 2112
- 23xx

MSA 的每种受管系统应在出厂时就安装了 SNMP。要获取基于目标的支持，需要在支持的 Web 浏览器中使用单独的界面配置 SNMP，以支持上述系统类型。

14.2.1 MSA 1510i

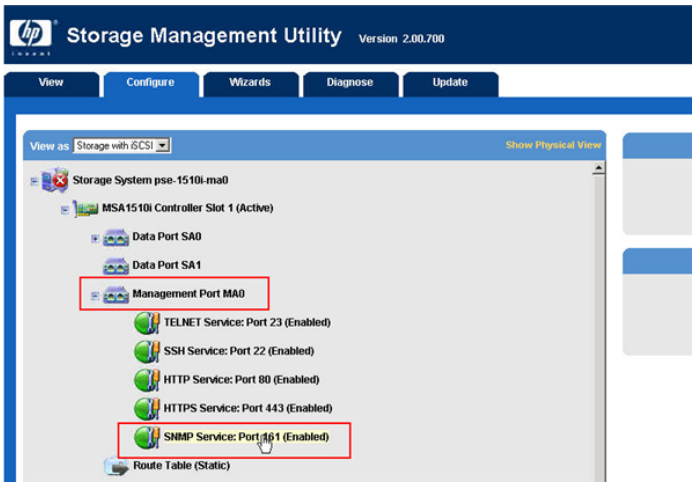
要访问 MSA 1510i 并配置 SNMP 以支持 Insight Remote Support Advanced，请完成以下步骤：

1. 登录 HP StorageWorks MSA Storage Management Utility

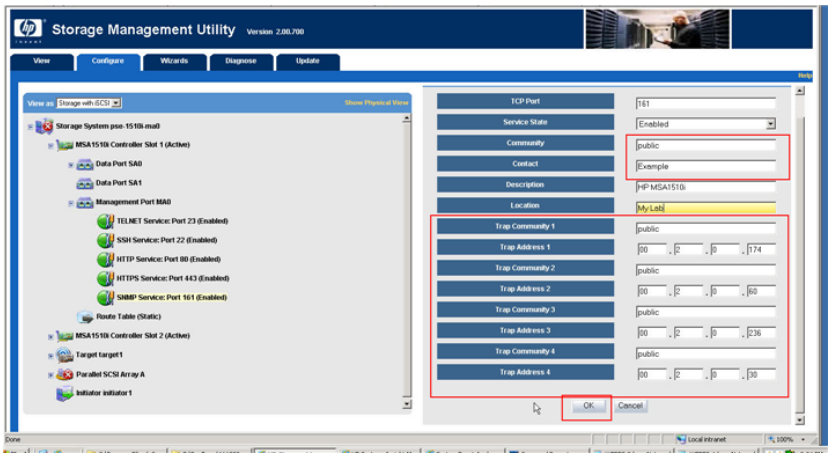
注释： 有关设置此工具和管理凭据的基本信息，请参阅 StorageWorks 文档。

2. 登录此实用程序后，选择 **Configure** 选项卡。

3. 在 **Configure** 选项卡上，展开 MSA 1510i 的 **Management Port** 列表。
4. 从列表中选择 **SNMP Service** 链接。



5. 修改所有必需的配置字段，并确保 CMS 的 IP 地址已列为 **Trap Address**。
6. 单击 **OK** 应用所做的更改。



7. 退出此实用程序并确认 HP SIM 已在 CMS 上发现您的 1510i。

14.2.2 MSA 2012 或 2112 系列

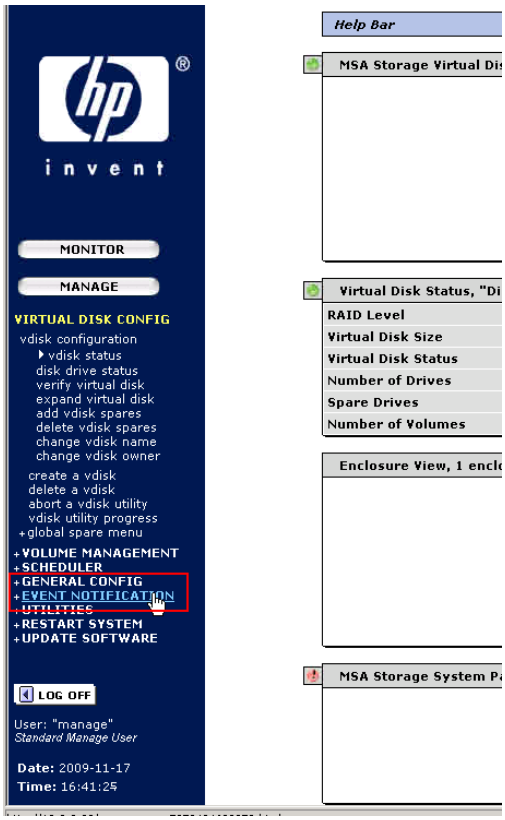
要访问 MSA 2012 或 2112 并配置 SNMP 以支持 Insight Remote Support Advanced，请完成以下步骤：

