HP SiteScope

软件版本： 11.30

部署指南

文档发布日期： 2015 年 5 月
软件发布日期： 2015 年 3 月

法律声明

担保

HP 产品和服务的唯一担保已在此类产品和服务随附的明示担保声明中提出。此处的任何内容均不构成额外担保。HP 不会为此处出现的技术或编辑错误或遗漏承担任何责任。

此处所含信息如有更改，恕不另行通知。

受限权利声明

机密计算机软件。必须拥有 HP 授予的有效许可证，方可拥有、使用或复制本软件。按照 FAR 12.211 和 12.212，并根据供应商的标准商业许可的规定，商业计算机软件、计算机软件文档与商品技术数据授权给美国政府使用。

版权声明

商标声明

Adobe® 和 Acrobat® 是 Adobe Systems Incorporated 的商标。

Intel®、Pentium® 和 Intel® Xeon® 是 Intel Corporation 在美国和其他国家/地区的商标。

iPod 是 Apple Computer, Inc. 的商标。

Java 是 Oracle 和/或其附属公司的注册商标。

Microsoft®、Windows®、Windows NT® 和 Windows® XP 是 Microsoft Corporation 在美国的注册商标。

Oracle 是 Oracle Corporation 和/或其附属公司的注册商标。

UNIX® 是 The Open Group 的注册商标。

文档更新

此文档的标题页包含以下标识信息：

- 软件版本号，用于指示软件版本。
- 文档发行日期，该日期将在每次更新文档时更改。
- 软件发布日期，用于指示该版本软件的发布日期。

要检查是否有最新的更新，或者验证是否正在使用最新版本的文档，请访问：**https://softwaresupport.hp.com**

需要注册 HP Passport 才能登录此站点。要注册 HP Passport ID，请访问：**https://hpp12.passport.hp.com/hppcf/createuser.do**

或单击 HP 软件支持页面顶部的“Register”链接。

此外，如果订阅了相应的产品支持服务，则还会收到更新的版本或新版本。有关详细信息，请与您的 HP 销售代表联系。

支持

请访问 HP 软件联机支持网站：**https://softwaresupport.hp.com**

此网站提供了联系信息，以及有关 HP 软件提供的产品、服务和支持的详细信息。

HP 软件联机支持提供客户自助解决功能。通过该联机支持，可快速高效地访问用于管理业务的各种交互式技术支持工具。作为尊贵的支持客户，您可以通过该支持网站获得下列支持：

- 搜索感兴趣的知识文档
- 提交并跟踪支持案例和改进请求
- 下载软件修补程序
- 管理支持合同
- 查找 HP 支持联系人
- 查看有关可用服务的信息
- 参与其他软件客户的讨论
- 研究和注册软件培训

大多数提供支持的区域都要求您注册为 HP Passport 用户再登录，很多区域还要求用户提供支持合同。要注册 HP Passport ID，请访问：

https://hpp12.passport.hp.com/hppcf/createuser.do

要查找有关访问级别的详细信息，请访问：

https://softwaresupport.hp.com/web/softwaresupport/access-levels

HP Software Solutions Now 访问 HPSW 解决方案和集成门户网站。此网站将帮助您寻找可满足您业务需求的 HP 产品解决方案，包括 HP 产品之间的集成的完整列表以及 ITIL 流程的列表。此网站的 URL 为 **http://h20230.www2.hp.com/sc/solutions/index.jsp**

内容

第 1 部分: SiteScope 简介

第 1 章: SiteScope 概述

HP SiteScope 是一个无代理监控解决方案，旨在确保分布式 IT 基础结构（例如，服务器、操作系统、网络设备、网络服务、应用程序和应用程序组件）的可用性和性能。

此基于 Web 的基础结构监控解决方案轻巧、可高度自定义，并且不要求在生产系统上安装数据收集代理。通过使用 SiteScope，您可以获得用于验证基础结构操作的实时信息，时刻关注问题所在，从而在问题变得严重之前将它们解决掉。

SiteScope 提供了多种工具（例如，模板、发布模板更改向导和自动模板部署），支持您将标准化的监控器类型及配置集合部署到单个结构中。可以在整个企业中快速地部署和更新 SiteScope 模板，以确保对基础结构的监控与模板中的标准集合相符合。

SiteScope 还包括可用于在多种媒体中通信和记录事件信息的警报类型。您可以自定义警报模板以满足您组织的需要。

SiteScope 还可用作其他 HP 产品/服务（例如 Business Service Management (BSM)、Network Node Manager i (NNMi)、HP Software-as-a-Service 和 LoadRunner/Performance Center）的监控基础。以 SiteScope 为基础，并添加 BSM 服务水平管理的等其他 HP 解决方案，可以创建坚实的基础结构监控，以便从企业的角度管理 IT 基础结构和服务水平。

SiteScope 还可与 HP Operations Manager (HPOM) 产品一起使用，提供强大的无代理和基于代理的基础结构管理系统组合。作为 HPOM 的代理，SiteScope 目标会自动添加到 Operations Manager 服务视图映射中。通过此映射，HPOM 可以无缝显示 SiteScope 数据和监控器状态。对于事件集成，会直接向 HPOM 发送 SiteScope 警报和监控器度量状态更改。无代理和基于代理的监控器的组合功能可提供强大而详细的监控解决方案。有关使用 HPOM 产品的详细信息，请参阅 HPOM 文档。

第 2 章: SiteScope 版本

本章包括:

SiteScope 版本概述

SiteScope 有各种版本，各个版本提供不同的功能。

SiteScope 安装时内置了“社区”版许可证，可无限期免费使用 SiteScope 的部分功能。另外，一次性的“试用”版可在 30 天内免费使用 SiteScope 的全部功能。

通过将社区版升级到下面的某个商业版，可扩展 SiteScope 的功能：“高级版”、“旗舰版”或“系统收集器版”。还提供了在安装 HP SiteScope for Load Testing 后立即可用的免费“负载测试”版。社区版、高级版和旗舰版对任何用户均可用，但系统收集器版和负载测试版分别随 HP Operations Manager 集成和 HP Load Runner/Performance Center 提供。

您可以通过导入额外许可证添加 SiteScope 功能和容量。这样可以灵活有效地扩展 SiteScope 以满足您的组织和基础结构的需求。有关购买许可证或额外许可证容量的详细信息，请与您的 HP 销售代表联系或使用 HP SiteScope 产品页面中的“Contact Us”链接。

有关许可的详细信息，请参阅SiteScope 许可证 (第 21 页)。

功能比较表

下表显示了 SiteScope 各版本中可用的功能。

功能	SiteScope 版本			仅随 HP 产品提供	
	共同体	试用版	高级版/ 旗舰版	系统收集器版	负载测试版
许可证持续时间	瞬时启动（永久）	30 天	限期 或永久	限期或永久	瞬时启动（永久）
许可证授权模式	25 个 OSI 25 个 URL （固定容量）	25 个 OSI 25 个 URL 10 个事务 （固定容量）	OSI、URL、事务 （数量由用户确定）	OSI （数量由用户确定）	25 个 OSI 25 个 URL （固定容量）
节点锁定[1]	x	x	✔	✔	x

功能	SiteScope 版本			仅随 HP 产品提供	
	共同体	试用版	高级版/旗舰版	系统收集器版	负载测试版
支持模型	SiteScope 社区	Web/电话	Web/电话	Web/电话	电子邮件
用户帐户	1	无限制	无限制	无限制	无限制
数据保留	30 天[2]	30 天[2]	无限制	无限制	无限制
警报	仅限电子邮件和事件控制台	✔	✔	✔	✔
报告	仅限快速报告	✔	✔	✔	✔
Multi-View、事件控制台	✔	✔	✔	✔	✔
分析	✔	✔	✔	✔	✔
监控器类型	除社区版中不包含的监控器 (第 13 页)中列出的监控器外的所有监控器。	所有监控器	所有监控器	所有监控器	除 Web 脚本监控器和集成监控器外的所有监控器
解决方案模板	x	所有解决方案模板	所有解决方案模板	所有解决方案模板	HP Quality Center、HP QuickTest Professional、HP Service Manager、HP Vertica、操作系统主机（AIX、Linux、Microsoft Windows、Solaris）
用户定义的模板	✔ 不含通过 CSV 或 XML 文件进行部署	✔	✔	✔	✔
API	x	✔	✔	✔	✔
集成	x	✔	✔	✔	常规数据集成
高可用性（故障转移）	x	x	✔	✔	x
更新和修补程序	x	x （可通过修补程序进行更新）	✔	✔	✔
支持的平台（安装）	多种 64 位 Windows 和 Linux 平台（请参阅系统要求 (第 52 页)了解支持的版本列表）。				

功能	SiteScope 版本			仅随 HP 产品提供	
	共同体	试用版	高级版/ 旗舰版	系统收集器版	负载测试版
多语言 UI 支持	10 种语言（请参阅《使用 SiteScope》指南的“国际化”部分中支持的语言列表）。				

[1] 部分许可证版本使用节点锁定，以避免出现许可证滥用现象。这意味着，许可证只在特定计算机上有效。

[2] 在日志首选项中对每日日志数进行的配置不会影响保留的每日日志数。

社区版中不包含的监控器

- Active Directory 复制监控器
- Amazon Web Services 监控器
- COM+ 服务器监控器
- HP Vertica JDBC 监控器
- 集成监控器
- Microsoft Exchange 监控器 - Microsoft Exchange 2007 消息通信、Microsoft Exchange、 Microsoft Exchange Base（弃用监控器：Microsoft Exchange 5.5/2000/2003 消息通信、Microsoft Exchange 2003 邮箱、Microsoft Exchange 2003 公用文件夹）
- Microsoft Lync 监控器 - 存档服务器、A/V 会议服务器、 导向服务器、边缘服务器、前端服务器、中介服务器、监控和 CDR 服务器及注册表服务器
- Oracle 数据库 解决方案模板 - Oracle 10g Application Server、Oracle 9i Application Server、Oracle 数据库监控器
- SAP 监控器 - SAP CCMS、SAP CCMS Alert、SAP Java Web Application Server、SAP Performance、SAP Work Processes
- Siebel 监控器 - Siebel Application Server、Siebel 日志、Siebel Web Server
- VMware 数据存储监控器
- VMware Host 监控器 - VMware 主机 CPU、 VMware 主机内存、VMware 主机网络、 VMware 主机状态、VMware 主机存储
- WebLogic Application Server 监控器
- Web 脚本监控器
- WebSphere 监控器 - WebSphare Application Server、WebSphare MQ Status、WebSphere Performance Servlet 监控器

社区版

社区版可免费无限期地提供 SiteScope 的有限功能。此版本会在执行 SiteScope 常规安装之后自动激活。

备注: 并非每次发布 SiteScope 次版本或次次版本时都会发布社区版。有关版本类型的详细信息，请参阅安装版本类型 (第 72 页)。

下表显示了社区版和 SiteScope 商业版之间的部分主要差异。

功能	描述
许可证持续时间	**社区版：** 此版本不会到期。导入许可证文件后，此版本可被任何其他版本覆盖，并在其他商业版许可证不存在或无效时重新激活。 **商业版：** 限期或永久。有关商业版许可证到期后的问题的详细信息，请参阅许可证到期 (第 29 页)。
容量	**社区版：** 此版本具有固定的容量，可监控至多 25 个操作系统实例和 25 个 URL（容量不能扩展）。如果在监控器运行期间超过了此容量，则所有监控器都将暂停，并在日志中显示错误。例如，动态 VMware 监控器的 OSi 容量消耗会在监控器运行期间随搜寻到的 VM 数而发生更改。 **商业版：** 用户可根据其监控需求购买用于操作系统实例、URL 和事务的许可证容量。
用户管理	**社区版：** 一个用户帐户（管理员）。 **商业版：** 不限制用户和用户角色的数量，并支持 LDAP 身份验证和授权集成。
解决方案模板和监控器	**社区版：** • 解决方案模板及其从属监控器不可用。 • 社区版中不包含的监控器 (第 13 页)中列出的监控器不可用。 • 所有其他监控器均可用。 **商业版：** 所有监控器和解决方案模板均可用。
数据保留	**社区版：** • 历史监控器数据仅保留 30 天（但不会删除日志文件）。在日志首选项中配置的每日日志数不会影响保留的每日日志数。 • 快速报告会显示过去 30 天的数据。 **商业版**无限制
警报操作	**社区版：** 仅启用电子邮件和事件控制台警报操作。 **商业版：** 所有警报操作均启用。
API	**社区版：** 不支持。

功能	描述
	商业版： 支持
集成	**社区版：**不支持。 **商业版：** 支持
高可用性（故障转移）	**社区版：**不支持。如果尝试使用社区版将 SiteScope 故障转移计算机连接到 SiteScope，则主 SiteScope 会向故障转移 SiteScope 返回异常，并且该异常会显示在用户界面中。相应的消息也将写入主 SiteScope 的 error.log 文件。 **商业版：** 支持
模板部署	**社区版：**不支持 CSV 模板部署（通过用户界面）和自动模板部署。 **商业版：**完全支持
升级	可将社区版升级到高级版、旗舰版或系统收集器版。有关详细信息，请参阅导入和升级许可证 (第 25 页)。

试用版

下面是使用 SiteScope 试用版的规范。

功能	描述
版本类型	免费、一次性试用许可证。
版本持续时间	30 天
容量	当从社区版激活时，试用版许可证包括的容量可最多监控 25 个操作系统实例、25 个 URL 和 10 个事务。 **注意：**试用许可证的容量是固定的，无法扩展或续订。
功能	SiteScope 的全部功能。有关详细信息，请参阅功能比较表 (第 11 页)。
节点是否锁定	否
激活	使用社区版时，通过选择“首选项”>“常规首选项”>“许可证”>“试用版”可使用。仅可启动一次；之后该按钮永久禁用。
停用	选择“首选项”>“常规首选项”>“许可证”。在“已安装的许可证”表中，选择“试用版”行，然后单击“删除许可证”。 该操作将 SiteScope 恢复到之前的版本（或社区版，如果未购买任何其他版本）。
升级	可以使用高级版、旗舰版或系统收集器版覆盖试用版。有关详细信息，请参阅导入和升级许可证 (第 25 页)。
到期	30 天后许可证自动过期，SiteScope 将恢复到社区版。其功能将根据当前活动许可证版本的功能相应减少。

商业版

SiteScope 包括以下商业版。下表列出了这些版本的规格。

有关每个版本中可用功能的列表，请参阅功能比较表 (第 11 页)。

- 高级版/旗舰版 (第 17 页)
- 系统收集器版 (第 18 页)

高级版/旗舰版

功能	描述
版本类型	商业版。
版本持续时间	限期或永久
容量	购买所需的 OSi、URL 和事务容量（没有最小容量）。 有关许可证购买查询（或如果需要额外容量），请与您的 HP 销售代表联系或使用 HP SiteScope 产品页面中的“Contact Us”链接。
功能	SiteScope 的全部功能
节点是否锁定	是（该许可证仅在特定计算机上有效）
激活	购买许可证后，请选择“首选项”>“常规首选项”>“许可证”，然后在“许可证文件”框中输入 SiteScope 许可证文件的路径，或单击“选择”按钮，然后选择许可证文件。
停用	选择“首选项”>“常规首选项”>“许可证”。在“已安装的许可证”表中，选择“高级版/旗舰版”行，然后单击“删除许可证”。删除高级版或旗舰版许可证时，还应删除所有高级版或旗舰版的容量类型行（OSi、URL 和事务）。 该操作将 SiteScope 恢复到之前的版本或社区版（如果未购买任何其他版本）。
升级	可以使用旗舰版或系统收集器版覆盖高级版。有关详细信息，请参阅导入和升级许可证 (第 25 页)。
到期	当活动版本中的所有容量类型的时间段结束时，许可证将到期。SiteScope 会在许可证到期日前 7 天向用户发送通知消息，并在许可证面板中显示此信息。 到期时，SiteScope 将版本（和功能）自动降级到层次结构中的前一个商业版（如有）。否则，社区版将变为活动版本。
容量降级	当超过 OSi、URL 或事务容量时，SiteScope 将： 1. 打开对话框显示一条警告消息。 2. 发送每日消息（最多 7 天）提醒用户删除额外的监控器或增加许可证容量。超过许可证容量 7 天后，SiteScope 将暂停所有监控器。

系统收集器版

功能	描述
版本类型	HP Operations Manager 集成附带的 SiteScope 版本。
版本持续时间	限期或永久
容量	购买所需要的 OSi 容量（没有最小容量）。 有关许可证购买查询（或如果需要额外容量），请与您的 HP 销售代表联系或使用 HP SiteScope 产品页面中的“Contact Us”链接。
功能	SiteScope 的全部功能。
节点是否锁定	是（该许可证仅在特定计算机上有效）
激活	购买许可证后，请选择“首选项”>“常规首选项”>“许可证”，然后在“许可证文件”框中输入 SiteScope 许可证文件的路径，或单击“选择”按钮，然后选择许可证文件。
停用	选择“首选项”>“常规首选项”>“许可证”。在“已安装的许可证”表中，选择“系统收集器版”行，然后单击“删除许可证”。删除系统收集器版许可证时，还应删除所有系统收集器版的容量类型行（OSi、URL 和事务）。 该操作将 SiteScope 恢复到之前的版本或社区版（如果未购买任何其他版本）。
升级	由于无法覆盖系统收集器许可证时，因此可以通过导入高级版或旗舰版许可证来增加 URL 和事务容量。有关详细信息，请参阅导入和升级许可证 (第 25 页)。
到期	当活动版本中的操作系统实例容量的时间段结束时，许可证将到期。SiteScope 会在许可证到期日前 7 天向用户发送通知消息，并在许可证面板中显示此信息。 到期时，SiteScope 将版本（和功能）自动降级到层次结构中的前一个商业版（如有）。否则，社区版将变为活动版本。
容量降级	当超过 OSi、URL 或事务容量时，SiteScope 将： 1. 打开对话框显示一条警告消息。 2. 发送每日消息（最多 7 天）提醒用户删除额外的监控器或增加许可证容量。超过许可证容量 7 天后，SiteScope 将暂停所有监控器。

负载测试版

下面是在 HP LoadRunner 或 HP Performance Center 中使用 SiteScope 负载测试版的规范。

功能	描述
版本类型	HP LoadRunner 和 HP Performance Center 随附的免费版 SiteScope。
版本持续时间	永久
容量	25 个操作系统实例，25 个 URL **注意：**此许可证容量固定，不能进行扩展。
功能	请参阅功能比较表 (第 11 页)。
节点是否锁定	否
激活	安装 SiteScope for Load Testing 后将自动激活。
停用	用户无法删除负载测试版的许可证。
升级	可以将负载测试版升级到高级版、旗舰版或系统收集器版。有关详细信息，请参阅导入和升级许可证 (第 25 页)。 **注意：**升级负载测试版需要进行其他配置，如将 SiteScope for Load Testing 安装许可证升级到高级版 (第 27 页)中所述。
到期	不适用（此为永久许可证）
容量降级	当超过许可证容量时，SiteScope 将： 1. 打开对话框显示一条警告消息。 2. 发送每日消息（最多 7 天）提醒用户删除额外的监控器。超过许可证容量 7 天后，SiteScope 将暂停所有监控器。

故障转移版

以下为使用 SiteScope 故障转移版的规范。

功能	描述
版本类型	SiteScope 故障转移可在 SiteScope 服务器遇到可用性问题时提供额外的冗余和自动备份保护。故障转移版许可证在高级版、旗舰版和系统收集器版中免费提供。
版本持续时间	SiteScope 故障转移依赖于使用高级版、旗舰版或系统收集器版许可证的主 SiteScope。
功能	SiteScope 的全部功能
激活	安装 SiteScope 故障转移后，需要导入故障转移许可证。 只有当故障转移服务器与主 SiteScope 服务器（使用高级版、旗舰版或系统收集器版许可证）同步后，故障转移才会开始工作。
停用	选择“首选项”>“常规首选项”>“许可证”。在“已安装的许可证”表中，选择“故障转移”行，然后单击“删除许可证”。删除故障转移版许可证时，还应删除所有故障转移版容量类型行（OSi、URL 和事务）。
到期/容量降级	SiteScope 故障转移依赖于使用高级版、旗舰版或系统收集器版许可证的主 SiteScope。主 SiteScope 版许可证到期时，故障转移许可证也将到期，SiteScope 故障转移计算机上将没有活动的版本。

第 3 章: SiteScope 许可证

本章包括:

SiteScope 许可概述

SiteScope 许可负责控制可以同时创建的监控器数量以及可以使用的监控器类型。请根据监控环境的需要购买许可证类型和容量。可以创建的 SiteScope 监控器数量取决于下面两个因素:

- 您为特定许可证容量类型（操作系统实例、URL、事务）购买的监控容量。
- 要使用的 SiteScope 监控器类型。

购买 SiteScope 许可证并注册 SiteScope 后，您就可以获得重要的权利和权限。已注册用户可以访问所有 HP 产品中的技术支持和信息，同时还能免费进行更新和升级。

同时，已注册用户还能够访问 HP 软件支持网站。可以使用此访问权在自助解决知识搜索中搜索技术信息，还能下载 SiteScope 文档更新。

新的监控器许可模型

SiteScope 使用的许可授权模型已从基于点的模型更改为基于 SiteScope 所监控对象的类型的容量型模型。有三种类型的受监控对象：操作系统实例 (OSi)、运行 VuGen 脚本的监控器的事务和 URL。

可用的许可证容量类型取决于安装类型和选择的 SiteScope 版本。这意味着，您可以灵活地调整 SiteScope 部署，以便符合组织和基础结构的要求。

有关许可机制的详细信息，请参阅:

新的解决方案模板许可模型

解决方案模板的每个解决方案不再需要一个单独许可证。而是所有解决方案模板均自动用于高级版、旗舰版和系统收集器版许可证。解决方案模板的许可证使用根据从解决方案模板部署的监控器数进行计算。

瞬时启动许可证

要使用 SiteScope，必须拥有有效的许可证。许可证会根据您选择的安装类型自动激活（瞬时启动）。

- **HP SiteScope。***社区* 版许可证在常规 SiteScope 安装后立即可用。此免费版支持无限期使用 SiteScope 的部分功能。如果要扩展初始部署的监控容量，享用 SiteScope 提供的全部功能，您可以

随时升级 SiteScope 的版本。有关可用的 SiteScope 版本列表，请参阅许可证版本 (第 23 页)。

- **HP SiteScope for Load Testing**。*负载测试* 版许可证在安装 HP SiteScope for Load Testing 后立即可用。此安装类型仅用于 HP LoadRunner 或 HP Performance Center 安装。

备注: 对于 SiteScope 故障转移安装，高级版、旗舰版和系统收集器版中免费提供了*故障转移* 版许可证。安装 SiteScope 故障转移后，需要导入故障转移许可证文件。

许可证版本

您可以根据想要监控的环境类型选择 SiteScope 版本和容量模型（请参阅许可证容量类型 (第 24 页)），升级初始 SiteScope 部署。

可选择以下版本：

许可证版本	描述
试用版	SiteScope 提供了免费的一次性试用许可证，可在 30 天内试用完整的 SiteScope 功能。有关详细信息，请参阅试用版 (第 16 页)。
高级版/旗舰版	提供完整的 SiteScope 功能，包括集成、SiteScope API、SiteScope 故障转移，且能够使用企业监控器和模板。 高级版和旗舰版功能相同，仅在捆绑的集成方面不同。有关详细信息，请联系您的 HP 销售代表。 有关详细信息，请参阅高级版/旗舰版 (第 17 页)。
系统收集器版	HP Operations Manager 集成中提供的一个 SiteScope 版本，允许将 SiteScope 监控器用于 HPOM 应用程序中。有关详细信息，请参阅系统收集器版 (第 18 页)。
负载测试版	HP LoadRunner 和 HP Performance Center 中提供的一个 SiteScope 版本，允许用户在 LoadRunner 或 Performance Center 应用程序上定义和使用 SiteScope 监控器。有关详细信息，请参阅负载测试版 (第 19 页)。