1. 登录 HP StorageWorks MSA Storage Management Utility

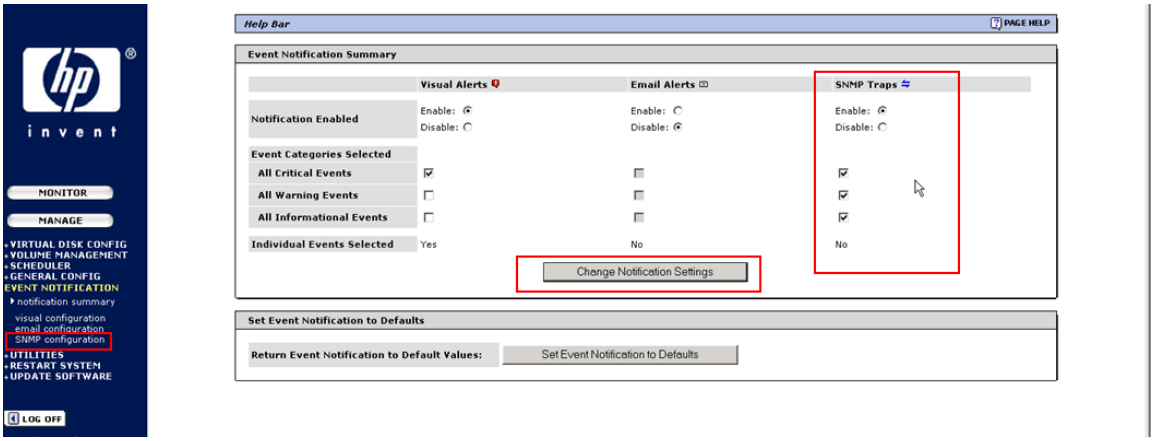
注释： 有关设置此工具和管理凭据的基本信息，请参阅 StorageWorks 文档。

2. 登录此实用程序后，选择 **Manage** 按钮。

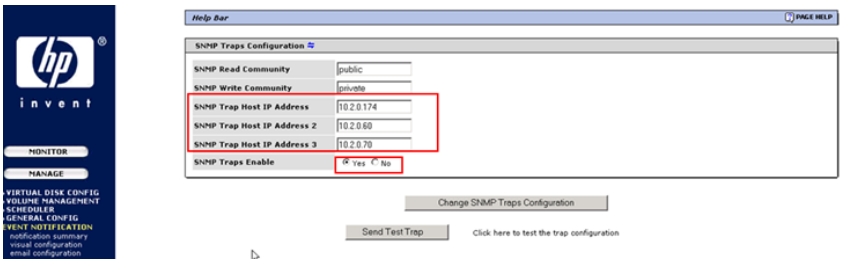
3. 在展开的列表中选择 **Event Notification** 链接。



4. 在 **Event Notification** 页面上，确认 SNMP 通知类型（三种均为推荐类型）已激活，然后单击 **Change Notification Settings** 应用所做的更改。



5. 在左侧面板列出的 **Event Notification** 下，单击 **SNMP configuration** 链接。
6. 修改 SNMP 设置使其包含作为测试陷阱主机的 CMS，并确保将 **SNMP Test Traps Enabled** 单选按钮设为 **Yes**。



7. 单击 **Change SNMP Test Traps Configuration** 应用所做的更改。

注释： 如果您的 Insight Remote Support Advanced CMS 已完全配置，您可以从此页面发送测试事件。如果尚未配置 CMS，您可以稍后返回此页面以发送测试事件。