有关各版本可用功能的比较，请参阅功能比较表 (第 11 页)。

有关许可证购买查询（或如果需要额外容量），请与您的 HP 销售代表联系或使用 HP SiteScope 产品页面中的“Contact Us”链接。如果您拥有许可证，并需要许可证密钥文件，请使用 HP 软件许可门户。

许可证容量类型

下表包含不同容量类型、用于计算许可证使用情况的规则以及各许可证容量类型支持的监控器的说明:

容量类型	描述
OSi 许可证	**支持的监控器:** 除 URL、URL 内容、URL 列表、URL 序列、Web 脚本、Web 服务、链接检查、XML 度量和免费监控器（复合监控器、公式复合监控器、Amazon Web Services 监控器、电子商务事务监控器和集成监控器）以外的所有监控器。
	许可证使用: 通常情况下，每个受监控的远程服务器使用一个 OSi 许可证实例，而不管该远程服务器配置了多少个监控器。例如，如果在同一操作系统或主机上使用 CPU 监控器、磁盘空间监控器和内存监控器，则将从许可证中扣除一个操作系统实例。 **例外:** • 自定义监控器、SNMP 陷阱和 Microsoft Windows 拨号每 15 个监控器使用一个操作系统实例。 • HP Vertica JDBC 监控器针对每个受监控的服务器消耗一个操作系统实例，针对每个受监控的节点消耗一个操作系统实例。 • Solaris Zones 监控器针对每个受监控的服务器消耗一个操作系统实例，针对每个受监控的区域消耗一个操作系统实例。 • VMware 数据存储监控器针对每个数据存储消耗一个操作系统实例。 • VMware 主机监控器针对每个受监控的主机消耗一个操作系统实例许可证，针对每个受监控的虚拟机消耗一个操作系统实例许可证。请注意，VMware 最佳实践建议将 VM 来宾的对象名称（在 vSphere 中）设置为与来宾本身的服务器名称（或计算机名称）相同。用此方法设置名称后，SiteScope 将对同一服务器的所有监控器仅使用一个操作系统实例。如果 vSphere 对象名称与来宾服务器名称不同，则 SiteScope 将对具有来宾服务器名称的所有 VMware 监控器和具有 vSphere 对象名称的所有监控器均使用一个操作系统实例。 **注意:** 各个版本之间不会聚合操作系统实例，因为各个版本的操作系统实例许可证的成本有所不同。但是，将在相同版本的各操作系统许可证之间聚合操作系统实例（例如，如果您具有多个高级版许可证，并且每个许可证包含多个操作系统实例）。
URL 许可证	**支持的监控器:** URL、URL 内容、URL 列表、URL 序列、Web 服务、链接检查、XML 度量。 **许可证使用:** • 每个受监控的 URL 或 URL 步骤消耗一个 URL 许可证实例。 • 除拥有自己的 URL 许可证的社区版、试用版和负载测试版以外，其他版本之间可聚合 URL 许可证。
事务许可证	**支持的监控器:** 使用 VuGen 脚本事务的 Web 脚本监控器。 **许可证使用:** • 每个 VuGen 脚本事务消耗一个事务许可证。

容量类型	描述
	• 除不支持监控事务的社区版和负载测试版以外，其他版本之间可聚合事务许可证。

导入和升级许可证

SiteScope 在安装时包含一个免费的社区版许可证。

要启用 SiteScope 社区版中不包含的功能，必须购买所需容量类型（OSi、URL 和事务）的 SiteScope 版本，然后将许可证文件密钥导入 SiteScope。

可通过以下方式导入 SiteScope 许可证：

- 在安装期间使用 SiteScope 配置向导导入，或者
- 在安装后使用“常规首选项”页面（请参阅导入 SiteScope 许可证 (第 27 页)）、API 或 SiteScope 配置工具（请参阅使用 SiteScope 配置工具 (第 107 页)）导入。

如果导入的版本许可证在层次结构中处于较高的位置，则会根据导入许可证的版本升级活动版本的功能。有关升级许可证的详细信息，请参阅升级 SiteScope 版本许可证 (第 26 页)。

此外，还可以增加高级版、旗舰版和系统收集器版的许可证容量。有关详细信息，请参阅增加许可证容量 (第 27 页)。

升级 SiteScope 版本许可证

您可以随时通过购买更高版本的许可证升级现有许可证版本。

从 SiteScope 社区版升级到 SiteScope 高级版或旗舰版，您可以获得 SiteScope 中其他可用功能的使用权。有关 SiteScope 社区版与其他 SiteScope 版本中可用功能的对比信息，请参阅功能比较表 (第 11 页)。

您可以根据以下层次结构升级版本许可证：

安装风格	版本层次结构	可用的版本升级			可用的容量提升	
		高级版	旗舰版	系统收集器版	事务/URL	OSi
SiteScope	共同体	✔	✔	✔		
	试用版	✔	✔	✔		
	系统收集器版（捆绑包）					✔
	高级版		✔	✔	✔	✔
	旗舰版（捆绑包）			✔	✔	✔
SiteScope for Load Testing[1]	负载测试版	✔				
	高级版				✔	✔
SiteScope 故障转移	故障转移版					
[1] 将 SiteScope for Load Testing 安装许可证升级到高级版需要进行其他配置，如将 SiteScope for Load Testing 安装许可证升级到高级版 (第 27 页)中所述。						

要升级版本许可证，请执行以下操作：

1. 购买您需要的 SiteScope 版本。有关许可证购买查询（或如果需要额外容量），请与您的 HP 销售代表联系或使用 HP SiteScope 产品页面中的“Contact Us”链接。如果您拥有许可证，并需要许可证密钥文件，请使用 HP 软件许可门户。
2. 导入许可证文件。有关详细信息，请参阅导入 SiteScope 许可证 (第 27 页)。

备注: 升级到 SiteScope 11.30 之后，可能需要较短的一段时间，才会使用当前许可证更新“许可”面板。

将 SiteScope for Load Testing 安装许可证升级到高级版

备注: 如果使用 SiteScope for Load Testing 安装，则不支持与 BSM 集成。

如果将 SiteScope for Load Testing 安装的许可证升级到高级版，则必须执行以下更改才能获得高级版的全部功能:

1. 在 SiteScope 中，选择“首选项”>“基础结构首选项”>“自定义设置”，并按如下所述更改下列属性的值:
   - disableRepeatedSchedules=false
   - disableReports=false
   - MultiViewDashboardEnabled=true

   备注: 此外，也可以从 **<SiteScope 根目录>\groups\master.config** 文件中删除 _disableRepeatedSchedules=true、_disableReports=true、_MultiViewDashboardEnabled=false 属性，然后重新启动 SiteScope。
2. 重新启动 SiteScope。

增加许可证容量

可以创建的 SiteScope 监控器数量取决于下面两个因素:

- 您已购买的特定许可证容量类型（操作系统实例、URL、事务）的监控容量。
- 要使用的 SiteScope 监控器类型。

可根据监控环境的需求增加高级版、旗舰版和系统收集器版的许可证容量。试用版、社区版和负载测试版的容量固定，不能增加。

备注: 购买和导入额外容量时:

- OSi 容量类型仅限当前版本。许可证容量不会与之前版本的 OSi 容量聚合。
- URL 容量类型在导入到当前高级版、旗舰版或系统收集器版时会与之前版本的 URL 容量聚合。
- 事务容量类型在导入到当前高级版、旗舰版或系统收集器版时会与之前版本的事务容量聚合。

要增加许可证容量，请执行以下操作:

1. 购买所需的操作系统实例、URL 和事务容量。有关许可证购买查询（或如果需要额外容量），请与您的 HP 销售代表联系或使用 HP SiteScope 产品页面中的“Contact Us”链接。
2. 导入许可证文件。有关详细信息，请参阅导入 SiteScope 许可证 (第 27 页)。

导入 SiteScope 许可证

当您从 HP 收到许可证文件时，请使用 SiteScope 用户界面将许可证密钥导入到 SiteScope 中。

要将许可证导入 SiteScope 中，请执行以下步骤:

1. 在 Web 浏览器中，打开要修改的 SiteScope 实例。SiteScope 服务或进程必须处于运行状态。
2. 选择“首选项”>“常规首选项”，然后展开“许可证”面板。
3. 在“许可证文件”框中输入 SiteScope 许可证文件的路径，或单击“选择”按钮，然后选择许可证文件。
4. 单击“导入”。在成功导入许可证之后，“已安装的许可证”表中将显示已导入许可证的相关信息。这些信息包括许可证版本、容量类型和详细信息（可用容量、已用容量和剩余容量）、到期日期以及许可证状态。

   备注: 升级到 SiteScope 11.30 之后，可能需要较短的一段时间，才会使用当前许可证更新“许可”面板。

许可证到期

版本许可证到期

对于基于时间的许可证，SiteScope 会在此许可证到期日前 7 天向用户发送一条警告消息。

如果版本许可证到期，则许可证将自动降级到版本层次结构中的前一个有效许可证（请参阅升级 SiteScope 版本许可证 (第 26 页)）。否则，社区版将变为活动状态。当用户删除许可证时也将发生这种情况。

将根据活动版本定义内提供的功能立即减少 SiteScope 功能。

备注: 用户无法从“首选项”>“常规首选项”>“许可证”的“已安装的许可证”表中删除社区版或负载测试版许可证。

容量许可证到期

当超过 OSi、URL 或事务许可证容量时，SiteScope 将:

1. 打开对话框显示一条警告消息。
2. 向用户发送已超过许可证容量的消息。SiteScope 最多会发送 7 天的每日通知。

如果用户在此时间内未删除额外的监控器或增加许可证容量，则 SiteScope 将暂停所有监控器，包括尚未超过容量的监控器类型。当监控器暂停时，仍能从 SiteScope 删除监控器。

降级到社区许可证

当商业许可证到期，且没有其他商业版本存在或有效时，社区版许可证将自动变为活动许可证。将立即禁用社区版许可证中不支持的功能。

下表显示了许可证降级对功能的影响:

功能	描述
监控器	如果超过社区版许可证容量，将暂停所有监控器，用户界面上将显示一条消息。 将停止运行并禁用社区版中不允许的所有已创建的监控器（例如，企业监控器和 Amazon Web Services 监控器）。
用户帐户	用户将不能使用其他用户帐户（常规或 LDAP）登录，也不能编辑其他用户帐户。这种情况不适用于 SiteScope 管理员帐户。
数据保留	尽管所有每日日志都将保留在文件系统中，但用户只能查看最近 30 天的报告和分析数据。
警报	将停止并禁用社区版中不允许的警报操作（仅允许电子邮件和事件控制台警报操作）。
报告	将不会发送计划报告，并且只能从用户界面激活快速报告。
API	将阻止所有公共和私有 SiteScope API。
集成	将停止并禁用所有集成。

功能	描述
SiteScope 故障转移	SiteScope 故障转移收到一条错误消息并停止从主 SiteScope 同步数据。

许可注意事项和限制

社区版

并非每次发布 SiteScope 次版本或次次版本时都会发布社区版。有关版本类型的详细信息，请参阅安装版本类型 (第 72 页)。

与 BSM 集成的 SiteScope

- 如果 SiteScope 已配置为向 BSM 发送数据，且 SiteScope 许可证已到期，则 SiteScope 将停止向 BSM 发送所有数据（包括拓扑）。当续订 SiteScope 许可证时，必须取消选中“首选项”>“集成首选项”>“BSM 集成”>“BSM 集成主设置”中的“禁用 Business Service Management 的所有登录”复选框才能启用 BSM 的登录和数据流，因为 SiteScope 在许可证到期时会自动禁用 BSM 登录。
- 如果在 SiteScope 高级版、旗舰版或系统收集器版许可证到期后（因此与 BSM 的集成已禁用）从 SiteScope 删除监控器，监控器不会从 BSM 中删除。需要在 BSM 的“RTSM 管理”>“IT 世界管理器”的“SiteScope 拓扑升级符合性”视图中手动删除监控器。

第 4 章: 入门指导

本节提供基本的 SiteScope 入门知识和逐步使用指导。

1. **注册 SiteScope。**

   注册 SiteScope，以获取技术支持服务和有关所有 HP 产品的信息。您还可以对产品进行更新和升级。您可以在 HP 软件支持网站上注册 SiteScope。

2. **了解可提供帮助信息的来源。**

   了解各种帮助信息来源，包括 HP 服务、HP 软件支持以及 SiteScope 帮助。

3. **制定 SiteScope 部署计划。**

   在安装 SiteScope 软件之前，制定完整的部署计划。您可以使用部署方法和计划 (第 32 页)获取帮助。有关详细的部署计划的最佳实践，请咨询 HP 代表。

4. **安装 SiteScope。**

   请参阅安装概述 (第 51 页)，初步了解 SiteScope 应用程序部署相关的步骤。有关安全部署 SiteScope 的信息，请参阅强化 SiteScope 平台 (第 127 页)。

5. **登录 SiteScope 并启动系统管理。**

   使用 Web 浏览器登录 SiteScope Web 界面。使用安装之后的管理任务 (第 162 页)中的清单，完成基本的平台和监控器管理任务，做好部署 SiteScope 的准备。

6. **向业务和系统用户推广 SiteScope。**

   SiteScope 系统使用所定义的用户和传入的监控数据启动并运行后，需要培训业务和系统用户，指导他们如何访问并使用 SiteScope 监控器、报告和警报功能。

有关使用和管理 SiteScope 的完整详细信息，请参阅 SiteScope 帮助。

第 5 章: 部署方法和计划

本章包括:

企业系统监控方法

在部署 SiteScope 时，需要规划资源、设计系统体系结构，以及制定适当的部署策略。本章概述为了成功部署和使用 SiteScope，用户需采用的方法及注意的事项。

备注: 下列信息可以帮助您做好安装前的准备工作。有关深入的部署计划最佳实践，请咨询 HP 专业服务代表。

采用一致的方法对于实施有效的系统监控十分必要。但是，获得、开发和部署企业监控解决方案的过程并非总是轻而易举。解决方案需要考虑 IT 基础结构所担当的角色，以及它如何帮助组织机构取得成功。系统监控工具用于确保组织所使用的服务的可用性和功能以实现其关键目标。在计划系统监控时，可以使用以下指南。

要监控的内容

高效的企业系统管理将会使用多层监控方法。SiteScope 为您提供了各种工具，可实现此目标。一方面，需要对基础结构中的各个硬件元素进行监控，以查看这些元素是否可用并正常运行。同时，还要对这些系统上的关键服务和进程进行监控。这包括低级别的操作系统进程，以及用于指示关键应用程序的运行状况和性能的进程。除此之外，还要对业务流程进行事务性监控，以查看关键应用程序和服务是否可用并按预期运行。

代表事件的阈值级别

信息系统的可用性和性能对企业业务取得成功至关重要。为监控器设置的阈值取决于您所监控的系统或业务流程的性质。

系统检查频率

系统检查频率与设置的事件阈值同等重要。在要访问关键业务信息系统的期间，应定期检查这些系统的可用性。在很多情况下，系统需要能够每周 7 天、每天 24 小时持续工作。通过使用每个监控器的“频率”设置，可以控制 SiteScope 检查系统的频率。两次检查之间的间隔时间太长可能会延误对问题的检测，间隔时间太短则会给本已繁忙的系统增加不必要的负载。

检测到事件后采取的措施

作为监控应用程序，SiteScope 为您提供了多种工具来检测问题。您可以使用 SiteScope 警报在事件阈值被触发时发送即时通知。电子邮件通知是常用的警报操作。SiteScope 还包括可以与其他系统集成的其他警报类型。

您可以通过定义具有不同警报触发条件的多个警报定义来制定警报升级方案。可以使用警报的“时间”设置自定义所检测事件与警报操作之间的关系。

其他的事件操作可以是对依赖于不再可用的系统的系统禁用监控和警报功能。SiteScope 组和监控器依赖性选项可用于避免一系列的警报级联。

可以执行的自动响应类型

检测到问题后，最好能够通过自动响应来解决问题。虽然这不可能适用于所有系统，但 SiteScope 脚本警报类型仍然提供了一款灵活简便且功能强大的工具，用于在不同情况下自动执行更正操作。对于工作环境中可能出现的问题，应考虑其中有哪些可以通过自动响应加以解决。

业务系统基础结构评估

1. 制定体系结构和部署决策前先收集技术和业务要求。此阶段的操作包括：
   - 为要监控的所有业务应用程序制定列表。这需要考虑端到端服务，如订单处理、帐户访问功能、数据查询、更新以及报告功能。
   - 制定可支持业务应用程序的服务器的列表。其中必须包括支持前端 Web 界面、后端数据库和应用程序服务器的服务器。
   - 制定可支持业务应用程序的网络设备的列表。这包括网络工具和身份验证服务。
   - 确定要监控的检测信号元素。检测信号元素是一些服务，可充当特定业务系统或资源的可用性基本指标。
   - 列出代表要在每个系统中监控的资源的监控器模板。
2. 确定业务系统监控活动的利益相关方和重要结果。这些结果包括：
   - 将要生成的报告。
   - 要在检测到事件后采取的警报操作。
   - 要将警报发送到的目标对象。
   - 要查看和管理 SiteScope 的用户。
   - 利益相关方需要访问的 SiteScope 元素。
   - 任何服务水平协议的阈值（如果可用）。

3. 了解运行系统监控功能时必须遵循的约束。这包括对可用协议、用户身份验证要求、业务敏感数据系统访问的限制以及网络流量限制。

调整 SiteScope 服务器的大小

合理调整运行 SiteScope 的服务器的大小是成功实现监控部署的基础。服务器的大小调整取决于多个因素，包括:

- 要在 SiteScope 安装上运行的监控器实例数。
- 监控器的平均运行频率。
- 要监控的协议和应用程序的类型。
- 需要在服务器上保留以用于报告的监控器数据量。

要估算所需的监控器数量，首先需要了解当前环境中服务器的数量、其使用的操作系统以及要监控的应用程序。

请参阅调整 Windows 平台上的 SiteScope 大小 (第 40 页)或调整 Linux 平台上的 SiteScope 大小 (第 41 页)，以获取推荐的服务器大小的列表（基于要运行的监控器数量评估得出）。

网络位置和环境

SiteScope 的主要监控功能是通过模拟 Web 客户端或网络客户端（这些客户端对网络环境中的服务器和应用程序发出各种请求）来实现的。因此，SiteScope 必须能够访问整个网络中的服务器、系统和应用程序。这样有助于确定 SiteScope 的安装位置。

SiteScope 用于监控系统、服务器和应用程序的方法可以划分为两类:

- **基于标准的网络协议。**其中包括 HTTP、HTTPS、SMTP、FTP 和 SNMP。
- **特定于平台的网络服务和命令。**其中包括 NetBIOS、telnet、rlogin 和安全 Shell (SSH)。

基础结构监控功能依赖于特定于平台的服务。作为无代理解决方案，监控功能要求 SiteScope 频繁登录到基础结构中的多个服务器，并对这些服务器进行身份验证。出于性能和安全考虑，最好在同一域中部署 SiteScope，并使之尽可能靠近要监控的系统元素。此外，最好能将 SiteScope 置于相应网络身份验证服务（如 Active Directory、NIS 或 LDAP）所在的子网中。根据需要，可以使用 HTTP 或 HTTPS 对 SiteScope 界面进行远程访问和管理。

备注: 如果某个位置中存在大量需要跨广域网 (WAN) 进行通信的监控活动，应尝试避免在该位置部署 SiteScope。

提示: 出于安全考虑，建议不要使用 SiteScope 通过防火墙对服务器进行监控，这是因为对服务器可用性的监控需要使用不同的协议和端口。SiteScope 的许可不基于服务器，但支持在防火墙的两端独立安装 SiteScope。可以使用 HTTP 或 HTTPS 从单个工作站同时访问两个或更多个独立安装的 SiteScope。

Windows 环境的注意事项

必须使用具有管理员权限的帐户安装 SiteScope。此外，还建议使用具有管理员权限的用户帐户运行 SiteScope 服务。可以使用本地系统帐户，但是这会影响远程 Windows 服务器连接配置文件的配置。

此外，SiteScope 还在远程计算机上使用 Windows 性能注册表，以监控服务器的资源和可用性。要启用此监控功能，必须激活远程计算机的远程注册表服务。

Linux 环境的注意事项

您必须使用 root 用户将 SiteScope 安装到 Linux 环境中。在安装 SiteScope 之后，您可以创建有权运行 SiteScope 的非 root 用户帐户（除非 SiteScope Web 服务器在特权端口上运行，这种情况下需要由 root 用户运行）。有关如何配置非 root 用户以使其有权运行 SiteScope 的详细信息，请参阅配置有权运行 SiteScope 的非 root 用户帐户 (第 35 页)。

使用 SiteScope 对远程 UNIX 服务器进行无代理监控设置的其他相关信息如下：

- **远程登录帐户 Shell。**作为应用程序，SiteScope 可以在最常用的 UNIX shell 下成功运行。与远程 UNIX 服务器通信时，SiteScope 会首先与 Bourne shell (sh) 或 tsch shell 通信。因此，每台远程 UNIX 服务器上的相关登录帐户也应将其各自的 shell 设置为使用其中一个 shell。

  备注: 仅为 SiteScope 用于与远程计算机通信的登录帐户设置 shell 配置文件。远程计算机上的其他应用程序和帐户可以使用它们当前定义的 shell。

- **帐户权限。**可能需要对用于监控远程 UNIX 服务器的命令权限设置进行解析。SiteScope 运行的用于从远程 UNIX 服务器获取服务器信息的大多数命令都位于远程服务器上的 **/usr/bin** 目录中。但是，某些命令，如用于获取内存信息的命令，则位于 **/usr/sbin** 中。这两个位置之间的差别在于，**/usr/sbin** 命令通常是为 root 用户或其他高级权限用户预留的。

  备注: 尽管 SiteScope 需要特权较高的帐户权限，但是出于安全考虑，不建议使用 root 帐户运行 SiteScope，或将其配置为使用远程服务器上的 root 登录帐户。

如果发生权限问题，则需要以其他有权运行该命令的用户身份登录 SiteScope，或对 SiteScope 所使用的用户帐户的权限进行更改。

配置有权运行 SiteScope 的非 root 用户帐户

您必须使用 root 用户帐户将 SiteScope 安装到 Linux 中。在安装 SiteScope 之后，您可以创建有权运行 SiteScope 的非 root 用户帐户。

备注: 虽然 SiteScope 需要特权较高的帐户权限才能启用全方位的服务器监控，但是不建议通过 root 帐户运行 SiteScope，也不要将 SiteScope 配置为使用 root 帐户访问远程服务器。

要创建有权运行 SiteScope 的非 root 用户帐户，请执行以下操作：

1. 添加新用户：useradd newuser
2. 更改 SiteScope 安装文件夹的权限：chmod 755 /opt/HP/SiteScope/ -R
3. 更改 SiteScope 安装文件夹的所有权：chown newuser /opt/HP/SiteScope/ -R
4. 以新用户身份登录：su newuser
5. 转至安装文件夹：cd /opt/HP/SiteScope
6. 运行 SiteScope：./start

备注: 要支持 HP Operations Manager 事件与度量的集成，在 SiteScope 计算机上运行 HP Operations Agent 的用户必须与 SiteScope 中运行的用户相同（即非 root 用户）。有关详细信息，请参阅《HP Operations Manager for UNIX - HTTPS Agent Concepts and Configuration Guide》中的“Configure an Agent to run Under an Alternative User on UNIX”。

第 6 章: 调整 SiteScope 的大小

本章包括:

调整 SiteScope 大小概述

虽然默认的 SiteScope 配置允许您运行数以千计的监控器，但仍需调整其中安装有 SiteScope 的服务器的大小以获得最佳性能。因为每个配置不尽相同，所以应当使用 SiteScope 容量计算器来验证是否需要为所做的配置调整大小。

正确调整要运行 SiteScope 的服务器的大小是成功进行监控部署的基础。为了实现最佳的大小调整操作，HP 强烈建议使用以下 SiteScope 服务器环境:

- 将 SiteScope 作为独立服务器运行。为获得最佳效果，请不要在服务器上运行 SiteScope 以外的程序。不能在 SiteScope 服务器上运行 BSM、BMC、HP LoadRunner、数据库、Web 服务器等程序。
- 只使用一个 SiteScope 实例，且该实例在单个服务器上运行。在单个服务器上运行多个 SiteScope 实例可能会导致严重的资源问题。此建议还适用于用来监控系统运行状况的 SiteScope 实例。
- 与 SiteScope 主服务器一样，SiteScope 故障转移也需要调整大小。

SiteScope 容量计算器

SiteScope 包括一个能帮助您预测系统行为和规划 SiteScope 容量的工具。您可以输入运行 SiteScope 的系统的 CPU 和内存详细信息、不同类型的监控器数量及其运行频率。之后，计算器将显示每一种监控器预期的 CPU 使用率和内存使用率，以及给定工作负荷的推荐系统要求。这样，您就可以确定是否需要调整配置。

备注: SiteScope 容量计算器只在 Windows 版本上运行的 SiteScope 中受支持，并受受支持的监控器和解决方案模板 (第 39 页)中列出的 64 位监控器和解决方案模板的支持。

要使用 SiteScope 容量计算器，请执行下列操作:

1. 使用计数器之前，估计 SiteScope 服务器上的负载，并使用本指南中的系统要求建议来确定硬件需求。

   有关详细信息，请参阅系统硬件要求 (第 52 页)。
2. 从以下位置打开 SiteScope 容量计数器:
   - SiteScope 安装文件夹: **<SiteScope 根目录>\tools\SiteScopeCapacityCalculator.xls**
   - HP 软件支持网站。

3. 根据安装 SiteScope 的计算机上的操作系统，选择“Monitor Usage”选项卡。请注意，SiteScope 11.30 仅支持 64 位操作系统。
4. 在“Requirements”部分中输入以下信息：
   - CPU 的平均使用百分比
   - CPU 类型
   - 内存堆大小（单位：MB）
   - 对于 64 位安装，如果 SiteScope 已与 BSM 集成，则选择 TRUE；如果独立安装 SiteScope，则选择 FALSE。
5. 在“Monitors”部分中，输入各类型监控器的数量和各监控器的更新频率。
6. “results and recommendations”部分将显示结果和建议。预期结果和实际结果之间存在 30%-40% 的差异是可以接受的。

受支持的监控器和解决方案模板

SiteScope 容量计算器支持以下监控器和解决方案模板:

监控器:

- CPU
- 数据库计数器
- 数据库查询（仅限 64 位）
- 目录监控器（仅限 64 位）
- 磁盘空间
- DNS 监控器
- 文件监控器（仅限 64 位）
- JMX 监控器（仅限 64 位）
- 日志文件监控器（仅限 32 位）
- 内存监控器
- Microsoft IIS 服务器监控器
- Microsoft SQL Server 监控器（仅限 32 位）
- Microsoft Windows 事件日志监控器（仅限 32 位）
- Microsoft Windows 资源监控器
- Ping 监控器
- SAP CCMS 监控器（仅限 32 位）
- 服务监控器
- Siebel 应用程序服务器监控器（仅限 32 位）
- SNMP (按 MIB) 监控器
- UNIX 资源监控器（仅限 64 位）
- URL 监控器
- URL 列表监控器（仅限 64 位）
- WebLogic 应用程序服务器监控器（仅限 32 位）
- Web 服务监控器（仅限 64 位）
- WebSphere 应用程序服务器监控器（仅限 32 位）

解决方案模板:

- Microsoft Exchange 2003 解决方案模板（仅限 32 位）
- Siebel 解决方案模板（仅限 32 位）

备注: SiteScope 32 位监控器已弃用，在升级到 SiteScope 11.30 后不再有效。有关详细信息，请参阅从 32 位迁移到 64 位 SiteScope (第 62 页)。

调整 Windows 平台上的 SiteScope 大小

调整安装在 Windows 平台上的 SiteScope 大小时，您应当在 SiteScope 和 Windows 操作系统上执行以下步骤：

1. **调整 SiteScope 的大小。**

   建议首先调整 SiteScope 的大小，然后在执行下一个步骤之前让 SiteScope 至少运行 24 个小时。有关详细信息，请参阅调整 SiteScope 的大小 (第 40 页)中的步骤。

2. **调整 Windows 操作系统。**

   完成 SiteScope 的大小调整并至少等待 24 小时之后，您需要调整 Windows 操作系统，然后重新启动 SiteScope 服务器，以使参数更改生效。有关详细信息，请参阅调整 Microsoft Windows 操作系统 (第 40 页)中的步骤。

3. **常规维护建议。**

   此外，您应当遵循某些常规维护建议，以确保获得最佳的调整效果。有关详细信息，请参阅常规维护建议 (第 41 页)。

备注:

- 建议对要更改的任何文件或参数进行备份，以便在需要时从备份进行还原。
- 如果设置未生效，请勿随意增减这些设置。请联系 HP 软件支持以执行进一步的分析和疑难解答。

调整 SiteScope 的大小

调整 SiteScope 的大小包括确认监控器是否只在绝对必要时才使用“验证错误”选项。此选项仅适用于少量监控器，以及由于网络或服务器负载问题而在受监控的远程计算机上出现“无数据”虚假警报历史记录的监控器。

启用此功能后，出现故障的监控器会立即重新运行，并在检查警报条件之前绕过计划程序。大量的这种额外运行过程会显著干扰计划程序，并导致 SiteScope 性能降级。对于因连接问题而发生故障的监控器，在监控器终止前，验证错误所花的时间可能与“连接超时”时间量相当。在此期间，监控器线程和连接会默认锁定两分钟。此延迟可能会使其他监控器进入等待状态，而发生故障的监控器将会被跳过。

要调整 SiteScope 的大小，请执行以下操作：

1. 对于每个监控器，选择“属性”选项卡，打开“监控器运行设置”面板，然后检查是否选中“验证错误”。为不需要此选项的监控器清除此复选框。

   提示: 对于多个监控器，建议使用“全局搜索和替换”来执行此任务。

2. 在调整 Windows 操作系统之前，请让 SiteScope 至少运行 24 个小时。

调整 Microsoft Windows 操作系统

在调整 Microsoft Windows 操作系统的过程中，需要使用“配置工具”更改大量参数。此外，您应当遵循某些常规维护建议，以确保获得最佳的调整效果。

要调整 Microsoft Windows 操作系统，请执行以下操作：

1. 运行“配置工具”，并选择“调整大小”选项。

   此工具可将 JVM 堆大小增加到 4096 MB，将桌面堆大小增加到 8192 KB，还可以将文件句柄数增加到 18,000。此外，它还会禁用 SiteScope 可执行文件的弹出警告。有关详细信息，请参阅在 Windows 平台上运行配置工具 (第 107 页)。

   备注: “配置工具”仅支持默认的 SiteScope 服务名称。如果更改了服务名称，请与 HP 软件支持联系，切勿运行“配置工具”。

2. 重新启动 SiteScope 服务器，以使参数更改生效。
3. 根据需要在“首选项”>“基础结构首选项”中配置其他与调整大小相关的参数。

   提示: 为获得最佳性能，建议使用这些设置的默认值。

常规维护建议

按照常规维护建议来调整 Windows 上的 SiteScope 大小。

- **确定适当的监控器频率。**

  检查监控器的运行频率，并确保监控器的运行间隔合理。例如，大多数磁盘监控器不必每 5 分钟运行一次。通常来说，可能除 /var、/tmp 和 swap 卷外，所有卷以每 15 分钟、30 分钟甚或每 60 分钟运行一次即足够。降低监控器频率可以减少每分钟运行的监控器数量，同时还能提升性能和增大容量。

- **优化组结构。**

  组结构应考虑到 SiteScope 的易用性，以及 SiteScope 的性能优化。在理想情况下，顶级组的数量和结构的深度均应最小化。

  如果在一个组结构中，顶级组的数量超过 50 个或是深度超过 5 级，则可能会导致性能降级。

- **解决 SiteScope 配置错误。**

  使用运行状况监控器可以解决监控器配置错误的问题。即使错误很少，也可能会导致性能和稳定性降级。有关解决这些错误的详细信息，请联系 HP 软件支持。

- **计划 SiteScope 服务器的物理位置。**

  SiteScope 服务器的位置应当尽可能接近正在监控的计算机所在的本地网络。尽管在某些情况下，当连接容量充足且延迟较低时也可以进行监控，但我们不建议通过 WAN 连接进行监控。

调整 Linux 平台上的 SiteScope 大小

调整 Linux 操作系统上的 SiteScope 大小需要更改大量参数。此外，您应当遵循某些常规维护建议，以确保获得最佳的调整效果。

1. **调整操作系统。**

   为 SiteScope 实例配置合适的线程数，同时配置 Linux 操作系统的参数。有关详细信息，请参阅调整操作系统 (第 42 页)中的步骤。

2. **调整 Java 虚拟机。**

   配置 JVM 堆大小、线程堆栈大小，并实施并行垃圾收集。有关详细信息，请参阅调整 Java 虚拟机 (第 43 页)中的步骤。

3. **常规维护建议。**

此外，您应当遵循某些常规维护建议，以确保获得最佳的调整效果。有关详细信息，请参阅常规维护建议 (第 43 页)。

调整操作系统

调整操作系统需要为 SiteScope 实例配置合适的监控器数量以及配置 Linux 操作系统的参数。

配置正在运行的监控器的最大数目

可以在“首选项”>“基础结构首选项”>“服务器设置”中配置“最大监控器运行”。有关详细信息，请参阅 SiteScope 帮助中《使用 SiteScope》的“首选项”部分。

提示: 为获得最佳性能，建议使用此设置的默认值。

配置 Linux 操作系统参数

Linux 操作系统能够支持大量线程。要启用此功能，请在 SiteScope 服务器上执行以下操作。

要配置 Linux 操作系统的参数，请执行以下操作:

1. **修改内核文件描述符的限制。**
   a. 编辑 **/etc/system** 文件，并添加以下行:

      set rlim_fd_max=8192

      备注: 1024 为默认值（此限制对 root 用户不适用）。数值 8192 足以满足最大的 SiteScope 实例需要。请使用此较高值，而不要使用较低值进行尝试。这样可避免在较低值不够的情况下需要稍后重新启动计算机。

   b. 重新启动服务器。
2. **修改用户运行时限制。**
   a. 在 **<SiteScope 根目录>\bin** 目录中，将以下行添加到 SiteScope 启动脚本 **start-monitor** 和 **start-service** 中:

      ulimit -n 8192

b. 确认下列参数具有下面的最小值。有关详细信息，请联系 UNIX 系统管理员。

参数	最小值
核心文件大小（块）	无限制
数据区段大小 (KB)	无限制
文件大小（块）	无限制
打开文件	8192
管道大小（512 字节）	10
堆栈大小 (KB)	8192
CPU 时间（秒）	无限制
最大用户进程数	8192
虚拟内存 (KB)	无限制

修改运行时限制条件后无需重新启动 SiteScope 应用程序或服务器。

调整 Java 虚拟机

要获得最佳的 JVM 性能，您需要按照下面的方式进行配置。

要配置 JVM，请执行下列操作：

1. **增大堆空间。**

   默认情况下，SiteScope 的 Java 堆空间为 512 MB。如果要正常运行大型实例，此大小是不够的。

   Java 堆空间的大小最多可增大到 4096 MB（建议对大型负载采用此堆大小），您可以通过修改 **<SiteScope 根目录>\bin** 目录中的 **start-service** 和 **start-monitor** 脚本来完成操作。

   我们建议将最小堆大小设置为等于最大堆大小，以增强 SiteScope 的启动性能。例如，将 -Xmx4096m –Xms512m 更改为 -Xmx4096m –Xms4096m。

2. **减小线程堆栈的大小 (-Xss)。**

   由 SiteScope 创建的每个线程都会实例化一个内存量为 -Xss 的堆栈。默认的 UNIX JRE 线程堆栈大小最大值 -Xss 为每线程 512 KB 内存。

   如果没有在 **<SiteScope 根目录>\bin\start-monitor** 中的 Java 命令行上予以指定，则会使用默认的线程堆栈大小最大值。默认大小可以超出可用内存，以限制线程的数量。

   拥有 4000 或更多数量的监控器实例可由 -Xss 为 128 KB 的线程栈满足。

常规维护建议

在此，我们为您提供调整 Linux 平台上 SiteScope 大小的常规维护建议。

- **使用运行状况监控器。**

  尽可能使用具有“依赖于”的运行状况监控器，特别是所有使用远程 UNIX 连接的监控器。运行状况监控器通过检测是否有多台计算机不可用来避免服务器性能降级，同时锁定 SSH 连接线程。

- **尽量避免使用“验证错误”功能。**

  如果在“监控器运行设置”面板中启用了“验证错误”选项，则出现故障的监控器将立即重新运行，并在检查警报条件之前绕过计划程序。大量的这种额外运行过程会显著干扰计划程序，并导致 SiteScope 性能降级。对于因连接问题而发生故障的监控器，在监控器终止前，验证错误所花的时间可能与“连接超时”时间量相当。在此期间，监控器线程和连接会默认锁定两分钟。此延迟可能会使其他监控器进入等待状态，而发生故障的监控器将会被跳过。

- **使用 SSH 和内部 Java 库。**

  使用 SSH 连接方法定义远程首选项时，请尽可能使用 SSH 和内部 Java 库选项。内部 Java 库是一种基于 Java 的第三方 SSH 客户端。此客户端可以显著地提升 Telnet 和主机操作系统的 SSH 客户端的性能和扩展能力。此客户端支持 SSH1、SSH2、公钥身份验证等身份验证方法。

  请确保已启用连接缓存（在“新建/编辑 Microsoft Windows/UNIX 远程服务器”对话框中，展开“高级设置”并清除“禁用连接缓存”复选框）。应当调整“连接限制”，以使所有针对特定服务器运行的监控器及时得以执行。

- **确定适当的监控器频率。**

  检查监控器的运行频率，并确保监控器的运行间隔合理。例如，大多数磁盘监控器不必每 5 分钟运行一次。通常来说，可能除 /var、/tmp 和 swap 卷外，所有卷以每 15 分钟、30 分钟甚或每 60 分钟运行一次即足够。降低监控器频率可以减少每分钟运行的监控器数量，同时还能提升性能和增大容量。

- **优化组结构。**

  组结构应考虑到 SiteScope 的易用性，以及 SiteScope 的性能优化。在理想情况下，顶级组的数量和结构的深度均应最小化。

  如果在一个组结构中，顶级组的数量超过 50 个或是深度超过 5 级，则可能会导致性能降级。

- **解决 SiteScope 配置错误。**

  使用运行状况监控器可以解决监控器配置错误的问题。即使错误很少，也可能会导致性能和稳定性降级。有关解决这些错误的详细信息，请联系 HP 软件支持。

- **计划 SiteScope 服务器的物理位置。**

  SiteScope 服务器的位置应当尽可能接近正在监控的计算机所在的本地网络。当进行跨 WAN 监控或是网络链接速度缓慢时，网络通常会变成您的瓶颈。在这种情况下，监控器需要等待更多时间才能运行。尽管在某些情况下，当连接容量充足且延迟较低时也可以进行监控，但我们不建议通过 WAN 连接进行监控。

- **使用本地用户帐户。**

  UNIX 远程身份验证通常更倾向于本地用户帐户，而非 Directory Service 帐户。本地用户帐户不会依赖用于身份验证的 Directory Service 服务器。这样能够保证快速执行身份验证，避免在 Directory Service 服务器宕机时连接失败。

  在某些情况下，过大的 SiteScope 实例可能会对目录服务服务器的性能产生负面影响。因此，建议将此服务器置于要监控的服务器附近。

疑难解答和限制

问题： JVM 崩溃，并显示错误消息“耗尽交换空间”。

可以通过以下方法检测关于交换空间耗尽的错误：

1. 创建 Microsoft Windows 资源监控器，以监控目标 SiteScope 服务器上的虚拟字节计数器。
2. 配置以下阈值设置：

   如果 >= 7.9 GB，则发生错误

   如果 >= 7.8GB，则发出警告

   （当该值达到 8 GB 时进程崩溃）

解决方案：

1. 减少 JVM 堆大小。有关更改 JVM 堆大小的详细信息，请参阅在 Windows 平台上运行配置工具 (第 107 页)。
2. 通过减少并发运行的监控器的数量来减少 SiteScope 所使用的线程数（“首选项”>“基础结构首选项”>“服务器设置”>“最大监控器进程数”）。

第 7 章: 了解无代理监控

本章包括:

SiteScope 监控功能概述

本节介绍了 SiteScope 的无代理监控概念。无代理监控意味着，即便不在要监控的服务器上部署代理软件，也可以完成监控。与其他性能或运行状况监控解决方案相比，SiteScope 的部署和维护更简单。与基于代理的监控方式不同，SiteScope 可通过下列方法降低总拥有成本:

- 收集基础架构组件的详细性能数据。
- 无须在生产系统上运行监控代理，从而节省内存或 CPU 资源。
- 通过将所有监控组件整合到一个中央服务器，从而减少执行维护操作所需的时间和成本。
- 无须为更新生产系统的监控代理而使生产系统脱机。
- 无须为使某个监控代理可与其他代理共存而调整此代理。
- 无须物理访问生产服务器或等待软件分发操作，从而缩短安装时间。
- 降低因代理不稳定而在生产服务器上造成系统停机的可能性。

SiteScope 是一个通用的运行状况监控解决方案，可提供很多不同的监控器类型，用于在各种级别监控系统和服务。可以进一步自定义很多监控器类型，以满足特殊的环境需求。

企业和组织通常需要部署并维护多个解决方案，以在这些不同级别监控运行状况和可用性。运行状况监控可以分为下表中描述的几个级别或层:

监控器类型	描述
服务器运行状况	监控 CPU 使用率、内存、存储空间等服务器计算机资源以及关键进程和服务的状态。
Web 进程和内容	监控关键 URL 的可用性、基于 Web 的关键进程的功能，并监控关键文本内容。
应用程序性能	监控 Web 服务器、数据库和其他应用程序服务器等关键任务应用程序的性能统计信息。
网络	监控服务的连接性和可用性。

了解无代理监控环境

主要的 SiteScope 监控功能是通过模拟 Web 客户端或网络客户端（这些客户端对网络环境中的服务器和应用程序发出各种请求）来实现的。因此，SiteScope 必须能够访问整个网络中的服务器、系统和应用程序。

本节包括以下主题:

SiteScope 监控方法

SiteScope 用于监控系统、服务器和应用程序的方法可以划分为两类:

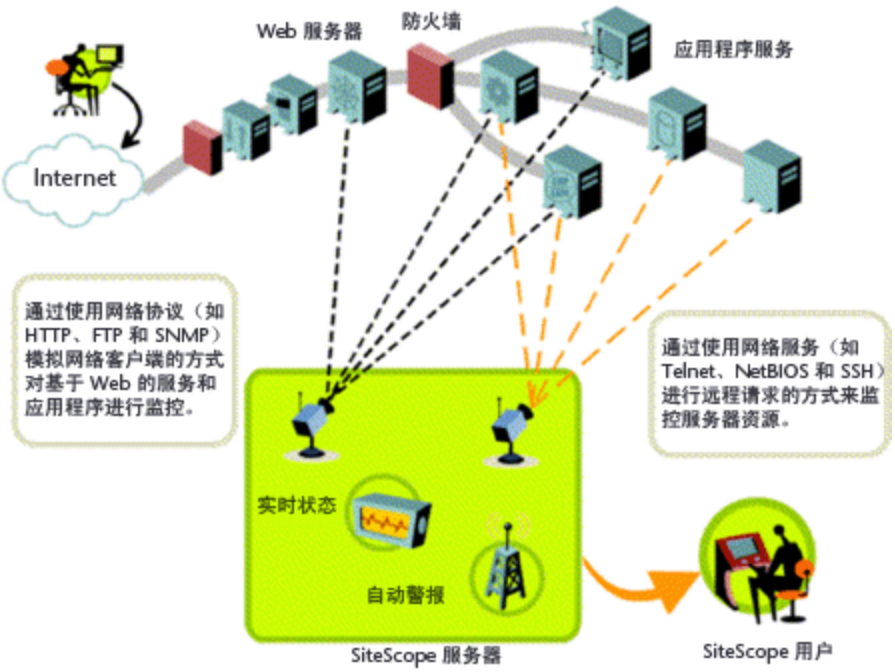
- **基于标准的网络协议。**

  此类别包括使用 HTTP、HTTPS、FTP、SMTP、SNMP 和 UDP 执行的监控。这些类型的监控器通常独立于运行 SiteScope 的平台或操作系统。例如，在 Linux 上安装的 SiteScope 可以监控运行 Windows、HP-UX 和 Solaris 的服务器上的网页、文件下载、电子邮件传输和 SNMP 数据。

- **特定于平台的网络服务和命令。**

  此类别包括作为客户端登录到远程计算机并请求信息的监控器类型。例如，SiteScope 可以使用 telnet 或 SSH 登录远程服务器，并请求有关磁盘空间、内存或进程的信息。在 Microsoft Windows 平台上，SiteScope 还会使用 Windows 性能计数器库。对于依赖特定于平台的服务的监控器类型而言，在跨不同操作系统实施监控时存在某些限制。

  下图显示了使用 SiteScope 进行无代理监控的概况。SiteScope 监控器对远程计算机上的服务生成请求以收集性能和可用性数据。



SiteScope 服务器监控器（例如，CPU、磁盘空间、内存、服务）可用于监控以下平台上的服务器资源: Windows、AIX、CentOS、FreeBSD、HP iLO、HP-UX、HP/UX、HP/UX 64 位、Linux、MacOSX、NonStopOS、OPENSERVER、Red Hat Enterprise Linux、SCO、SGI Irix、Solaris Zones、Sun Fire X64 ILOM、Sun Solaris、SunOS、Tru64 5.x、Tru64 Pre 4.x (Digital) 和 Ubuntu Linux。

备注: 要从在 Linux 上运行的 SiteScope 监控 Windows 计算机上的服务器资源（例如，CPU 使用率、内存），必须使用 SSH 连接。必须在每台要以此方式实施监控的 Windows 计算机上安装安全

Shell 服务器。有关如何启用此功能的详细信息，请参阅 SiteScope 帮助中《使用 SiteScope》的“使用安全 Shell (SSH) 进行 SiteScope 监控”部分。

SiteScope 包含一个适配器配置模板，允许您扩展 SiteScope 功能以监控其他版本的 UNIX 操作系统。有关详细信息，请参阅 SiteScope 帮助中的“UNIX 操作系统适配器”。

需要在 SiteScope 将远程访问系统数据的每个服务器上启用登录帐户。必须相应地配置受监控服务器上的登录帐户，使其与安装和运行 SiteScope 的帐户匹配。例如，如果 SiteScope 在用户名为 **sitescope** 的帐户下运行，则由此 SiteScope 安装监控的服务器上的远程登录帐户需要将用户登录帐户配置为 **sitescope** 用户。

防火墙和 SiteScope 部署

出于安全考虑，建议不要使用 SiteScope 通过防火墙对服务器进行监控，这是因为对服务器的监控需要使用不同的协议和端口。SiteScope 许可支持在防火墙的两端单独安装 SiteScope。可以使用 HTTP 或 HTTPS 从单个工作站访问两个或更多个 SiteScope 安装。

下表列出了在典型监控环境中 SiteScope 常用于实施监控和发出警报的端口:

SiteScope 函数	使用的默认端口
SiteScope Web 服务器	端口 8080
SiteScope 报告	端口 8888
FTP 监控器	端口 21
邮件监控器	端口 25 (SMTP)、110 (POP3)、143 (IMAP)
新闻监控器	端口 119
Ping 监控器	ICMP 数据包
SNMP 监控器	端口 161 (UDP)
URL 监控器	端口 80、443
远程 Windows 监控	端口 139
电子邮件警报	端口 25
公告警报	端口 80、443
SNMP 陷阱警报	端口 162 (UDP)
远程 UNIX ssh	端口 22
远程 UNIX Telnet	端口 23
远程 UNIX rlogin	端口 513