8. 退出此实用程序并确认 HP SIM 已在 CMS 上发现您的 2012/2112。

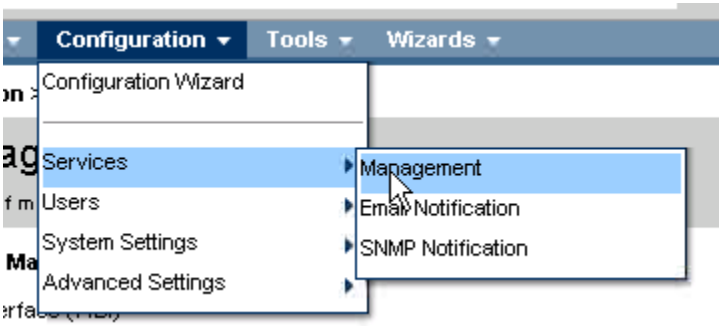
14.2.3 MSA 23xx 系列

要访问 MSA 23xx 并配置 SNMP 以支持 Insight Remote Support Advanced，请完成以下步骤：

1. 登录 Storage Management Utility

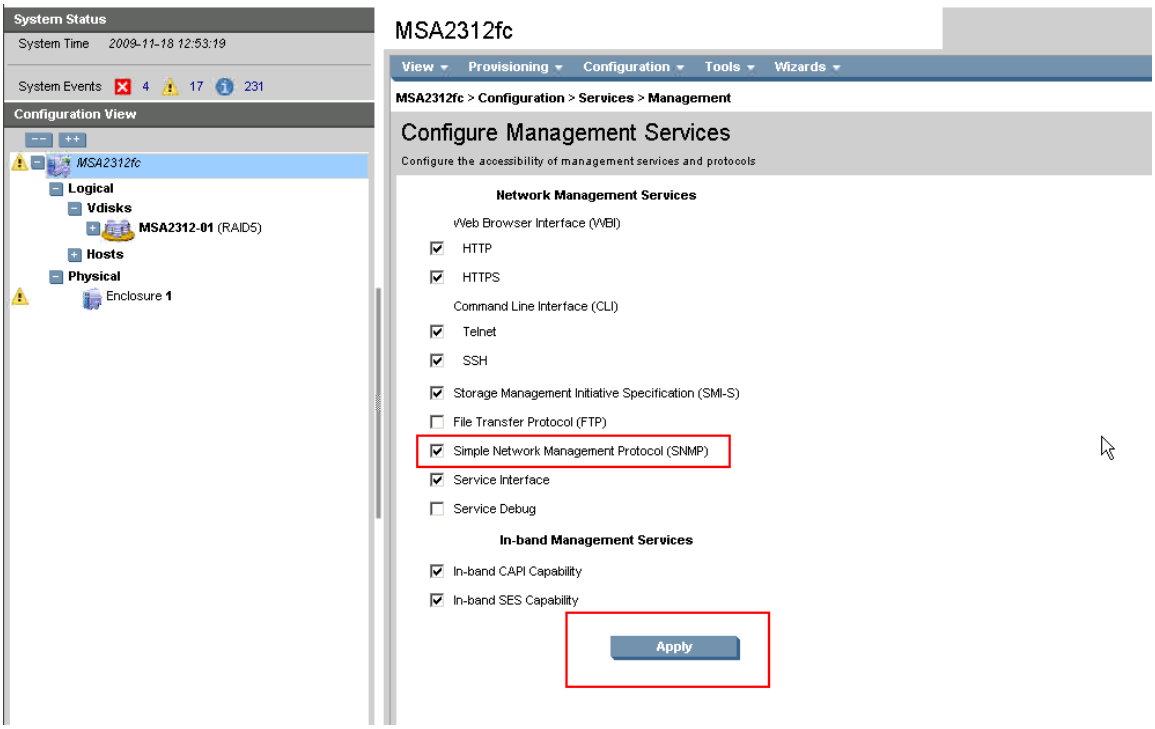
注释： 有关设置此工具和管理凭据的基本信息，请参阅 StorageWorks 文档。