监控器权限和凭据

访问每个监控器都需要用户权限和凭据。有关所需权限和凭据以及每个监控器使用的相应协议的详细信息，请参阅 SiteScope 帮助中《Monitor Reference》指南的 Monitor Permissions and Credentials 部分。

第 2 部分: 安装 SiteScope 之前

第 8 章: 安装概述

SiteScope 安装在单个服务器上，且在 Windows 平台上作为单个应用程序运行，或者在 Linux 平台上作为单个应用程序或多个进程运行。

在安装 SiteScope 之前，需要考虑几个计划步骤和操作，以便简化对监控环境的部署和管理。

以下是对在部署 SiteScope 应用程序时执行的步骤的概述。

1. **准备一台要在其中安装和运行 SiteScope 应用程序的服务器。**

   备注:

   - 建议不要在一台计算机上安装多个 SiteScope。
   - 如果计划使用 SiteScope 故障转移来提供备份监控可用性以应对 SiteScope 服务器故障情况，请参阅位于 **<SiteScope 根目录>\sisdocs\pdfs\SiteScopeFailover.pdf** 的《HP SiteScope Failover Guide》。

2. **获取 SiteScope 可执行安装文件。**

   有关详细信息，请参阅安装流程 (第 73 页)。

3. **创建一个用于安装应用程序的目录，并根据需要设置用户权限。**

   备注: 必须创建一个新目录用于安装 SiteScope 11.30。不要将 SiteScope 11.30 安装到其旧版本的安装目录中。

4. **运行 SiteScope 可执行安装文件或安装脚本，引导脚本将应用程序安装到已准备好的位置。**

   有关详细信息，请参阅安装流程 (第 73 页)。

5. **如有必要，重新启动服务器（仅限 Windows 安装）。**

6. **通过使用兼容的 Web 浏览器与 SiteScope 连接来确认它是否正在运行。**

   有关详细信息，请参阅开始使用和访问 SiteScope (第 161 页)。

7. **执行安装后步骤来设置 SiteScope，以便其可用于生产。**

   有关详细信息，请参阅安装之后的管理任务 (第 162 页)。

第 9 章: 安装要求

本章包括:

系统要求

本节描述了在受支持的操作系统上运行 SiteScope 时所需的最低系统要求和推荐配置。

备注:
- 不再支持在 32 位 Windows 或 Linux 操作系统上安装 SiteScope，或在 64 位 Windows 操作系统上安装 32 位的该应用程序。只能将 SiteScope 作为 64 位应用程序安装并运行。
- 已弃用在 Solaris 平台上运行 SiteScope，Solaris 安装程序不再可用。
- 有关在不同环境中安装 SiteScope 的疑难解答和限制信息，请参阅疑难解答和限制 (第 78 页)。

本节包括以下主题:

系统硬件要求

硬件要求规范:

运算器/处理器	至少 1 个核心/2000 MHZ
内存	至少 2 GB 高负载环境通常为 8 GB 到 16 GB
可用磁盘空间	至少 10 GB
网卡	至少 1 个千兆物理网卡

虚拟化要求规范:

- 在所有受支持的操作系统上均支持使用 VMware 和 Hyper-V 虚拟机（请参阅针对 Windows 的服务器系统要求 (第 53 页)、针对 Linux 的服务器系统要求 (第 53 页)）。
- 为了获得更好的性能和稳定性，尤其在高负载 SiteScope 环境中，建议使用物理硬件。
- 对于 VMware，VMware 工具必须安装在来宾操作系统中。

已验证的配置

下列配置已在高负载环境下经过验证，可安装与 BSM 集成的 SiteScope。

操作系统	Microsoft Windows Server 2012 R2（64 位）
系统类型	ACPI 多处理器基于 x64 的 PC
CPU	4 个 2.67 GHz 的 Intel Xeon (R) x5650 物理处理器
总物理内存 (RAM)	16 GB
Java 堆内存	8192 MB
监控器总数	24,000
远程服务器总数	2,500
监控器每分钟运行次数	3,500

备注:

- 监控器容量和速度可受很多因素的显著影响，这些因素包括（但不限于）以下内容：SiteScope 服务器硬件、操作系统、修补程序、第三方软件、网络配置和体系结构、SiteScope 服务器与受监控服务器的相对位置、远程连接协议类型、监控器类型和监控器分布（按类型）、监控器频率、监控器执行时间、Business Service Management 集成以及数据库日志记录。
- 在高负载下工作时，应当在首次连接到 BSM 之前暂停所有监控器。

针对 Windows 的服务器系统要求

以下 Microsoft Windows 操作系统版本已获得认证:

- Microsoft Windows Server 2008 R2 SP1 Standard/Enterprise/Datacenter Edition（64 位）
- Microsoft Windows Server 2012 Standard/Datacenter Edition（64 位）
- Microsoft Windows Server 2012 R2 Standard Edition（64 位）

针对 Linux 的服务器系统要求

以下 Linux 操作系统版本已获得认证:

- Oracle Enterprise Linux (OEL) 6.0-6.5（64 位）
- CentOS 6.2（64 位）
- Red Hat ES/AS Linux 5.5-5.8、6.0-6.5（6.0、6.2、6.4、6.5 已获得认证）（64 位）

备注:

- 在安装 SiteScope 之前，必须手动配置 OEL 和 CentOS 环境。有关详细信息，请参阅在 Oracle Enterprise Linux 环境中安装 SiteScope (第 75 页)和在 CentOS 6.2 环境中安装 SiteScope (第 76 页)。

- 如果您计划将 SiteScope 与 HPOM 或 BSM 集成，则需要先配置 Red Hat ES Linux 6.0（64 位）环境的依赖关系，再安装 HP Operations Agent（需要代理将事件发送到以及将度量数据存储到 HPOM 或 BSM）。有关配置依赖关系和安装代理的详细信息，请参阅《Integrating SiteScope with HP Operations Manager Products Guide》，该文档在 SiteScope 帮助中或 HP 软件集成网站上提供。
- 在 Red Hat Linux 上安装了 SiteScope 后，SiteScope 服务器运行状况监控器需要 sar -W 和 sar -B 命令的有效输出，包括 SwapIns/sec、SwapOuts/sec、PageIns/sec 和 PageOuts/sec 计数器。如果这些命令不起作用，则不会抛出错误，并且这些计数器将显示为“暂缺”。要运行这些计数器，请通过添加命令“**/usr/local/lib/sa/sadc -**”编辑 crontab，使它们每天运行一次。
- 要监控在 Red Hat Linux 环境中运行的 SiteScope 或远程服务器的 CPU 和内存使用情况，必须在要监控的 SiteScope 服务器和所有远程服务器上安装 **sysstat** 程序包（没有预先提供）。
- 不支持带有本地 POSIX 线程库 (NPTL) 的 Red Hat Linux 9。
- 对于 Linux，要查看 SiteScope 中的特定报告元素，必须在运行 SiteScope 的服务器上安装并运行 X Window 系统。

客户端系统要求

使用以下软件的所有 Microsoft Windows 系统均支持 SiteScope 客户端：

支持的浏览器： SiteScope UI	• Microsoft Internet Explorer 9、10、11 **使用 Internet Explorer 10 的注意事项：** • 警报、监控器和以服务器为中心的报告仅支持使用“文档模式：Quirks”的兼容性模式；不支持默认的“文档模式：IE5 quirks”。要启用 **quirks** 模式，请打开警报、监控器或以服务器为中心的报告，然后按 F12。在开发人员工具中，选择“文档模式”**>**“Quirks”。 • 如果从“开始”屏幕中使用 Internet Explorer 10，则不会启用对 Java 等加载项的支持。要在 Internet Explorer 10 中使用 SiteScope，就必须切换到 Internet Explorer 桌面模式，并安装 Java。有关详细信息，请参阅 http://windows.microsoft.com/en-us/internet-explorer/install-java#ie=ie-10。 • Mozilla Firefox（最新认证版本）：31.2.0 ESR • Mac OS (10.10 Yosemite) 上的 Safari 8.0 **先决条件：** • 浏览器必须设置为接受第三方 Cookie 并允许会话 Cookie。 • 浏览器必须设置为启用 JavaScript 执行。 • 浏览器必须允许 SiteScope 应用程序的弹出窗口。 • （仅限 Safari）Java 插件必须在 **Preferences > Security > Manage Website Settings** 中单独为 SiteScope 主机或为所有站点设置为 **Run in Unsafe Mode**。
支持的浏览器：统一控制台（Multi-	• Google Chrome（最新认证版本）：34.0.1847.137 m • Mozilla Firefox（最新认证版本）：31.2.0 ESR • Safari（最新认证版本）：8.0（适用于 Mac）

View、事件控制台）	• Internet Explorer 9、10、11 **注意：**支持 Internet Explorer 9，但具有下列限制： • Microsoft Windows 7 N 版本上不支持此版本。 • Microsoft Windows Server 2008 上不支持此版本。 • 使用 Safari 的 iPad 3（具有最新更新的 iOS 7） • 使用 Chrome 34.0.1847 的 Android 平板电脑（全高清显示屏）
支持的浏览器： MyBSM 中的 SiteScope Multi-View 页面	• Internet Explorer 9、10、11 **注意：**虽然 Internet Explorer 8 可用于访问 MyBSM 中的 Multi-View 页面，但是它不再受正式支持。建议切换到受支持的浏览器之一，因为在 Internet Explorer 8 中，统一控制台中的事件控制台和选项卡功能将不起作用。
Java 插件（打开 SiteScope 用户界面时需要）	• **支持：**JRE 版本 6 或 7（最新认证版本为 JRE 7 update 67） • **建议：**JRE 7（请注意，我们计划在下一个 SiteScope 版本中弃用对 JRE 版本 6 的支持） **提示：**Java 将在安装 SiteScope 时安装，并且不应单独安装修补程序或更新。若要查看 Java 的版本，可以转到 **<SiteScope 安装文件夹>\java\bin** 并从命令行运行以下命令： java -server -fullversion

SiteScope 容量限制

- 当 SiteScope 与 BSM 集成时，执行超高负载的操作可能导致 SiteScope 出现问题。请根据下面的原则执行操作：
  - 不要一次对超过 3000 个监控器运行“发布模板更改向导”。
  - 不要通过运行“监控器部署向导”一次创建超过 3000 个监控器。
  - 不要在单次操作中复制/粘贴超过 3000 个监控器。
  - 不要通过执行“全局搜索和替换”一次为超过 2500 个监控器修改 Business Service Management 集成属性。
- 建议不要创建 1000 个以上使用 SSH 连接的监控器（假定使用默认参数设置，例如运行频率、连接数等）。如果您需要 1000 个以上使用 SSH 的监控器，则应添加其他 SiteScope 服务器。

提示: SiteScope 包括一个能帮助您预测系统行为和规划 SiteScope 容量的工具。有关详细信息，请参阅SiteScope 容量计算器 (第 37 页)。

SiteScope 支持列表

本节包括：

备注: SiteScope 11.30 与其他产品的共存部署既未经测试，也未获得认证。我们不支持也不推荐使用这种部署。

HP Business Service Management 集成支持列表

HP SiteScope 版本	HP Business Service Management 版本				
	9.25	9.2x	9.1x	9.0x	8.x
SiteScope 11.3x	√（建议）	√	√	√	√

HP Operations Manager (HPOM) 集成支持列表

有关最新版的支持列表，包括最新认证的服务包，请查看 HP 集成网站 (http://support.openview.hp.com/sc/solutions/index.jsp#tab=tab3)。

HPOM 版本	SiteScope 11.3x 集成			
	事件集成	节点搜寻集成	监控器搜寻集成	模板集成
HPOM for Windows 8.1x（带有 OMW_00149 修补程序）	支持	支持	支持	不支持
HPOM for Windows 9.0	支持	支持 OMW_00097/98 或更高版本（32 位/64 位）修补程序	支持	支持修补程序 159
HPOM for Linux/Solaris 9.0	支持	不支持	支持	支持
HPOM for Linux/Solaris 9.10	支持	支持 9.10.200 或更高版本修补程序	支持	支持修补程序 9.10.210 和 QCCR1A125751，或高于 9.10.210 的修补程序
HPOM for Linux/Solaris 9.20	支持	支持	支持	支持

备注: 有关 HP Operations Manager 硬件和软件配置的要求，请参阅相关版本的《Operations Manager for Windows/UNIX Installation Guide》，该指南可从 HP 软件支持网站获取。

HP Operations Agent 支持列表

HP SiteScope 版本	HP Operations Agent 版本
11.0x	8.60.70
11.1x	8.60.501
11.20 - 11.22	11.02.011
11.23	11.02.011, 11.13*
11.24	11.02.011, 11.13**, 11.14**
11.30	11.14***
*从已安装的 HP Operations Agent 11.02 升级到认证版本时受支持。 **HP Operations Agent 需要使用 SiteScope 配置工具进行单独安装和配置。 ***HP Operations Agent 不再包含在 SiteScope 安装程序或 SiteScope 配置工具中。必须手动安装并配置该代理。有关详细信息，请参阅《Integrating SiteScope with HP Operations Manager Products Guide》，该文档在 SiteScope 帮助中或 HP 软件集成网站上提供。	

备注:

- 安装 HP Operations Agent 需要 Microsoft Installer 4.5 或更高版本。
- 有关 HP Operations Agent 安装要求的详细信息，请参阅《HP Operations Agent 11.14 Installation Guide》，该指南可从 HP 软件支持网站获取。

HP SiteScope for Load Testing 支持列表

有关此版本中支持的 LoadRunner 和 Performance Center 版本的列表，请参考 HP 集成网站:

- HP Performance Center: http://support.openview.hp.com/sc/solutions/integrations.jsp?intid=599
- HP LoadRunner: http://support.openview.hp.com/sc/solutions/integrations.jsp?intid=587

备注: 需要 HP Passport 登录才能进行访问（请在 http://h20229.www2.hp.com/passport-registration.html 中注册 HP Passport）。

HP Network Node Manager i (NNMi) 支持列表

有关最新版的支持列表，包括最新认证的服务包，请查看 HP 集成网站 (http://support.openview.hp.com/sc/solutions/index.jsp#tab=tab3)。

集成	支持的版本
事件集	SiteScope 版本 11.10 或更高版本

成	NNMi 版本 9.10 或更高版本（9.21 是最新的 NNMi 认证版本）
度量集成	SiteScope 版本 11.10 或更高版本 NNMi 版本 9.10 或更高版本 NNM iSPI Performance for Metrics 版本 9.10 或更高版本（9.22 是最新的 NNMi 认证版本）

第 10 章: 升级 SiteScope

本章包括:

执行升级之前的准备工作

本节描述如何在最大限度地减少系统和操作中断的情况下，将现有的 SiteScope 安装升级到 SiteScope 11.30。

SiteScope 具有向后兼容性。这意味着，您可以安装更新版本的 SiteScope，并从现有 SiteScope 安装传输监控器配置。

在升级 SiteScope 之前，应考虑下列事项:

- 必须将 SiteScope 安装到系统要求 (第 52 页)中列出的支持的 Windows 或 Linux 环境中。
- 如果计划使 SiteScope 能够在其与 HP Operations Manager 或 BSM 集成时发送事件并充当度量数据的数据存储器，则必须在 SiteScope 服务器上安装 HP Operations Agent。有关安装代理的详细信息，请参阅《Integrating SiteScope with HP Operations Manager Products Guide》，该文档在 SiteScope 帮助中或 HP 软件集成网站上提供。
- 您可以通过使用配置工具备份当前 SiteScope 配置数据、卸载当前 SiteScope 版本、安装 SiteScope 11.30，然后将配置数据导回 SiteScope 来从 11.13 或 11.24 升级到 SiteScope 11.30。有关升级的详细信息，请参阅升级现有 SiteScope 安装 (第 63 页)。
- 您可以通过以下方式从 SiteScope 10.x 升级：先升级到 SiteScope 11.13 或 11.24，再将 SiteScope 11.13 或 11.24 升级到 SiteScope 11.30。有关升级说明，请参阅从 SiteScope 10.x 升级到 SiteScope 11.13 或 11.24 (第 65 页)。

注意事项和限制

- 不支持跨平台升级。
- 将 SiteScope Windows 配置导入 Linux 部署时（例如添加使用 NetBIOS 或 WMI 连接类型的 Windows 远程计算机时），可能会出现问题。请检查是否未使用特定于平台的监控器设置，如使用 WinInet 选项的 URL 监控器、Windows 远程计算机上的文件监控器或脚本监控器。
- 以下监控器已弃用。如果在先前的 SiteScope 版本中配置了这些监控器，则在执行升级后，这些监控器仍然会显示在 SiteScope 中（尽管仅限 32 位的监控器不会工作）。请注意，SiteScope 11.24 和更早版本支持这些监控器。

仅限 32 位的监控器 （无法在 64 位环境中运行）	32/64 位监控器
• Microsoft Exchange 2003 邮箱[1] • Microsoft Exchange 2003 公用文件夹[1] • Microsoft Windows Media Player [2] • Real Media Player[2] • Sybase • Tuxedo	• Microsoft Exchange 5.5 消息通信[1] • Microsoft Exchange 2000/2003 消息通信[1] • Microsoft Windows 拨号[2]
注意： [1] 建议迁移到 Microsoft Exchange 2007 或更高版本。 [2] 当前尚未在将来版本中计划。	

从 32 位迁移到 64 位 SiteScope

SiteScope 11.30 仅支持 64 位操作系统和 64 位 Java 版本。因此，在 SiteScope 11.30 中，不再存在 SiteScope 32 位和 64 位安装程序上的 SiteScope 32 位。

从 SiteScope 11.30 开始，将支持 64 位 Web 脚本监控器。要使用该监控器，必须在 SiteScope 服务器上安装 HP Load Generator 12.02，并指定 Load Generator 的路径。有关详细信息，请参阅《SiteScope Monitor Reference》指南中的 Web Script Monitor 部分。

其他 32 位监控器已弃用，在从 SiteScope 11.13 或 11.24 升级到 SiteScope 11.30 后不再有效。有关受影响的监控器和建议的备用监控器列表以及更多详细信息，请参阅执行升级之前的准备工作 (第 60 页)中的“注意事项和限制”部分。

要从 SiteScope 10.x（32 位版本）升级到 SiteScope 11.30（64 位版本），请执行以下操作:

1. 根据从 SiteScope 10.x 升级到 SiteScope 11.13 或 11.24 (第 65 页)中的步骤执行操作。
2. 根据将 SiteScope 11.13 或 11.24 升级到 SiteScope 11.30 (第 66 页)中的步骤执行操作（在步骤 5 中，确保在 64 位计算机上安装 SiteScope）。

升级现有 SiteScope 安装

备注: 本主题包含如何将 SiteScope 当前版本升级到 SiteScope 11.30 的说明。如果要安装 SiteScope 而不执行升级，请参阅安装工作流 (第 72 页)。

建议您执行以下步骤升级 SiteScope 的版本:

1. **请确保 SiteScope 进程/服务已停止（安装程序应在安装之前自动停止该进程）。**

   有关详细信息，请参阅在 Windows 平台上启动和停止 SiteScope 服务 (第 165 页)或在 Linux 平台上启动和停止 SiteScope 进程 (第 166 页)。

2. **使用当前版本 SiteScope 中的配置工具备份 SiteScope 监控器配置数据。**

   使用配置工具通过将 SiteScope 数据从当前的 SiteScope 导出供稍后导入 SiteScope 来备份当前的 SiteScope 安装目录。有关详细信息，请参阅备份 SiteScope 配置数据 (第 65 页)。

3. **卸载 SiteScope 当前版本，然后安装 SiteScope 11.30。**

   有关卸载 SiteScope 的详细信息，请参阅卸载 SiteScope (第 123 页)。

   在干净的目录结构中安装 SiteScope 11.30。为安装 SiteScope 创建的新目录必须命名为 SiteScope。有关安装 SiteScope 11.30 的详细信息，请参阅安装流程 (第 73 页)。

4. **导入新的 SiteScope 许可证。**

   要从 SiteScope 的较早版本升级到 SiteScope 11.30，请先与您的 HP 支持续订代表联系，请求产品合同迁移。完成合同迁移后，请访问“My Software Updates”门户 (https://h20575.www2.hp.com/usbportal/softwareupdate.do)，然后单击“Get Licensing”选项卡获取新的许可证密钥。

   收到许可证密钥后，打开 SiteScope，选择“首选项”>“常规首选项”，然后展开“许可证”面板。导入新的许可证文件。SiteScope 应开始运行。

   备注: 有关许可证购买查询（或如果需要额外容量），请与您的 HP 销售代表联系或使用 HP SiteScope 产品页面中的“Contact Us”链接。

5. **安装和配置 HP Operations Agent（将 SiteScope 与 HPOM 或 BSM 集成时需要）**

   有关安装和配置代理的详细信息，请参阅《Integrating SiteScope with HP Operations Manager Products Guide》，该文档在 SiteScope 帮助中或 HP 软件集成网站上提供。

6. **安装 Microsoft 修补程序。**

   为了改进 SiteScope 的扩展性和性能，我们建议安装 Microsoft 修补程序。有关详细信息，请参阅安装 Microsoft 修补程序 (第 164 页)。

7. **导入监控器配置数据。**

   安装之后，使用配置工具（从步骤 2）导入监控器配置数据。有关详细信息，请参阅导入配置数据 (第 65 页)。

8. **（可选）从较早版本的 SiteScope 导入数据后，通过运行批处理文件/start 命令 shell 脚本启动 SiteScope。**

   为避免当监控器运行时间超过 15 分钟时 SiteScope 在升级后自行重新启动的问题，请从 **<SiteScope 根目录>\bin** 目录（Windows 平台）运行 **go.bat** 文件，或通过使用语法 <安装路径>/SiteScope/start（Linux 平台）运行 start 命令 shell 脚本来启动 SiteScope。

9. **如果使用 SiteScope 故障转移，则使用对应的 SiteScope 故障转移版本升级故障转移服务器。**

在升级主服务器之后，使用对应的 SiteScope 故障转移版本升级故障转移服务器，然后将故障转移服务器连接到已升级的主服务器。有关详细信息，请参阅《SiteScope 故障转移 Guide》中的“Upgrading SiteScope 故障转移”部分。

备份 SiteScope 配置数据

为 SiteScope 升级做准备的最简单方法是，使用“配置工具”来生成当前 SiteScope 安装目录以及其中所需子目录的备份。通过使用配置工具，您可以将模板、日志、监控器配置文件、服务器证书、脚本等 SiteScope 数据从当前 SiteScope 导出，以便将来导入 SiteScope。用户数据将导出为 **.zip** 文件。

另外，还可以手动备份 SiteScope 安装。有关详细信息，请参阅在无法启动 SiteScope 时备份和恢复 SiteScope 安装 (第 169 页)。

备注: 由于导出 SiteScope 数据时不会复制 **<SiteScope>\htdocs** 目录，因此需要备份此目录，并在升级后将其复制到 SiteScope 11.30 目录，以便查看旧报告。

有关如何使用配置工具导出 SiteScope 数据的详细信息，请参阅使用 SiteScope 配置工具 (第 107 页)。

另外，还可以在安装过程中导出 SiteScope 数据。有关详细信息，请参阅安装工作流 (第 72 页)。

导入配置数据

升级 SiteScope 后，可以使用配置工具从较早版本的 SiteScope 复制监控器配置数据。有关详细信息，请参阅使用 SiteScope 配置工具 (第 107 页)。

另外，如果手动创建了备份，则必须从新安装目录中删除已备份的所有文件夹和文件，然后，将备份的文件夹和文件复制到安装目录。有关详细信息，请参阅在无法启动 SiteScope 时备份和恢复 SiteScope 安装 (第 169 页)。

从 SiteScope 10.x 升级到 SiteScope 11.13 或 11.24

因为 SiteScope 不支持直接从 SiteScope 10.x 升级到 11.30，所以您必须先升级到 SiteScope 11.13 或 11.24，然后再将 SiteScope 11.13 或 11.24 升级到 SiteScope 11.30。

备注: 我们建议先将 SiteScope 10.x 版本更新到 SiteScope 10.14，再升级到 SiteScope 11.13 或 11.24。

要进行升级，请执行以下操作:

1. 停止 SiteScope 服务。
2. 从 SiteScope 10.x 导出 SiteScope 配置（升级到 SiteScope 10.14 后更佳）。
   a. 备份 SiteScope 10.x 文件夹（将其复制到系统上的某个临时文件夹）。
   b. 导出 SiteScope 配置:
      - 启动 SiteScope 配置工具（“开始”>“程序”>“HP SiteScope”>“配置工具”），然后单击“下一步”。
      - 选择“导出/导入用户数据”，然后单击“下一步”。
      - 选择“导出用户数据”，然后单击“下一步”。
      - 选择 SiteScope 10.x 安装目录位置，以及要用于保存导出数据的目标目录。输入备份文件名。如果要为旧数据生成报告，请选择“包括日志文件”。

- 导出完成后，单击“下一步/完成”。
- 将用于各种监控器（例如 SAP 客户端和 JDBC 驱动程序）的第三方库和 jar 文件复制到临时目录，这是因为在导出中不会包括这些文件。

3. 卸载 SiteScope 10.x。
   a. 选择“开始”>“设置”>“控制面板”>“添加或删除程序”。
   b. 此时将启动卸载窗口。连续单击“下一步”，将开始卸载。
   c. 卸载完成后，单击“完成”。
   d. 删除 SiteScope 目录下的任何剩余文件。
   e. 确定已通过卸载过程从 Windows 服务中删除 **SiteScope** 服务。如果仍然显示 SiteScope 服务，则可通过从命令提示符运行“sc delete SiteScope”，手动删除该服务。
   f. 重新启动服务器。
4. 安装 SiteScope 11.10 或 11.20，然后安装从 HP 软件支持网站的“Software Patches”部分获取的最新次次版本（11.13 或 11.24）。
5. 将数据导入 SiteScope 11.13 或 11.24:
   - 运行配置工具（“开始”>“程序”>“HP SiteScope”>“配置工具”），然后单击“下一步”。
   - 选择“导入配置”，然后单击“下一步”。
   - 单击“下一步”。
   - 选择先前从 10.x 安装导出的 **.zip** 文件，并验证目标目录是否正确，然后单击“下一步”。
   - 导入完成后，单击“完成”（此时将关闭配置工具）。

     备注: 再次运行配置工具，并选择“调整大小”选项。

   - 如果要使用之前生成的报告，请将现有的 **<SiteScope>\htdoc** 文件夹替换为在步骤 2a 中从之前的 SiteScope 备份的 **\htdocs** 文件夹。
6. 启动带有 SiteScope 10.x 配置的 SiteScope 11.13 或 11.24。SiteScope 将升级该配置。
7. 继续执行将 SiteScope 11.13 或 11.24 升级到 SiteScope 11.30 (第 66 页)中的步骤

将 SiteScope 11.13 或 11.24 升级到 SiteScope 11.30

建议您执行以下步骤以从 SiteScope 11.13 或 11.24 升级到 SiteScope 11.30:

要进行升级，请执行以下操作:

1. 停止 SiteScope 服务。
2. 备份 SiteScope 11.13 或 11.24 文件夹（将其复制到系统上的某个临时文件夹）。
3. 从 SiteScope 11.13 或 11.24 导出 SiteScope 配置:
   - 启动 SiteScope 配置工具（“开始”>“程序”>“HP SiteScope”>“配置工具”），然后单击“下一步”。

- 选择“导出配置”，然后单击“下一步”。
- 在“导出配置”屏幕中，选择 SiteScope 11.13 或 11.24 安装目录位置，以及要用于保存导出数据的目标目录。输入备份文件名。如果要为旧数据生成报告，请选择“包括日志文件”。
- 导出完成后，单击“下一步/完成”。
- 将用于各种监控器（例如 SAP 客户端和 JDBC 驱动程序）的第三方库和 jar 文件复制到临时目录，这是因为在导出中不会包括这些文件。

4. 卸载 SiteScope 11.13 或 11.24（“开始”>“设置”>“控制面板”>“添加或删除程序”）：
   a. 此时将启动卸载窗口。连续单击“下一步”，将开始卸载。
   b. 卸载完成后，单击“完成”。
   c. 删除 SiteScope 目录下的任何剩余文件。
   d. 确定已通过卸载过程从 Windows 服务中删除 **SiteScope** 服务。如果仍然显示 SiteScope 服务，则可通过从命令提示符运行“sc delete SiteScope”，手动删除该服务。
   e. 重新启动服务器。
5. 安装 SiteScope 11.30：
   a. 运行 SiteScope 11.30 安装程序，然后单击“下一步”。
   b. 接受许可证协议并单击“下一步”。
   c. 为 SiteScope 11.30 选择目录，然后单击“下一步”。
   d. 选择“HP SiteScope”安装类型，然后单击“下一步”。
   e. 保留默认端口，然后单击“下一步”。如果使用默认端口，则输入 8088。
   f. 将许可证留空，然后单击“下一步”。
   g. 在概要屏幕中单击“下一步”。
   h. 安装完成后，单击“下一步”（此时将关闭安装程序窗口）。
   i. 恢复之前（在步骤 3 中）复制到临时文件夹的第三方库和 jar。
   j. 停止 SiteScope 服务。
6. 将 SiteScope 服务设置为在监控帐户下运行。
7. 将数据导入 SiteScope：
   - 运行配置工具（“开始”>“程序”>“HP SiteScope”>“配置工具”），然后单击“下一步”。
   - 选择“导入配置”，然后单击“下一步”。
   - 在“导入配置”屏幕中，选择先前从 11.13 或 11.24 安装导出的 zip 文件，并验证目标目录是否正确，然后单击“下一步”。
   - 导入完成后，单击“完成”（此时将关闭配置工具）。

     备注: 再次运行配置工具，并选择“调整大小”选项。

   - 如果要使用之前生成的报告，请将现有的 **<SiteScope>\htdoc** 文件夹替换为在步骤 2 中从之前的 SiteScope 备份的 **\htdocs** 文件夹。

8. 在 **master.config** 文件中更改数据简化以及其他参数:
   - 打开 **<SiteScope 根目录>\groups\master.config**。
   - 将行 **_topazEnforceUseDataReduction=** 更改为 **_topazEnforceUseDataReduction=false**。

     备注: 如果此参数不存在，则添加此参数，将其设置为 false。
   - 将行 **_suspendMonitors=** 更改为 **_suspendMonitors=true**。
   - 添加参数 **_disableHostDNSResolution=true**。

     备注: 应按字母顺序添加所有参数。
   - 保存并关闭 **master.config** 文件。
9. 启动 SiteScope 服务。SiteScope 将升级配置并重新启动。在用户界面中登录，并在“首选项”>“集成设置”下验证到 BSM 的集成是否正确。
10. 请与您的 HP 支持续订代表联系，请求产品合同迁移。完成合同迁移后，请访问“My Software Updates”门户 (https://h20575.www2.hp.com/usbportal/softwareupdate.do)，然后单击“Get Licensing”选项卡获取新的许可证密钥。

    收到许可证密钥后，打开 SiteScope，选择“首选项”>“常规首选项”，展开“许可证”面板，然后导入新的许可证文件。

    备注: 有关许可证购买查询（或如果需要额外容量），请与您的 HP 销售代表联系或使用 HP SiteScope 产品页面中的“Contact Us”链接。
11. 停止 SiteScope。
12. 打开 **master.config** 文件并执行以下操作:
    - 将 **_suspendMonitors=true** 更改为 **_suspendMonitors=** 取消暂停监控器。
    - 将 **_topazEnforceUseDataReduction= false** 更改为 **_topazEnforceUseDataReduction=** 启用数据简化。
    - 更改参数 **_disableHostDNSResolution=false** 的值。
    - 保存并关闭 **master.config** 文件，然后启动 SiteScope。

疑难解答和限制

本节描述有关 SiteScope 升级过程的疑难解答和限制。

备注: 您还可以在自助解决知识搜索中查看与升级 SiteScope 有关的其他信息。要访问该知识库，必须使用 HP Passport ID 登录。

升级后首次重新启动 SiteScope 时可能需要很长的时间

问题： 升级后首次重新启动 SiteScope 可能需要很长的时间（超过 15 分钟）。如果在 15 分钟之后监控器仍未开始运行，则 SiteScope 会重新启动。

可能的解决方案：

为避免当监控器运行时间超过 15 分钟时 SiteScope 自行重新启动的问题，请从 **<SiteScope 根目录>\bin** 目录（Windows 平台）运行 **go.bat** 文件，或通过使用语法 **<安装路径>/SiteScope/start**（Linux 平台）运行 start 命令 shell 脚本来启动 SiteScope。

禁用指向未运行的环境的所有监控器。这样做可以缩短等待系统应答的时间。

SiteScope 无法获取客户 ID

问题： 在 9.0 之前的 SiteScope 版本中，当 SiteScope 连接到 BSM 时，SiteScope 会将客户 ID 存储在 **<SiteScope 根目录>\cache\persistent\TopazConfiguration** 下的设置文件中。

升级到 9.x 之后，首次加载 SiteScope 时，SiteScope 会尝试读取此设置文件，并检索 BSM 连接详细信息。如果此文件损坏（可能是由导出配置执行错误导致的），SiteScope 可能无法获取客户 ID，并将尝试从 BSM 进行检索。如果 BSM 在重新启动期间关闭，则 SiteScope 将无法检索客户 ID，且 SiteScope 会再次重新启动。

可能的解决方案： 在升级完成后启动 SiteScope 之前，请确保所有连接到 SiteScope 的 BSM 均已启动并运行。

默认警报操作根据操作类型进行命名

问题： 向 SiteScope 9.0 添加警报操作。升级到 SiteScope 9.0 或更高版本时，会创建默认的警报操作，并根据操作类型（例如，电子邮件、寻呼机或 SMS）对其命名。如果需要使默认名称与保持操作的警报串联，则可能会造成问题。

可能的解决方案： 在升级前，打开位于 **<SiteScope 根目录>\groups** 中的 **master.config** 文件，并将 **_AlertActionCompositeNameDelimiter** 关键字更改为包含要出现在串联中的分隔符。

BSM/ServiceCenter 或 Service Manager 集成

如果要从 10.00 之前的版本升级 SiteScope，并正在使用 BSM/ServiceCenter 或 Service Manager 集成，则应注意本事项。在 SiteScope 中设置 ServiceCenter 监控器时，会创建名为 **peregrine.jar** 的文件，并将该文件置于 SiteScope 计算机上的 **WEB-INF\lib** 目录中。在升级 SiteScope 前必须备份此文件，否则文件会在升级过程中删除。升级完成后，将备份的 **peregrine.jar** 文件复制回 **WEB-INF\lib** 目录。

SiteScope 升级失败

如果升级过程失败，请检查位于 <**SiteScope 根目录>\logs** 目录下的 **upgrade.log** 文件，了解升级失败的原因。

在 Windows 环境上安装 SiteScope 时，如果升级过程失败，SiteScope 将继续尝试执行重新启动。

可能的解决方案：再次执行 SiteScope 安装。

在与 BSM 集成的情况下，将 SiteScope 移到其他服务器

如果要将 SiteScope 服务器移动到新硬件（具有新主机名和 IP 地址），并且要使用 BSM 集成，则需执行此过程。请执行以下步骤以最大程度地减小对集成的影响：

1. 生成当前 SiteScope 安装的备份。有关详细信息，请参阅备份 SiteScope 配置数据 (第 65 页)。
2. 在新硬件上安装 SiteScope，并且将 SiteScope 配置数据导入到 SiteScope 安装目录。有关详细信息，请参阅导入配置数据 (第 65 页)。
3. 使用旧硬件上的相同端口号配置 SiteScope 服务器。
4. 在 BSM 中执行以下操作：
   - 在“新 SiteScope”页面中更新 SiteScope 配置文件的相关字段。
   - 在 HOSTS 表中更新有关 SiteScope 计算机的信息。

第 3 部分: 安装 SiteScope

第 11 章: 安装工作流

本章包括:

安装版本类型

SiteScope 作为 64 位应用程序安装并运行。它是一个自解压的可执行文件和程序包文件夹。对于主版本或次版本，此文件在 SiteScope 安装程序包（zip 文件）中提供。

对于次次版本和修补程序版本，请从 HP 软件支持网站上的“Software Patches”门户下载此文件。

备注: SiteScope 次次版本和修补程序版本只应基于标准 SiteScope 安装进行安装，而不能基于 SiteScope 故障转移或系统运行状况等非标准安装。

如果想要安装最新可用版本，则必须先安装 SiteScope 11.30，然后再安装适用于次次版本的最新累积/中间修补程序（如 HP 支持网站上的适用于 11.30 版的“Patches”部分中所示）。

正式名称	版本类型	示例	安装
重大 次版本	完整安装程序版本	10.0, 11.0 10.10, 11.30 示例文件名: HPSiteScope_11.30_setup.exe	安装在一个干净的系统上，然后导入先前版本的配置。首次启动时将执行升级。
次次（修补程序）	相应主版本或次版本缺陷修复的集合	10.11（基于 10.10） 11.01（基于 11.00） 11.24（基于 11.20 或 11.2x） 示例文件名: HPSiS1122_11.24_setup.exe	次次修补程序基于其相应版本安装。不需要升级。
累积/中间/公共修补程序	包含用于紧急缺陷的正式修复的程序包	SS1122130529 SS<版本><日期>	只能基于单个专用的主版本、次版本或次次版本安装。

正式名称	版本类型	示例	安装
		示例文件名: SS1122130529-11.22.000-WinNT4.0.msi	

安装流程

此主题包含有关安装 SiteScope 11.30 的说明。

备注: 如果计划从现有版本的 SiteScope 升级，请按照升级现有 SiteScope 安装 (第 63 页)中的说明操作。

1. **安装先决条件（仅限 Linux）。**
   a. 选择合适的安装位置并设置帐户权限。有关详细信息，请参阅为 Linux 安装做准备 (第 75 页)。
   b. 如果在以下任一平台上安装 SiteScope，则需要在安装 SiteScope 前手动配置环境:

平台	安装先决条件
Oracle Enterprise Linux 6.0、6.1	请参阅在 Oracle Enterprise Linux 环境中安装 SiteScope (第 75 页)。
CentOS 6.2	请参阅在 CentOS 6.2 环境中安装 SiteScope (第 76 页)。
在 CentOS 6.2 操作系统上运行的 HP Cloud Services (HPCS) 实例	请参阅在运行于 CentOS 6.2 上的 HP Cloud Services 实例上安装 SiteScope (第 76 页)。
Red Hat ES/AS Linux 6.0	如果您计划将 SiteScope 与 HPOM 或 BSM 集成，则需要先配置 Red Hat ES Linux 6.0（64 位）环境的依赖关系，再安装 HP Operations Agent（需要代理将事件发送到以及将度量数据存储到 HPOM 或 BSM）。有关配置依赖关系和安装代理的详细信息，请参阅《Integrating SiteScope with HP Operations Manager Products Guide》，该文档在 SiteScope 帮助中或 HP 软件集成网站上提供。

2. **下载 SiteScope 11.30。**
   a. 将特定于平台的安装包（**SiteScope_11.30_Windows.zip** 或 **SiteScope_11.30_Linux.zip**）下载到要安装 SiteScope 的计算机上。可通过 HP 系统从以下途径获得 SiteScope:

客户	下载选项
评估客户	电子下载评估链接 HP 授权的软件合作伙伴可使用 HP 软件合作伙伴中心 （以上链接需要 HP Passport 帐户。请转到 http://h20229.www2.hp.com/passport-registration.html 注册 HP Passport。）
新客户	电子软件下载。客户通过电子邮件接收软件下载链接；该链接特定于订购者。
现有客户更新	https://h20575.www2.hp.com/usbportal/softwareupdate.do **先决条件：** i. 访问以上链接需要 HP Passport 帐户以及支持协议 ID (SAID)，用于通过 SSO 门户接收更新。要注册 HP Passport，请参阅 http://h20229.www2.hp.com/passport-registration.html。有关激活 SAID 的详细信息，请参阅软件联机支持网站上的常见问题解答。 ii. 软件升级需要新的许可证密钥。请先与您的 HP 支持续订代表联系，请求产品合同迁移。完成合同迁移后，请访问“My Software Updates”门户 (https://h20575.www2.hp.com/usbportal/softwareupdate.do)，然后单击“Get Licensing”选项卡获取新的许可证密钥。 **要下载软件更新，请执行以下操作：** i. 选择“My software updates”。 ii. 展开“Application Performance Management”，选择所需的 HP SiteScope 11.30 软件电子介质，然后单击“Get software updates”。 iii. 在“Selected Products”选项卡中，单击所需产品更新的“Get Software”，然后根据网站上的说明下载软件。

b. 将压缩文件提取到合适的目录。

3. **安装 SiteScope 11.30。**

使用以下任一安装选项安装 SiteScope：

操作系统	安装选项
Windows	• 用户界面可执行文件（安装向导）。有关详细信息，请参阅使用安装向导进行安装 (第 80 页)。 • 静默安装。有关详细信息，请参阅在静默模式下安装 SiteScope (第 105 页)。
Linux	• 用户界面可执行文件（安装向导）。有关详细信息，请参阅使用安装向导进行安装 (第 80 页)。 • 使用命令行输入进行的控制台模式安装脚本。有关详细信息，请参阅使用控制台模式在 Linux 上执行安装 (第 99 页)。 • 静默安装。有关详细信息，请参阅在静默模式下安装 SiteScope (第 105 页)。

备注:

- Windows 安装不支持控制台模式安装。
- 如果已安装了 SiteScope 的一个现有版本，则必须将其卸载后，才能安装 SiteScope 11.30。
- 如果先前使用配置工具导出了 SiteScope 数据（有关详细信息，请参阅使用 SiteScope 配置工具 (第 107 页)），则可以导入用户数据 **.zip** 文件。
- 如果具有第三方中间件和驱动程序，则必须手动复制或安装这些程序。

4. **安装和配置 HP Operations Agent（将 SiteScope 与 HPOM 或 BSM 集成时需要）**

   有关安装和配置代理的详细信息，请参阅《Integrating SiteScope with HP Operations Manager Products Guide》，该文档在 SiteScope 帮助中或 HP 软件集成网站上提供。
5. **安装 Microsoft 修补程序。**

   为了改进 SiteScope 的扩展性和性能，我们建议安装 Microsoft 修补程序。有关详细信息，请参阅安装 Microsoft 修补程序 (第 164 页)。
6. **连接到 SiteScope。**

   有关详细信息，请参阅连接到 SiteScope (第 166 页)。

为 Linux 安装做准备

如果准备在 Linux 上安装 SiteScope，则需要根据环境选择合适的安装位置并设置帐户权限。

要准备在 Linux 上安装 SiteScope，请执行以下操作：

1. 验证 SiteScope 应用程序的安装位置 (/opt/HP/SiteScope) 中是否有足够的磁盘空间可用于安装和运行 SiteScope。
2. 创建用于运行 SiteScope 应用程序的非 root 用户帐户，然后为此用户设置对 /opt/HP/SiteScope 的帐户权限。设置帐户的默认 shell。有关详细信息，请参阅配置有权运行 SiteScope 的非 root 用户帐户 (第 35 页)。

备注:

- 不能在安装期间更改 Linux 安装目录，最好也不要在安装完成后对其进行更改。
- 虽然 SiteScope 要求具有高级帐户权限才能启用全方位的服务器监控，但是建议您不要从 root 帐户运行 SiteScope，也不要将 SiteScope 配置为使用 root 帐户访问远程服务器。
- 还可以使用静默安装方式安装 SiteScope。有关详细信息，请参阅在静默模式下安装 SiteScope (第 105 页)。

在 Oracle Enterprise Linux 环境中安装 SiteScope

在 Oracle Enterprise Linux 上安装 SiteScope 之前，必须在环境中安装以下依赖项:

- glibc-2.12-1.25.el6.i686.rpm
- glibc-common-2.12-1.25.el6.i686.rpm
- nss-softokn-freebl-3.12.9-3.el6.i686.rpm

- libXau-1.0.5-1.el6.i686.rpm
- libxcb-1.5-1.el6.i686.rpm
- libX11-1.3-2.el6.i686.rpm

通过运行以下命令，您可以使用 Oracle Enterprise Linux 提供的 yum 包管理器安装这些依赖项:

yum install -y glibc glibc-common nss-softokn-freebl libXau libxcb libX11 libXext

您可以在所有基于 Red Hat 的系统的默认库 (**/etc/yum.repos.d**) 中找到这些相关程序。

在 CentOS 6.2 环境中安装 SiteScope

在 CentOS 6.2（64 位）上安装 SiteScope 之前，请确保在 Linux 环境中安装以下附加库之一（推荐第一个选项）:

- 通过执行以下命令安装 **glibc.i686** 和 **libXp.i686** 库:

  [root@centos ~]# yum install glibc.i686 libXp.i686
- 检查是否已安装了任何 JRE，以及指向 JRE 的路径拼写是否正确:

  [root@centos ~]# java -version
  java version "1.6.0_22"
  OpenJDK Runtime Environment (IcedTea6 1.10.6) (rhel-1.43.1.10.6.el6_2-x86_64)
  OpenJDK 64-Bit Server VM (build 20.0-b11, mixed mode)

  如果出现“未找到命令”错误，则应安装 JRE。请使用以下命令安装 JRE:

  root@centos ~]# yum install java-1.6.0-openjdk

备注: 通常 CentOS 在安装时已安装了所有库。在这种情况下，安装程序会使用 glibc.i686，因为 JRE 依赖于 glibc 和 libXp。由于 SiteScope 自身包含了 java，因此仅在运行安装程序时需要该 JRE。

在 CentOS 6 服务器上安装 SiteScope 的提示:

检查 CentOS 6.2 服务器的主机名，并确保该主机已解析。

1. 通过运行主机名命令获取主机名。
2. 运行 ping <您的主机名>。如果 ping 请求成功，则表示主机已经可解析。
3. 如果 ping 请求失败，请使用 ifconfig 查找您的 IP。
4. 运行 echo "<您的 ip> <您的主机名>" >> /etc/hosts，将带有与主机名相对应 IP 的字符串添加到 hosts 文件中。
5. 再次运行 ping <您的主机名>，以确保主机已解析。

   如果无法解析主机名，SiteScope 可能因此而无法启动。

在运行于 CentOS 6.2 上的 HP Cloud Services 实例上安装 SiteScope

在 CentOS 6.2 操作系统上运行的 HP Cloud Services (HPCS) 实例可支持 SiteScope。

关于在 HPCS 上安装 SiteScope 的提示:

1. **检查 HP Cloud Services 服务器的主机名，并确保该主机已解析。**
   a. 通过运行主机名命令获取主机名。
   b. 运行 ping <您的主机名>。如果 ping 请求成功，则表示主机已经可解析。
   c. 如果 ping 请求失败，请使用 ifconfig 查找您的 IP。
   d. 运行 echo "<您的 ip> <您的主机名>" >> /etc/hosts，将带有与主机名相对应 IP 的字符串添加到 hosts 文件中。
   e. 再次运行 ping <您的主机名>，以确保主机已解析。
2. **检查交换大小。**
   a. 运行 free 命令，确保已创建了交换空间。
   b. 如果发现缺少交换:

      [root@centos ~]# free | grep Swap
      Swap: 0 0 0

      运行以下命令:

      创建一个 2 GB 的文件:

      [root@centos ~]# dd if=/dev/zero of=/swapfile bs=1M count=2048

      将其初始化为交换:

      [root@centos ~]# mkswap /swapfile

      将其启用:

      [root@centos ~]# swapon /swapfile

   c. 再次检查交换:

      root@centos ~]# free | grep Swap
      Swap: 2097144 0 2097144
3. **安装附加库。**
   有关详细信息，请参阅在 CentOS 6.2 环境中安装 SiteScope (第 76 页)。

安全组配置

IP 协议	起始端口	终止端口	类型	CIDR IP
tcp	8080	8080	IP	0.0.0.0/0
tcp	22	22	IP	0.0.0.0/0
tcp	8888	8888	IP	0.0.0.0/0
icmp	-1	-1	IP	0.0.0.0/0