2. 登录此实用程序后，依次选择 **Configuration > Services > Management**。

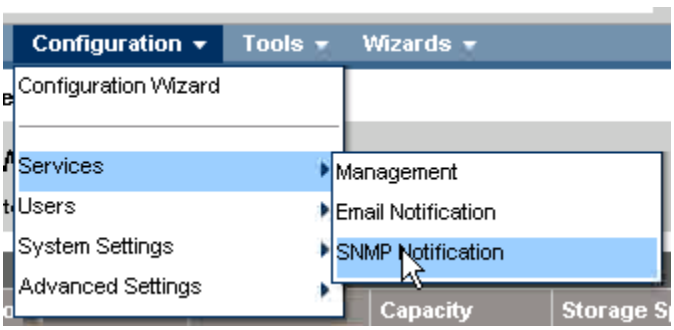


3. 确保已从 **Network Management Services** 列表中选择 SNMP，然后单击 **Apply**。

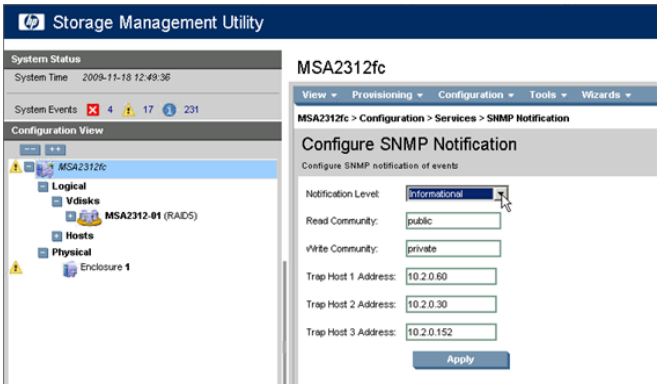
重要信息： 缺省情况下 SNMP 应处于激活状态，如果由于某种原因而未激活，将不支持 Insight Remote Support Advanced。必须验证 SNMP 是否已激活。



4. 从菜单中依次选择 **Configuration → Services → SNMP**。



5. 在 **Configure SNMP Notification** 页面上修改 SNMP 设置，使其包含作为测试陷阱主机的 CMS，并从下拉菜单中选择 **Notification Level**（建议选择信息级别）。



6. 单击 **Apply** 应用所做的更改。
7. 退出此实用程序并确认 HP SIM 已在 CMS 上发现您的 23xx。

15 配置基于主机的 MSA

必须执行下列操作，才能监控基于主机的 MSA：

- 参阅 《A.05.40 Insight Remote Support Advanced Release Notes》 ，确认托管系统是受支持的受管系统。
- 确认已使用 OpenVMS 或 Tru64 Unix 将托管系统正确配置为受管系统，并且是根据本文档对应章节的说明配置的。

如果已经按照制造商的说明书正确配置了 MSA，那么它应该可以与主机进行通信。如果已经按照本文档所述将主机正确配置成受管系统，主机/受管系统就可以将您的 MSA 事件信息发送至 CMS 以获取远程支持。