在 HPCS 上安装 SiteScope

要在 HPCS 上安装 SiteScope，请执行以下操作:

1. 将当前目录更改为 SiteScope 安装程序所在的位置，然后运行 SiteScope 安装程序：
   [root@centos ~]# sh ./HPSiteScope_11.30_setup.bin -i console
2. 使用控制台模式安装 SiteScope。有关详细信息，请参阅使用控制台模式在 Linux 上执行安装 (第 99 页)。
3. 安装完成后，运行 SiteScope：
   [root@centos ~]# /opt/HP/SiteScope/start
4. 等待几分钟，直到 SiteScope 服务启动，然后检查必需的进程是否正在运行：
   [root@centos ~]# ps -ef | grep SiteScope | grep -v grep |awk '{print $3}'84758477
   最后一个命令将显示 SiteScope 进程的进程 ID。如果有两个进程，则说明 SiteScope 服务器已成功启动。

注意事项和限制情况

目前不支持在 CentOS 6.2 服务器中安装的 SiteScope 11.30 上进行 Operations Manager 集成。

疑难解答和限制

本节描述有关安装 SiteScope 的疑难解答和限制。

可能无法使用控制台模式在 Linux 上安装 SiteScope

如果打开的 X 会话过多，则在 Linux Red Hat 环境中使用控制台模式安装 SiteScope 时会失败。

解决方法：关闭一些 X 会话，或清除 DISPLAY 变量。

安装 HP Operations Agent 时出错 - 查看日志文件

如果在安装 HP Operations Agent 时遇到错误，或者希望查看安装状态，请查看以下日志文件：

- SiteScope 日志。该日志仅会显示安装是否已成功。
  日志文件名：**HPSiteScope_config_tool.log**
  日志文件位置：
  - **win- %temp%**（Windows 平台）
  - **/temp** 或 **/var/temp**（UNIX/Linux 平台）
    （搜索“installOATask”的结果）
- HP Operations Agent 日志文件。
  日志文件名：**oainstall.log**、**oapatch.log**
  日志文件位置：

- **%ovdatadir%\log**（Windows 平台）
- **/var/opt/OV/log/**（UNIX/Linux 平台）

卸载 SiteScope 之后，后续的 SiteScope 安装失败

卸载 SiteScope 之后，无法完成后续安装，并显示以下消息：“Please enable windows scripting host”。这是因为 Windows 无法解析 PATH 环境变量中的 %SystemRoot% **变量（即使** %SystemRoot% **确实出现在路径中）。**

解决方法：将 PATH 环境变量中的 %SystemRoot% **变量替换为 C:\Windows\system32 的实际路径。**

第 12 章: 使用安装向导进行安装

可使用安装向导按照下列步骤在受支持的 Windows 或 Linux 环境中安装 SiteScope。有关受支持环境的列表，请参阅系统要求 (第 52 页)。

如果服务器上已安装了 X11 库，则安装向导会自动执行。如果没有安装这些库，您可以执行以下任一操作：

- 在没有 X11 服务器的计算机上以图形模式安装 SiteScope。有关详细信息，请参阅在无 X11 服务器的计算机上使用安装向导安装 SiteScope (第 97 页)。
- 在 Linux 平台上以控制台模式安装 SiteScope。有关详细信息，请参阅使用控制台模式在 Linux 上执行安装 (第 99 页)。

备注:

- 还可以使用静默安装方式安装 SiteScope。有关详细信息，请参阅在静默模式下安装 SiteScope (第 105 页)。
- 如果计划升级现有版本的 SiteScope，请按照升级现有 SiteScope 安装 (第 63 页)中的步骤操作。
- 配置向导和配置工具中已删除直接从 SiteScope 安装和卸载 HP Operations Agent 的选项。必须手动安装并配置该代理。如果 SiteScope 与 HPOM 或 BSM 集成，则需要使用该代理发送事件和存储度量数据（使用 BSM 中的配置文件数据库将度量数据绘制到性能图的情况除外）。 有关安装和配置代理的详细信息，请参阅《Integrating SiteScope with HP Operations Manager Products Guide》，该文档在 SiteScope 帮助中或 HP 软件集成网站上提供。

要安装 SiteScope，请执行以下操作：

1. 获取 SiteScope 安装包。
   a. 将特定于平台的安装包（**SiteScope_11.30_Windows.zip** 或 **SiteScope_11.30_Linux.zip**）下载到要安装 SiteScope 的计算机上。可通过 HP 系统从以下途径获得 SiteScope：

客户	下载选项
评估客户	电子下载评估链接 HP 授权的软件合作伙伴可使用 HP 软件合作伙伴中心 **注意：** 以上链接需要 HP Passport 帐户。请转到 http://h20229.www2.hp.com/passport-registration.html 注册 HP Passport。
新客户	电子软件下载。客户通过电子邮件接收软件下载链接；该链接特定于订购者。
现有客户更新	https://h20575.www2.hp.com/usbportal/softwareupdate.do **先决条件：** i. 访问以上链接需要 HP Passport 帐户以及支持协议 ID (SAID)，用于通过 SSO 门户接收更新。要注册 HP Passport，请参阅 http://h20229.www2.hp.com/passport-registration.html。有关激活 SAID 的详细信息，请参阅软件联机支持网站上的常见问题解答。

客户	下载选项
	ii. 软件升级需要新的许可证密钥。请先与您的 HP 支持续订代表联系，请求产品合同迁移。完成合同迁移后，请访问“My Software Updates”门户 (https://h20575.www2.hp.com/usbportal/softwareupdate.do)，然后单击“Get Licensing”选项卡获取新的许可证密钥。 **要下载软件更新，请执行以下操作：** i. 选择“My software updates”。 ii. 展开“Application Performance Management”，选择所需的 HP SiteScope 11.30 软件电子介质，然后单击“Get software updates”。 iii. 在“Selected Products”选项卡中，单击所需产品更新的“Get Software”，然后根据网站上的说明下载软件。

b. 将压缩文件提取到合适的目录。

2. 根据操作环境运行 SiteScope 安装。请注意，SiteScope 仅作为 64 位应用程序安装和运行。

对于 Windows：

a. 运行 **HPSiteScope_11.30_setup.exe**。

b. 根据操作环境和体系结构，输入要从其安装 SiteScope 的位置，后跟可执行文件的名称。

例如：

<SiteScope 安装目录>\HPSiteScope_11.30_setup.exe

对于 Linux：

a. 以 **root** 用户身份登录服务器。

b. 通过输入以下内容运行安装程序：**./HPSiteScope_11.30_setup.bin**。

备注： 如果服务器上正在运行 Microsoft 终端服务器服务，则当您安装 SiteScope 时，该服务必须处于“安装模式”。如果该服务的模式不正确，向导会显示错误消息，然后退出安装。使用 **change user** 命令可更改为安装模式。有关详细信息，请参阅 Microsoft 支持站点 (http://support.microsoft.com/kb/320185)。

3. 此时将显示“选择区域设置”屏幕。

从列出的语言中选择安装 SiteScope 的语言。取决于操作系统的区域设置，安装程序会列出不同的语言。有关 SiteScope 用户界面支持的语言的列表，请参阅《使用 SiteScope》指南中的“SiteScope 国际化”部分。

单击“确定”继续安装。此时将显示“初始化”屏幕。

如果安装程序检测到系统上正在运行任何杀毒程序，则会提示您在继续安装之前检查警告。

4. 查看“应用程序要求”检查警告屏幕中显示的警告（如果有），然后按照屏幕中的说明执行操作。

如果安装程序检测到防病毒程序，则可以尝试在不禁用防病毒程序的情况下安装 SiteScope。

单击“继续”继续安装。

5. **在打开的“(安装)简介”屏幕中，单击“下一步”。**

6. 此时将打开“许可证协议”屏幕。

阅读 SiteScope 许可证协议。

要安装 SiteScope，请选择“我接受‘许可证协议’的条款”，然后单击“下一步”。

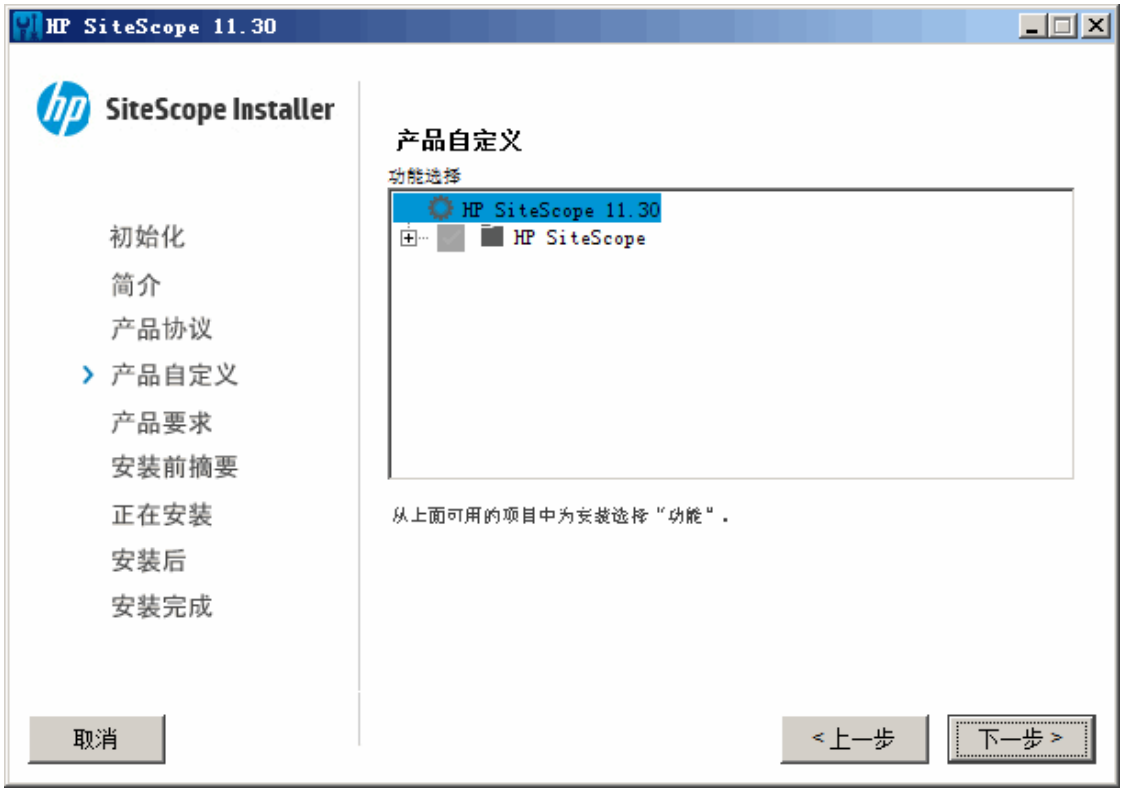
7. 在“产品自定义”屏幕中，选择 SiteScope 安装类型。

- **HP SiteScope。**这是标准的 SiteScope 安装。
- **HP SiteScope 故障转移。**此安装可在 SiteScope 主服务器出现故障时提供基础结构监控功能的备份。
- **HP SiteScope for Load Testing。**此安装类型仅用于 HP LoadRunner 或 HP Performance Center 安装，用于支持用户在 LoadRunner 或 Performance Center 应用程序上定义和使用 SiteScope 监控器。SiteScope 提供可对本机 LoadRunner 和 Performance Center 监控器起补充作用的附加监控。有关详细信息，请参阅相关 LoadRunner 或 Performance Center 文档。

  备注: 在 Linux 平台上执行安装时，不能使用此安装选项。

单击“下一步”继续。

8. **在功能选择屏幕上，选择安装选项。**

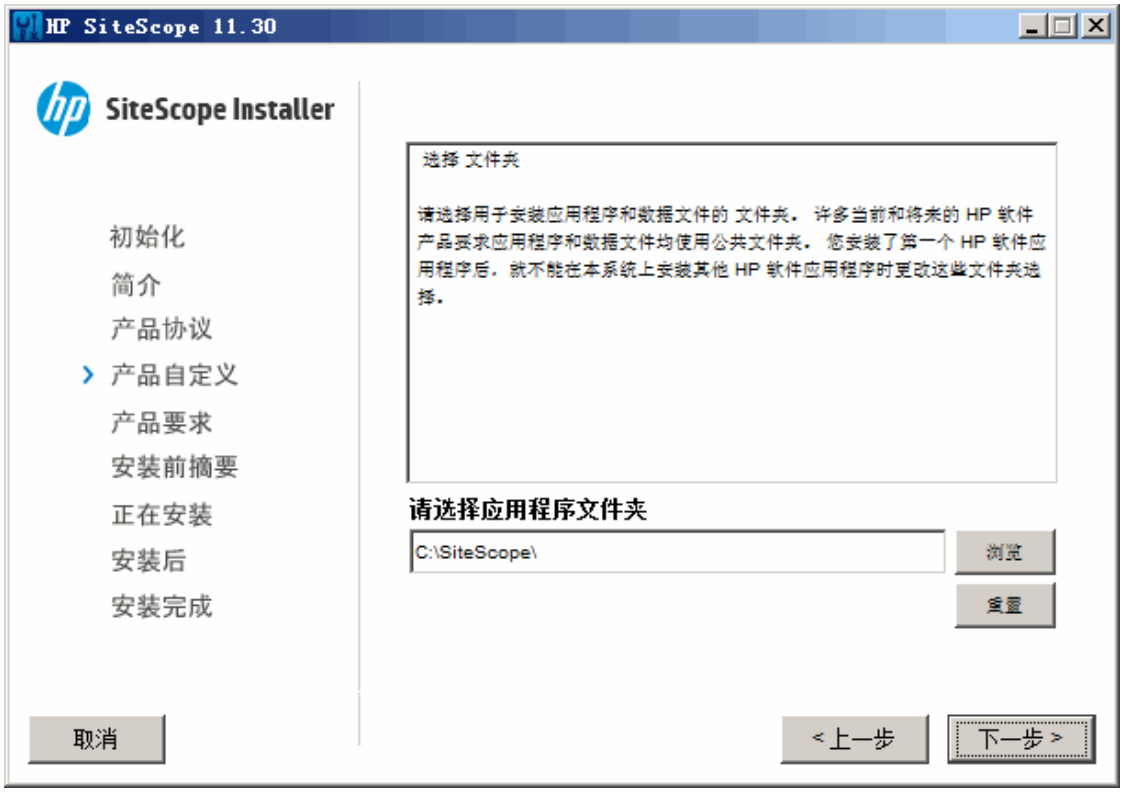


- **HP SiteScope。**在 64 位操作系统上作为 64 位应用程序安装 SiteScope。

单击“下一步”继续。

9. 如果在 Linux 平台上执行安装，则 SiteScope 将自动安装在 **/opt/HP/SiteScope/** 文件夹中。将跳至步骤 10。

   此时将打开“选择文件夹”屏幕。



   接受默认的目录位置，或单击“浏览”选择其他目录。如果选择其他目录，则安装路径中不得包含空格或非拉丁字符，且必须以名为 **SiteScope**（文件夹名称区分大小写）的文件夹结尾。要恢复默认安装路径，请单击“重置”。

   单击“下一步”继续。

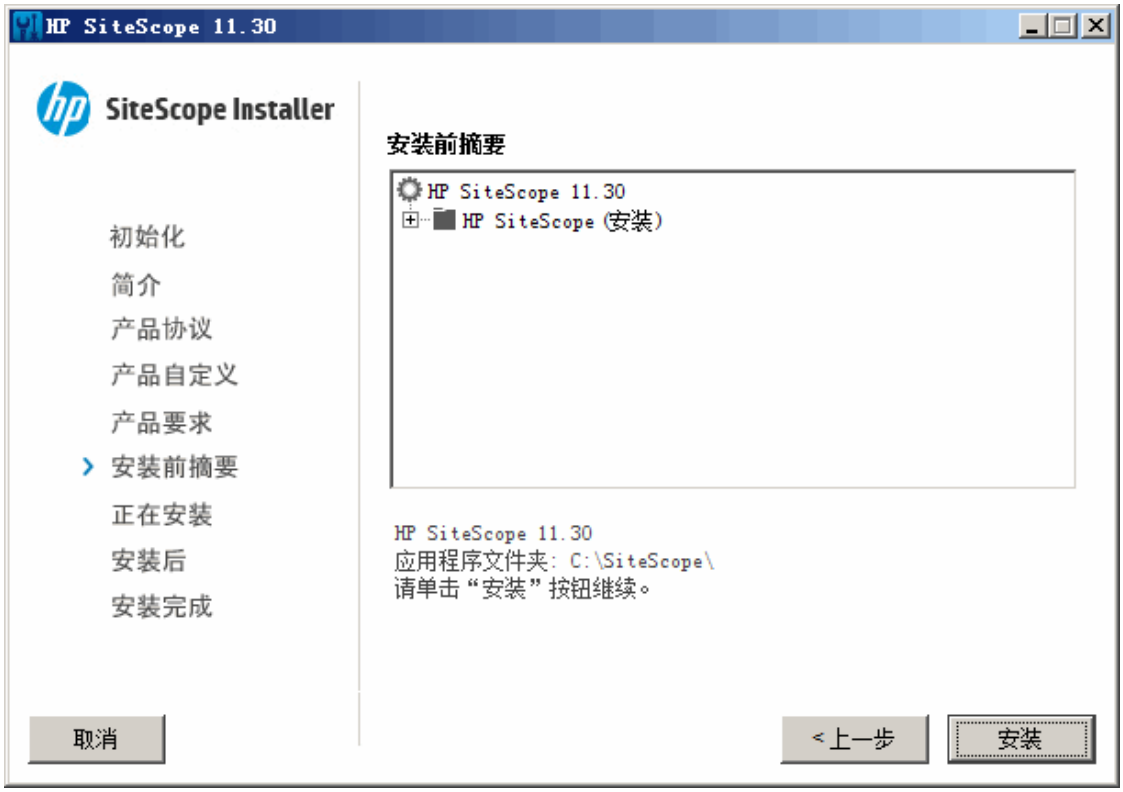
10. 此时将显示“安装检查项”屏幕并运行验证检查操作。

可用磁盘空间验证成功完成之后，单击“下一步”。

如果可用磁盘空间验证过程失败，请执行以下操作：

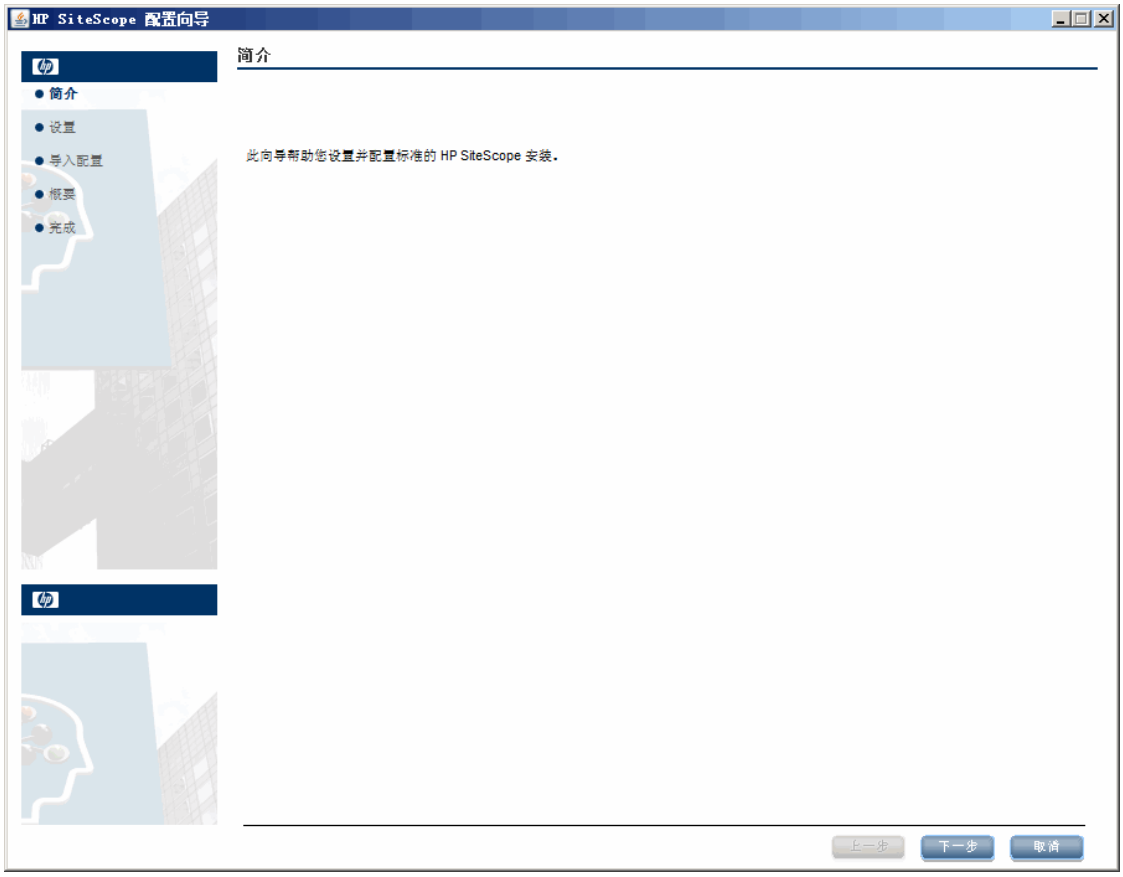
- 释放磁盘空间（例如，通过使用 Windows 磁盘清理实用程序）。
- 重复步骤 9 和 10。

11. 在“安装前摘要”屏幕中，单击“安装”。



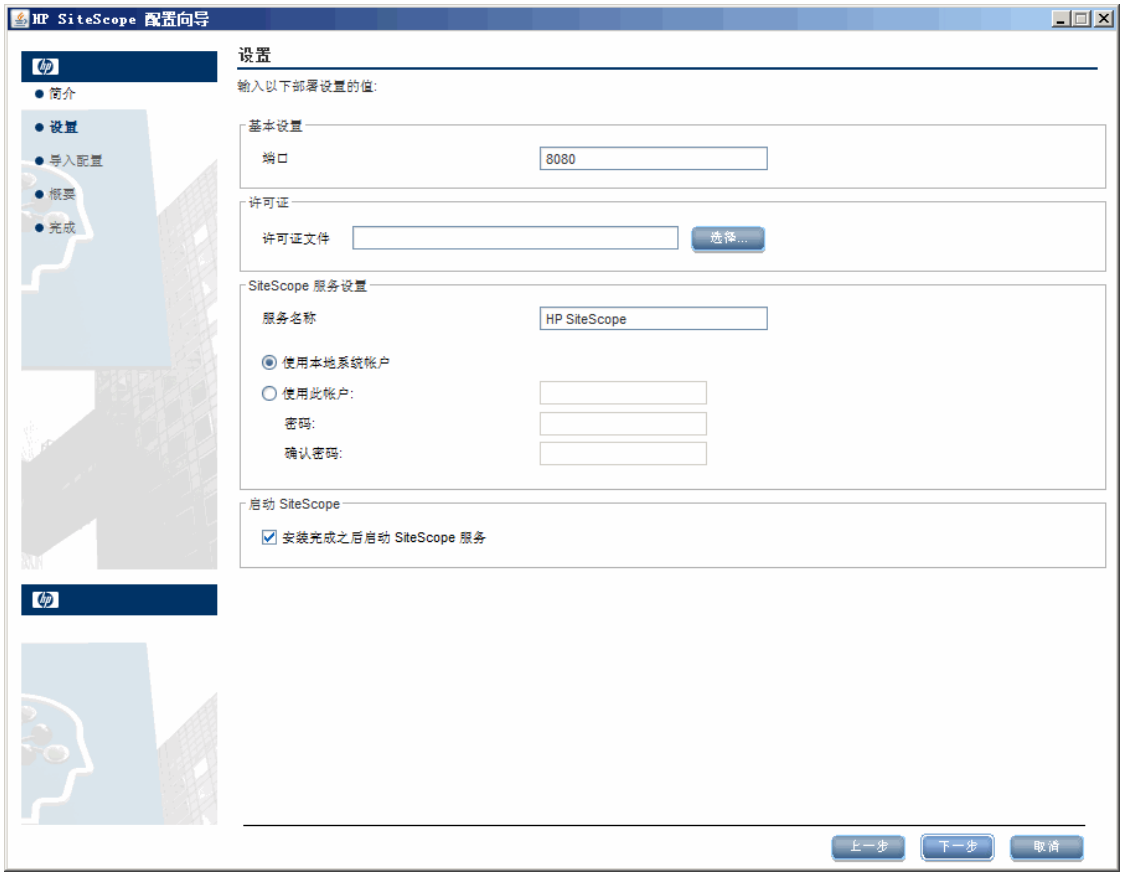
12. 此时将打开安装屏幕，安装程序将选择并安装需要的 SiteScope 软件组件。在安装期间，会在屏幕上显示每个软件组件及其安装进度。

13. 安装完 SiteScope 组件之后，将显示 SiteScope 配置向导的“简介”屏幕。



单击“下一步”。

14. 将显示 SiteScope 配置向导的“设置”屏幕。



输入所需的配置信息，然后单击“下一步”：

- **端口。**SiteScope 端口号。如果该端口号已被使用（将会显示错误消息），请输入其他端口。如有必要，可在以后使用配置工具更改端口。默认端口是 8080。

- **许可证文件。**输入许可证文件的路径，或单击“选择”，然后选择 SiteScope 许可证密钥文件。常规 SiteScope 安装后会自动激活 SiteScope 社区版许可证，因此并不一定需要输入许可证信息。要启用除 SiteScope 社区版包含的有限功能以外的功能，需要购买商业版许可证（请参阅升级 SiteScope 版本许可证 (第 26 页)）。

- **使用本地系统帐户**（不适用于 Linux 安装）。默认情况下，SiteScope 被安装为以本地系统帐户运行。此帐户在本地计算机上具有多种权限，并可以访问大多数系统对象。在本地系统帐户下运行时，SiteScope 会尝试使用 SiteScope 中配置的服务器凭据连接到远程服务器。

  备注: 建议将 SiteScope 服务设置为以具有域管理权限的用户身份登录，因为本地系统帐户可能没有足够的权限（本地系统帐户在域环境中具有域管理员用户权限，在非域环境中具有内置管理员用户权限）。

- **使用此帐户**（不适用于 Linux 安装）。选择更改 SiteScope 服务的用户帐户。可以将 SiteScope 服务设置为以具有域管理权限的用户身份登录。这能让 SiteScope 有权访问域中的监控器服务器数据。输入可以访问远程服务器的帐户和密码（并确认密码）。

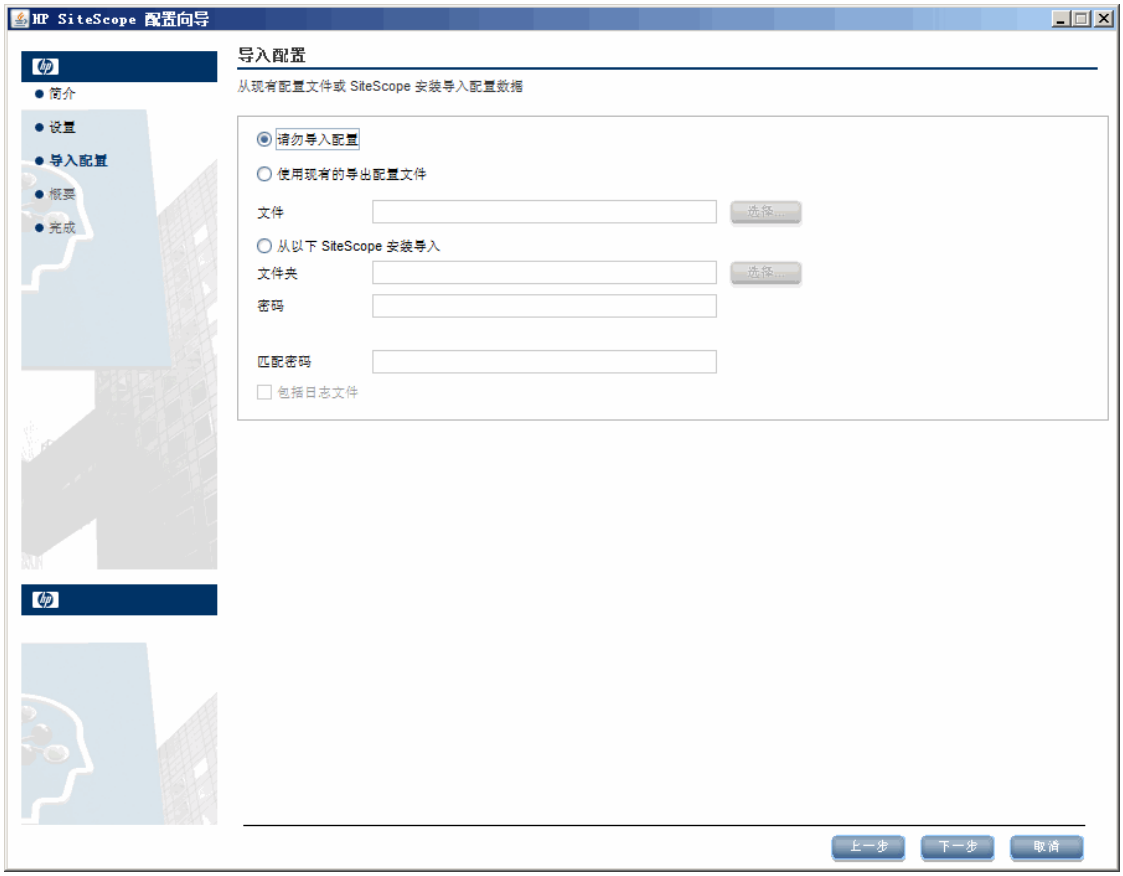
  备注: 如果 SiteScope 安装为以自定义用户帐户运行，则所使用的帐户必须具有“作为服务登录”权限。要授予用户登录服务访问权限，请执行以下操作:

  i. 在 Windows 控制面板中，双击“管理工具”。
  ii. 双击“本地安全策略”，并选择“本地策略”>“用户权限分配”>“作为服务登录”。
  iii. 单击“添加用户或组”，选择要授予登录服务访问权限的用户，然后单击“确定”。
  iv. 单击“确定”保存更新后的策略。

- **服务名称**（不适用于 Linux 安装）。SiteScope 服务的名称。如果计算机安装了先前版本的 SiteScope，请输入 SiteScope 服务的其他名称。默认的服务名称为 SiteScope。

- 安装完成之后启动 **SiteScope** 服务（不适用于 Linux 安装）。安装完成之后，SiteScope 服务会自动启动。

15. 此时将显示“导入配置”屏幕，该屏幕允许您将现有 SiteScope 配置数据导入新的 SiteScope 安装。



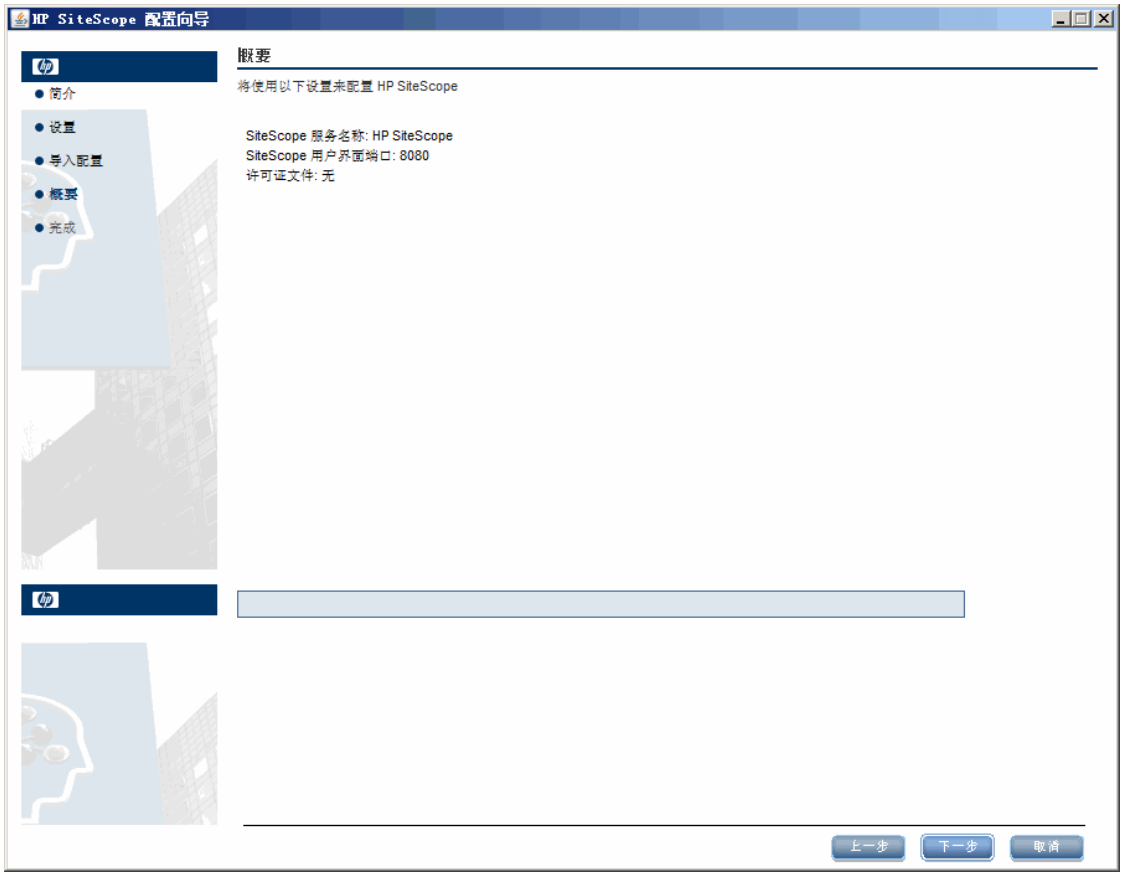
择以下其中一个选项，然后单击“下一步”：

- **请勿导入配置。**
- **使用现有的导出配置文件。**允许您使用已导出的现有配置文件中的各种 SiteScope 数据，如模板、日志、监控器配置文件等。SiteScope 数据使用“配置工具”导出，并以 **.zip** 格式保存。单击“选择”按钮，然后浏览到要导入的用户数据文件。
- **从以下 SiteScope 安装导入。**单击**“选择”**按钮，然后浏览到要从中导入配置数据的 SiteScope 安装文件夹。
  - **包括日志文件。**允许您从所选的 SiteScope 安装文件夹导入日志文件。
- 如果 SiteScope 已配置为使用密钥管理的加密运行，则在“密码短语”框中输入用于 SiteScope 服务器密钥库的密码短语。在“匹配密码短语”框中确认密码短语。有关详细信息，请参阅将 SiteScope 配置为使用自定义密钥加密数据 (第 144 页)。使用默认 SiteScope 加密时，这些框处于禁用状态。

备注:

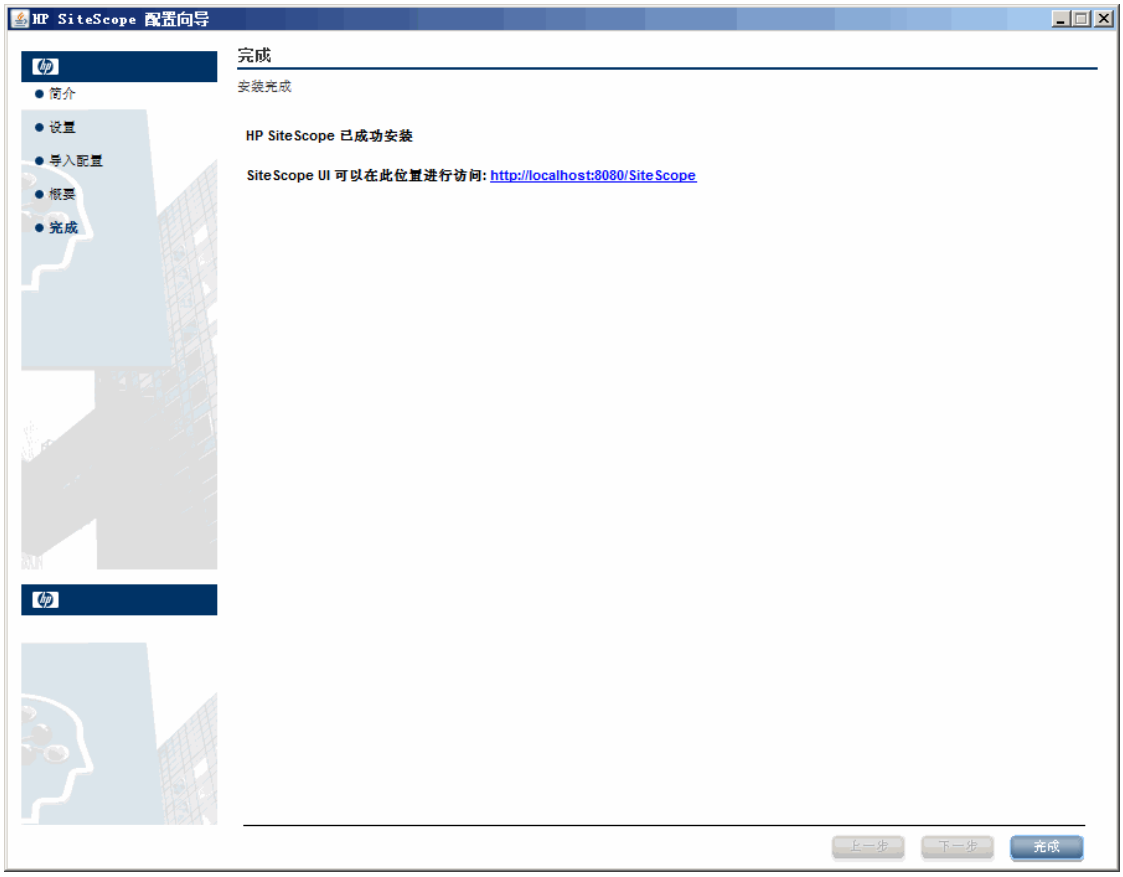
- 将配置数据从一个 SiteScope 安装移动到另一个 SiteScope 安装时，请确保您从中获取配置数据的源 SiteScope 服务器与要向其导入数据的目标 SiteScope 服务器位于相同的时区中。
- 如果导入的配置包含过期证书，过期证书将在配置导入的默认 SiteScope 密钥库内进行合并。这种情况可导致 SSL 证书监控器处于错误状态。要避免这种情况的发生，应在导出配置数据之前删除所有过期证书。

16. **此时将打开“概要”屏幕。**



检查信息是否正确，然后单击“下一步”继续，或单击“上一步”返回上一个屏幕以更改选择内容。

17. 此时将打开“完成”屏幕。



要访问 SiteScope 用户界面，请单击此 SiteScope 的连接地址。

备注: 如果未在“配置设置”屏幕中选择“安装完成之后启动 SiteScope 服务”，则需要先启动 SiteScope 服务，然后才能连接到 SiteScope。有关详细信息，请参阅开始使用 SiteScope (第 165 页)。

单击“完成”关闭“SiteScope 配置向导”。

18. 安装完成后，将会打开“安装完成”窗口，其中显示了有关所使用的安装路径及安装状态的摘要信息。

如果安装失败，请在“安装完成”窗口中单击“查看日志文件”链接，然后在 Web 浏览器中查看日志文件，以便在安装日志文件中检查任何出错信息。

有关已安装程序包的详细信息，请单击“详细信息”选项卡。

单击“完成”以关闭安装程序。

如果安装程序确定必须重新启动服务器，它会提示您重新启动服务器。

19. 要获取最新的可用功能，请从安装 SiteScope 的位置下载并安装最新的 SiteScope 修补程序（如果可用）。有关访问 SiteScope 界面的信息，请参阅连接到 SiteScope (第 166 页)。
20. 在 Linux 环境中安装 SiteScope 之后，设置 SiteScope 安装目录的权限，使得用于运行 SiteScope 应用程序的用户帐户具有读取、写入和执行权限。还必须为 SiteScope 安装目录中的所有子目录设置这些权限。

在无 X11 服务器的计算机上使用安装向导安装 SiteScope

可以通过以下任一方式在没有 X11 服务器的计算机上使用安装向导安装 SiteScope：

- 使用 VNC 服务器（在很多 Linux 系统上，默认情况下已安装 VNC 服务器）。
- 编辑 DISPLAY 环境变量，以使程序使用其他计算机上的 X 服务器。

要使用 VNC 服务器在无 X11 的计算机上安装 SiteScope，请执行以下操作：

1. 在命令行中，运行 vncserver。运行后，选择密码，并记下 VNC 服务器所使用的显示内容（通常为 :1）。
2. 通过 VNC 客户端连接到 SiteScope 计算机，格式为：hostname:display。例如，sitescope.company.name:1
3. 在打开的控制台中，浏览到 SiteScope 安装目录，然后照常运行安装。

要通过重定向 X 在没有 X11 的计算机上安装 SiteScope，请执行以下操作：

1. 运行任意带有 X 服务器的 Linux 系统，或在 Windows 上安装 X 服务器（例如 xming）。
2. 检查 X 访问控制是否允许 SiteScope 计算机连接。在 Linux 平台上，请参见 man xhost。在 Windows 平台上，请参阅有关 X 服务器实施的文档。
3. 在 SiteScope 计算机上运行 **export DISPLAY=x-server.machine.name:display**（display 通常为 0）。
4. 在同一个 shell 中浏览到 SiteScope 安装目录，然后照常运行安装。

第 13 章: 使用控制台模式在 Linux 上执行安装

可以使用命令行或控制台模式在 Linux 上安装 SiteScope。在远程服务器上安装 SiteScope 时，或者因为任何其他原因导致无法通过用户界面使用安装选项时，可使用此选项。

备注: 已从 SiteScope 控制台模式中删除安装 HP Operations Agent 的选项。必须手动安装并配置该代理。如果 SiteScope 与 HPOM 或 BSM 集成，则需要使用该代理发送事件和存储度量数据（使用 BSM 中的配置文件数据库将度量数据绘制到性能图的情况除外）。 有关安装和配置代理的详细信息，请参阅《Integrating SiteScope with HP Operations Manager Products Guide》，该文档在 SiteScope 帮助中或 HP 软件集成网站上提供。

要使用控制台模式在 Linux 上安装 SiteScope，请执行以下操作:

1. 将安装包 (**SiteScope_11.30_Linux.zip**) 下载到要安装 SiteScope 的计算机上。或者，将 SiteScope 安装文件复制到用于安装 SiteScope 的用户帐户可以访问的磁盘或网络位置。

   可通过 HP 系统从以下途径获得 SiteScope:

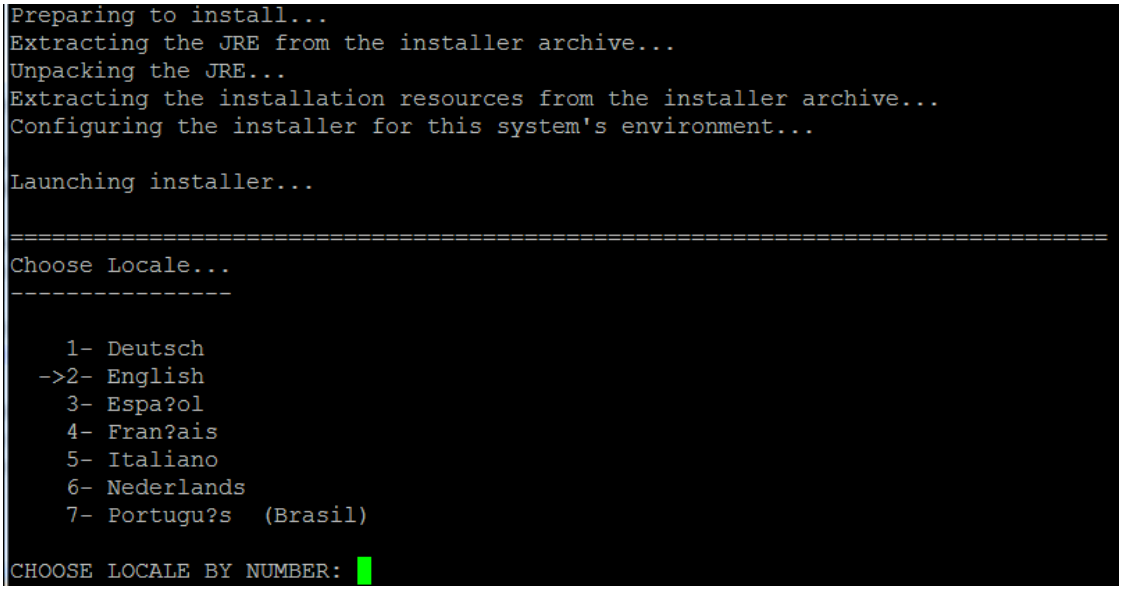
客户	下载选项
评估客户	电子下载评估链接 HP 授权的软件合作伙伴可使用 HP 软件合作伙伴中心 （以上链接需要 HP Passport 帐户。请转到 http://h20229.www2.hp.com/passport-registration.html 注册 HP Passport。）
新客户	电子软件下载。客户通过电子邮件接收软件下载链接；该链接特定于订购者。
现有客户更新	https://h20575.www2.hp.com/usbportal/softwareupdate.do **先决条件:** a. 访问以上链接需要 HP Passport 帐户以及支持协议 ID (SAID)，用于通过 SSO 门户接收更新。要注册 HP Passport，请参阅 http://h20229.www2.hp.com/passport-registration.html。有关激活 SAID 的详细信息，请参阅软件联机支持网站上的常见问题解答。 b. 软件升级需要新的许可证密钥。请先与您的 HP 支持续订代表联系，请求产品合同迁移。完成合同迁移后，请访问“My Software Updates”门户 (https://h20575.www2.hp.com/usbportal/softwareupdate.do)，然后单击“Get Licensing”选项卡获取新的许可证密钥。 **要下载软件更新，请执行以下操作:** a. 选择“My software updates”。 b. 展开“Application Performance Management”，选择所需的 HP SiteScope 11.30 软件电子介质，然后单击“Get software updates”。 c. 在“Selected Products”选项卡中，单击所需产品更新的“Get Software”，然后根据网站上的说明下载软件。

2. 运行以下命令:

```
HPSiteScope_11.30_setup.bin -i console
```

安装脚本将初始化 Java 虚拟机以启动安装。

3. 此时将显示“选择区域设置”屏幕。

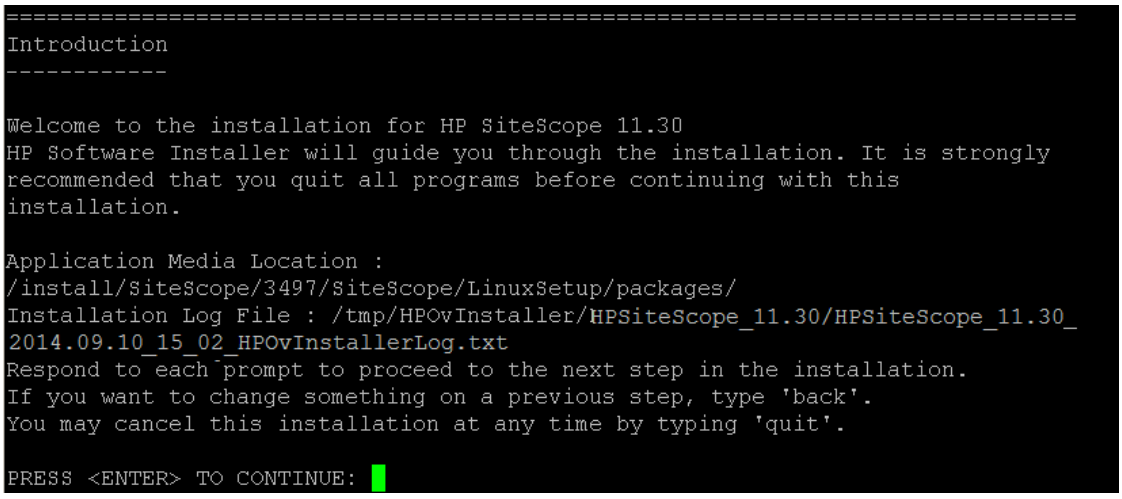


输入数字以选择所需的区域设置，然后按 ENTER 键继续。

4. 此时将显示确认屏幕。

按 ENTER 键继续。

5. 此时将显示“简介”屏幕。



按 ENTER 键继续安装。

6. 此时将显示许可证协议的文本。SiteScope 许可证协议会分多页显示。请逐页阅读所显示的页面。按 ENTER 键可以继续阅读下一页。查看完许可证协议的所有页面后，可以选择接受或不接受许可证协议。

```
我接受“许可证协议”的条款 (Y/N): Y
```