词汇表

Event Log Monitoring Collector (ELMC)	ELMC（以前称为 WCCProxy）用于检测事件日志的错误状况并将这些事件发送给 WEBES。
HP System Management Homepage (SMH)	HP System Management Homepage (SMH) 是一种基于 Web 的界面，它整合并简化了在 HP-UX、Linux 和 Windows 操作系统上对 HP 服务器进行单系统管理的过程。
HP Systems Insight Manager (HP SIM)	HP Systems Insight Manager (HP SIM) 是统一的服务器与存储管理平台。系统管理员从一个管理控制台即可使用安全管理工具集来管理整个 HP 服务器与存储环境。
HP 金牌服务	HP 金牌服务可随 HP 产品与服务一起购买，以通过增强的支持包升级或延长标准保修。通过从基本到关键的支持级别，它们可以降低停工的风险。 许多产品在原来的保修到期后，还可以获得续保 HP 金牌服务。
Insight Remote Support Advanced	Insight Remote Support Advanced 提供主动式远程监控、诊断和故障排除，以帮助提高数据中心内 HP 支持的服务器与存储系统的可用性。HP 远程支持通过系统支持来降低成本和复杂程度。HP 远程支持将硬件事件信息通过防火墙和/或 Web 代理安全地传送到 HP 支持中心以进行响应式支持。此外还会根据支持协议的规定，收集系统信息进行主动分析与服务。
Internet 协议 (IP)	指定数据包（封包）的格式，以及网络上的地址解析方案。大多数网络会将 IP 与传输控制协议 (TCP) 结合在一起，在目的地与来源之间建立虚拟连接。
OSEM (Open Service Event Manager)	安装在 CMS 上的远程支持组件，可通过产品的专属规则集来执行实时服务事件过滤与分析。改进功能推出后，这些规则集会定期更新。
Remote Support Software Manager (RSSWM)	HP Remote Support Software Manager 是安装在 CMS 上的应用程序，并附带下载和安装 Insight Remote Support Advanced 组件所需的 HP SIM。
标识	发现过程的一个阶段，用于标识管理协议和系统类型。
存储管理服务器 (SMS)	安装了 HP StorageWorks 企业虚拟阵列 (EVA) 软件的系统，包括 HP Command View EVA 和 HP Replication Solutions Manager（如果使用）。它是独占运行 EVA 管理软件的专用管理服务器。
存储区域网络 (SAN)	存储区域网络 (SAN) 是由存储设备构成的网络，它也是存储和检索这些设备（包括通信基础设施）上信息的发起方。在大型企业中，SAN 会将多个服务器连接至磁盘存储集中池。与管理数百台有各自磁盘的服务器相比，SAN 加强了对系统的管理。
发现	管理应用程序的一项功能，用于查找和识别网络对象。在 HP 管理应用程序中，发现功能会查找并识别指定网络范围内的所有 HP 系统。
基于 Web 的企业服务 (WEBES)	安装在 CMS 上的远程支持组件，可通过产品的专属规则集来执行实时服务事件分析。改进功能推出后，这些规则集会定期更新。
基于 Web 的企业管理 (WBEM)	基于 Web 的企业管理 (WBEM) 是为统一管理分布式计算环境而开发的一组管理技术和 Internet 标准技术。 WBEM 实质上是一项业界倡议，用来将不同平台间的管理信息进行标准化。
集合	使用 HP SIM 时，一种分组搜索系统或事件的方法。
简易网络管理协议 (SNMP)	HP Systems Insight Manager 支持的管理协议之一。网络系统与多数服务器广泛使用的传统管理协议。MIB-2 是可以持续供所有供应商使用的标准信息。
配置数据集合	HP SIM 使用术语**集合**来表示受管系统组，而 Insight Remote Support Advanced 则使用术语**配置集合**表示从受管系统收集的数据。这些数据将发送给 HP 进行主动分析。
企业虚拟阵列 (EVA)	EVA 是针对高端企业环境的一种高性能、高容量、高可用性虚拟 RAID 存储解决方案。
系统	通过 TCP/IP 或 IPX 进行通信的网络节点。要管理系统，系统上必须有某些类型的管理协议（例如 SNMP、DMI 或 WBEM）。例如服务器、工作站、台式机、便携式装置、路由器、交换机、集线器和网关等，都可称作系统。

系统故障管理 (SysFaultMgmt 或 SFM)	SFM 是实施 WBEM 标准的 HP-UX 故障管理解决方案。SysFaultMgmt 与其他易于管理的应用程序（如 HP SIM 和 HP SMH）以及其他任意基于 WBEM 的客户端（如 WEBES）集成在一起。
拥有完整配置权限的用户	自动获得授权，可使用所有系统（包括 CMS）上 **All Tools** 工具箱的用户。此类用户已获得管理 HP Systems Insight Manager 软件的特殊权限。
用户	能够有效登录 CMS 且已添加至 HP Systems Insight Manager 的网络用户。
域名服务 (DNS)	一种将域名翻译成 IP 地址的服务。
远程支持服务	通过远程支持服务，可以为企业的任意和所有合格系统启用或禁用远程支持。远程支持服务还会显示合格系统的远程支持授权检查状态，并且您可以通过该服务访问远程支持授权检查。
远程支持合格系统	运行 Windows 2003 或 Linux Red Hat 的 HP ProLiant 服务器是合格系统，启用时会将事件提交给 HP 支持中心来解决。系统还必须具备接受远程支持的资格，否则将会关闭提交的事件。您可以使用远程支持服务中的远程支持授权检查来验证合格的系统确实受支持。
远程支持设置	远程支持设置是一个集合点，集合了贵公司的企业合同信息、指定的企业支持联系人信息，以及 HP 客户服务团队的联系信息。
远程支持授权检查 (RSEC)	RSEC 是一种检查，负责检查 HP 授权数据存放区中特定系统的当前义务状况。RSEC 窗口显示远程支持授权检查的结果，通过 **Remote Support Services** 选项卡中的 **Support Obligation** 列可访问此窗口。
中央管理服务器 (CMS)	管理域中执行 HP Systems Insight Manager 软件的系统。HP Systems Insight Manager 中的所有核心操作都是从该系统中启动的。

索引