要安装 SiteScope，必须接受许可证协议的各项条款。默认选择为不接受协议。要接受许可证协议并继续执行安装，请输入 Y。

> **备注:** 要在查看完 SiteScope 许可证协议之后取消安装，请输入 N。

7. 此时将打开 SiteScope 安装类型屏幕。

```
================================================================================


Install Groups are combined sets of features.
If you want to change something on a previous step, type 'back'.
You may cancel this installation at any time by typing 'quit'.



  ->1- HP SiteScope: ()
    2- HP SiteScope Failover: ()

Please select one of the above groups ...: 1
```

选择适合于您的站点的类型。输入安装类型的编号，然后按 ENTER 键继续。

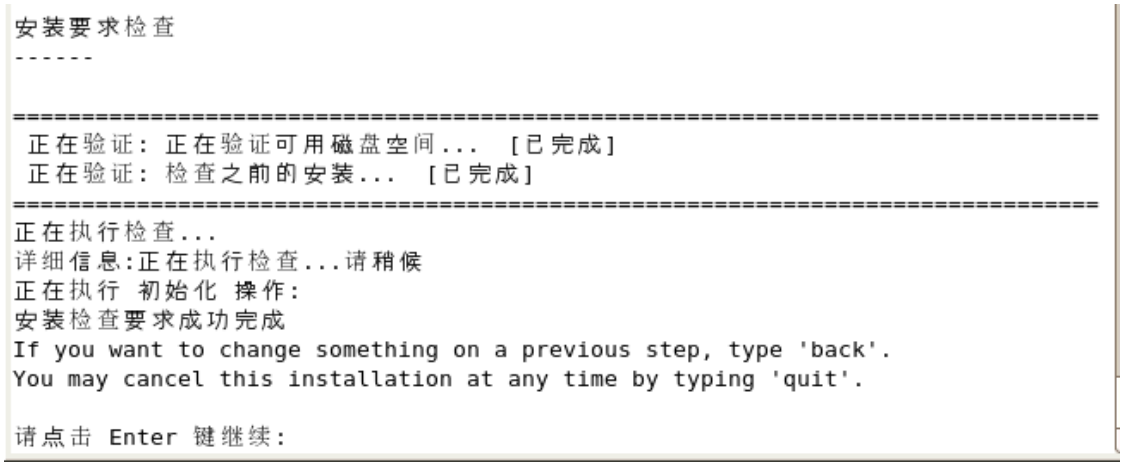
8. 此时将打开“选择功能”屏幕。

```
================================================================================
Select Features
---------------

Install Features represent a group of functionality
If you want to change something on a previous step, type 'back'.
You may cancel this installation at any time by typing 'quit'.



  ->1- HP SiteScope(Required)

Please Select Features(Use a comma to separate your choices): 1
```

输入数字 1（必需）安装 SiteScope。

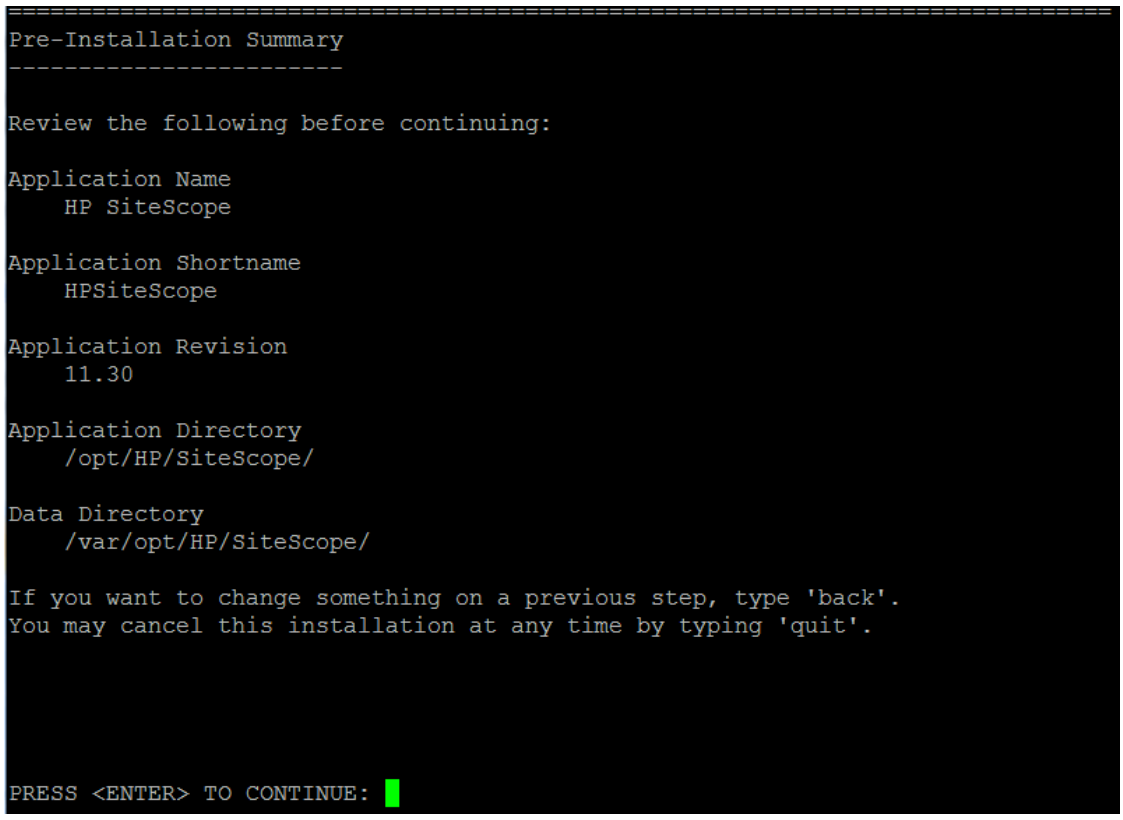
按 ENTER 键继续安装。

9. 此时将打开“安装要求”屏幕。



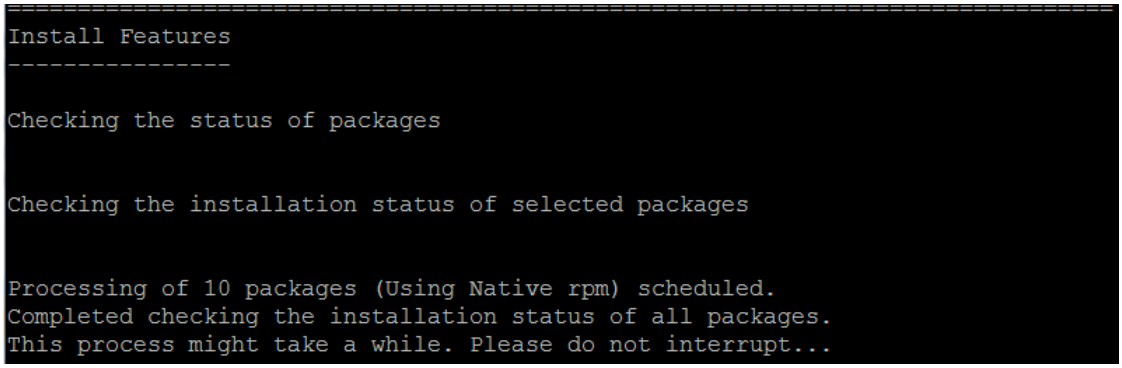
按 ENTER 键继续安装。

10. 此时将打开“安装前摘要”屏幕。



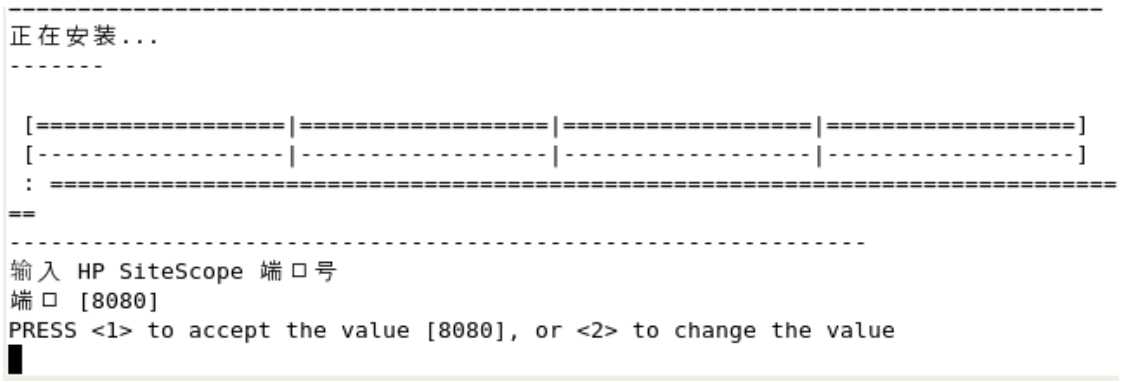
按 ENTER 键继续安装。

11. 此时将打开“安装功能”屏幕，开始安装过程。



安装过程完成后，将打开安装后配置屏幕。

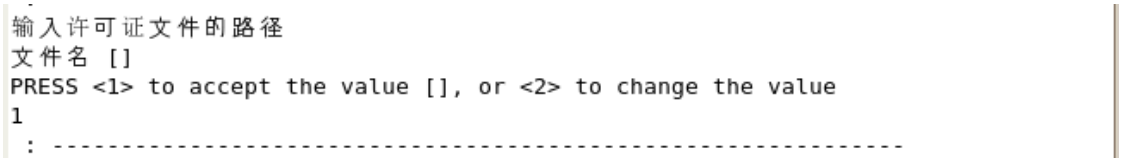
12. 此时将显示端口提示信息。



输入数字 1 接受默认端口 8080，或输入数字 2 更改端口，然后在端口变更提示中输入其他数字。

按 ENTER 键继续安装。

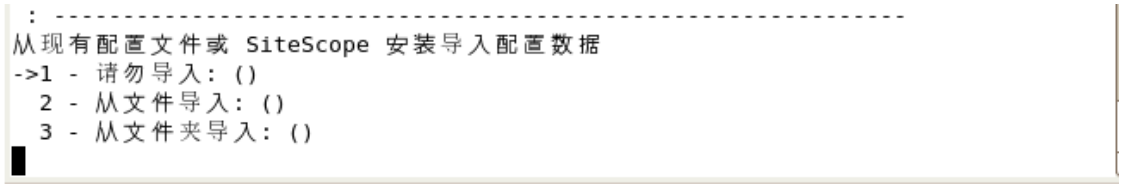
13. 此时将显示许可证文件路径提示。



输入数字 1 将许可证文件路径保留为空（常规 SiteScope 安装后会自动激活 SiteScope 社区版许可证，因此不需要输入许可证信息即可使用 SiteScope），或输入数字 2 并在下一个文本框中输入许可证文件路径。

按 ENTER 键继续安装。

14. 此时将打开“导入配置数据”屏幕。



如果不需要导入数据，则输入数字 1。

输入数字 2 可使用已导出的现有配置文件中的各种 SiteScope 数据，如模板、日志、监控器配置文件等。如果选择此选项，请在下一个文本框中输入配置文件的路径。

输入数字 3 可从 SiteScope 安装目录导入配置数据。如果选择此选项，请输入要从其中导入配置数据的 SiteScope 安装文件夹的路径。

如果已将 SiteScope 配置为使用密钥管理数据加密运行，请在出现提示时输入 SiteScope 服务器密钥库的密码短语，然后再次输入以确认该密码短语。有关详细信息，请参阅将 SiteScope 配置为使用自定义密钥加密数据 (第 144 页)。

按 ENTER 键继续安装。

备注:

- 将配置数据从一个 SiteScope 安装移动到另一个 SiteScope 安装时，请确保您从中获取配置数据的源 SiteScope 服务器与要向其导入数据的目标 SiteScope 服务器位于相同的时区中。
- 如果导入的配置包含过期证书，过期证书将在配置导入的默认 SiteScope 密钥库内进行合并。这种情况可导致 SSL 证书监控器处于错误状态。要避免这种情况的发生，应在导出配置数据之前删除所有过期证书。

15. 控制台将显示需要确认的安装参数。

```
-------------------------------------------------------------
HP SiteScope will be configured with the following settings
SiteScope user interface port: 8080
License file: None
Press <1> to continue, or <2> to change values:
1
 : Please wait ...
```

输入 1 可以使用所显示的参数继续安装，或输入 2 返回进行更改，然后按 ENTER 键。

安装过程随即完成。此时将显示安装状态消息。

```
=============================================================================
Installation Complete
---------------------

Congratulations!
HP SiteScope 11.30
The installation has been successfully completed.
Application Directory: /opt/HP/SiteScope/

View log file./tmp/HPOvInstaller/HPSiteScope_11.30/HPSiteScope_11.30_2014.09.10
_15_02_HPOvInstallerLog.txt
[root@myd-vm04854 Release]#
```

16. 安装 SiteScope 之后，设置 SiteScope 安装目录的权限，使得用于运行 SiteScope 应用程序的用户帐户具有读取、写入和执行权限。还必须为 SiteScope 安装目录中的所有子目录设置这些权限。

    有关如何创建负责运行 SiteScope 应用程序的非 root 用户，以及如何设置帐户权限的详细信息，请参阅配置有权运行 SiteScope 的非 root 用户帐户 (第 35 页)。

17. 要连接到 SiteScope，请按照在 Linux 平台上启动和停止 SiteScope 进程 (第 166 页)部分中的步骤操作。

第 14 章: 在静默模式下安装 SiteScope

本章包括:

关于在静默模式下安装 SiteScope

可以在静默模式下安装 SiteScope。静默安装时，整个安装过程会在后台运行，无需您在安装屏幕中进行导航，也无需输入选择项。所有配置参数将按照您在响应文件中定义的值进行分配。要运行不同配置的静默安装，可以创建多个响应文件。

注意事项和限制情况

在运行静默安装之前，请考虑以下问题:

- 在静默模式下运行安装时将不会显示任何消息。但是，您可以在日志文件中查看安装是否成功等安装信息。可以在下列目录中找到安装日志文件:
  - **%tmp%\HPOvInstaller\HPSiteScope_11.30**（Windows 平台）
  - **/tmp/HPOvInstaller/HPSiteScope_11.30**（Linux 平台）
- SiteScope 安装路径 (prodInstallDir=<安装路径>) 的名称中不能包含空格或非拉丁字符，并且必须以名为 **SiteScope**（文件夹名称区分大小写）的文件夹结尾。
- 已删除直接从 SiteScope 安装 HP Operations Agent 的选项。必须手动安装并配置该代理。如果 SiteScope 与 HPOM 或 BSM 集成，则需要使用该代理发送事件和存储度量数据（使用 BSM 中的配置文件数据库将度量数据绘制到性能图的情况除外）。 有关安装和配置代理的详细信息，请参阅《Integrating SiteScope with HP Operations Manager Products Guide》，该文档在 SiteScope 帮助中或 HP 软件集成网站上提供。

运行静默安装

使用 **ovinstallparams.ini** 文件来运行静默安装。由于此文件具有特定的格式，所以必须根据示例 **ovinstallparams.ini** 文件来创建静默安装文件。

备注: 只有安装 SiteScope 后，**<SiteScope 安装目录>\examples\silent_installation** 文件夹中的示例 **ovinstallparams.ini** 文件才可用。

要运行 SiteScope 11.30 的静默安装，请执行以下操作:

1. 导航到位于 **<SiteScope 安装目录>\examples\silent_installation** 文件夹中的 **ovinstallparams.ini** 文件。
2. 复制该文件，然后根据安装需要进行修改。
3. 将文件复制到 SiteScope 安装文件（**HPSiteScope_11.30_setup.exe** 或 **HPSiteScope_11.30_**

setup.bin ）所在的安装文件夹。

4. 从命令行使用 **-i silent** 标志运行安装程序。在 Windows 中，请指定“等待”模式。例如：
   start /wait HPSiteScope_11.30_setup.exe -i silent (Windows)
   HPSiteScope_11.30_setup.bin -i silent (Linux)

要在静默模式下卸载 SiteScope，请执行以下操作：

对于 Linux，请运行：

/opt/HP/SiteScope/installation/bin/uninstall.sh -i silent

对于 Windows，请运行：

%SITESCOPE_HOME%\installation\bin\uninstall.bat -i silent

第 15 章: 使用 SiteScope 配置工具

本章包括:

在 Windows 平台上运行配置工具

配置工具是一个非常方便的实用程序，可用于将配置数据从一个 SiteScope 安装移动到另一个 SiteScope 安装。您可以将模板、日志、监控器配置文件、脚本、服务器证书等 SiteScope 数据从当前 SiteScope 导出，以便将来导入 SiteScope。您还可以使用向导，通过在 Windows 注册表项中更改大小来优化 SiteScope 的性能，以及更改分配到 SiteScope 的端口和完成 HP Operations Agent 的安装。

如果在安装过程中导出了 SiteScope 数据，则可以使用配置工具将这些数据导入。另外，您也可以使用配置工具从当前的 SiteScope 单独导出数据。如果您在先前版本的 SiteScope 中创建或修改了监控器配置文件，则可能需要将它们导入到当前的 SiteScope 目录。

备注:

- 也可以通过控制台模式在 Windows 平台上运行配置工具。有关详细信息，请参阅使用控制台模式运行配置工具 (第 116 页)。
- 配置工具中已删除直接从 SiteScope 安装和卸载 HP Operations Agent 的选项。必须手动安装并配置该代理。如果 SiteScope 与 HPOM 或 BSM 集成，则需要使用该代理发送事件和存储度量数据（使用 BSM 中的配置文件数据库将度量数据绘制到性能图的情况除外）。有关安装和配置代理的详细信息，请参阅《Integrating SiteScope with HP Operations Manager Products Guide》，该文档在 SiteScope 帮助中或 HP 软件集成网站上提供。
- 您必须在导出或导入数据之前停止 SiteScope 服务，并在导出或导入数据之后重新启动该服务。有关详细信息，请参阅在 Windows 平台上启动和停止 SiteScope 服务 (第 165 页)。
- 将配置导入到相同版本的 SiteScope 中时，必须重命名或删除所有模板示例容器，以便导入新的模板示例。
- 将配置数据从一个 SiteScope 安装移动到另一个时，请确保从中获取配置数据的源 SiteScope 服务器与要向其导入数据的目标 SiteScope 服务器位于同一个时区中。
- 如果导入的配置包含过期证书，过期证书将在配置导入的默认 SiteScope 密钥库内进行合并。这种情况可导致 SSL 证书监控器处于错误状态。要避免这种情况的发生，应在导出配置数据之前删除所有过期证书。
- 导入配置数据时不能覆盖以下文件夹中的文件：**templates.os**、**templates.post**、**templates.health**、**templates.applications** 和 **conf\ems**。
- 配置工具支持在导出数据时包含服务器证书和脚本。有关从 SiteScope 的早期版本导出数据时如何包括服务器证书和脚本的详细信息，请参阅升级现有 SiteScope 安装 (第 63 页)。

要运行 SiteScope 配置工具，请执行以下操作:

1. 在 SiteScope 服务器上，选择“开始”>“所有程序”>“HP SiteScope”>“配置工具”。此时将打开“SiteScope 配置向导”。
2. 选择要执行的操作，然后单击“下一步”。

- **调整大小。**允许通过在 Windows 注册表项中增大 JVM 堆大小、桌面堆大小以及文件句柄数来优化 SiteScope 的性能。有关详细信息，请参阅步骤 3。

  备注: 如果通过运行 **<SiteScope 安装>\bin** 目录中的 **go.bat** 文件来启动 SiteScope，请打开 **go.bat** 文件，并根据需要增加 **–Xmx1024m** 参数，最大可增加到 **–Xmx8192m**（适用于 8GB）。

- **更改端口。**允许更改 SiteScope 服务器所使用的任何端口。有关详细信息，请参阅步骤 4。
- **导入配置。**允许从导出的配置数据 (**.zip**) 文件或从现有 SiteScope 安装导入配置数据。有关详细信息，请参阅步骤 5。
- **导出配置。**允许将模板、日志、监控器配置文件等 SiteScope 数据从当前 SiteScope 导出，以便将来导入 SiteScope。有关详细信息，请参阅步骤 6。
- **配置单独安装的 HP Operations Agent。**需要完成 HP Operations Agent 的安装。当 SiteScope 与 HP Operations Manager 或 BSM 网关服务器集成时，该代理支持 SiteScope 或 SiteScope 故障转移发送事件并充当度量数据的数据存储设备。有关详细信息，请参阅步骤 7。

  备注: 如果 SiteScope 服务器上未安装 HP Operations Agent 11.14，则此选项处于禁用状态。有关安装和配置代理的详细信息，请参阅《Integrating SiteScope with HP Operations Manager Products Guide》，该文档在 SiteScope 帮助中或 HP 软件集成网站上提供。

3. 如果选择了“调整大小”选项，则将打开“调整大小”屏幕，列出 Windows 注册表中的参数。

可以通过在以下 Windows 注册表项中进行更改来优化 SiteScope 的性能:

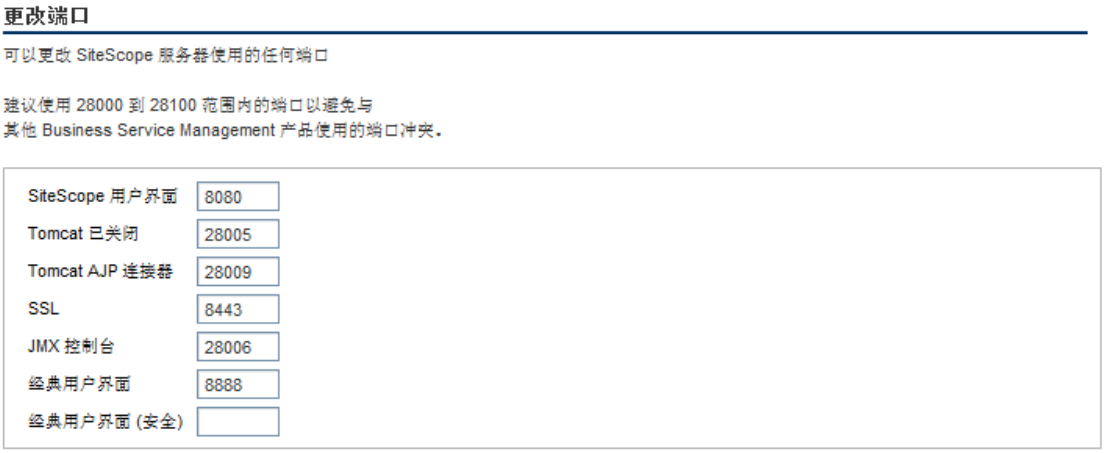
- **JVM 堆大小。**值将从 512 MB 更改为 4096 MB。有关 JVM 堆大小的详细信息，请参阅 http://java.sun.com/j2se/1.5.0/docs/guide/vm/gc-ergonomics.html。
- **桌面堆大小。**值将从 512 KB 更改为 8192 KB。有关桌面堆大小的详细信息，请参阅 http://support.microsoft.com/kb/126962。

  备注: 仅当 SiteScope 服务器的物理内存大于配置工具配置的最大 JVM 堆大小（Xmx，64 位安装为 4 GB）时，才可以更改大小。

  单击“下一步”完成调整大小的操作。

- **句柄数。**值将从 10,000 增加到 18,000 个文件句柄。有关更改文件句柄数的详细信息，请参阅 http://support.microsoft.com/kb/326591。

4. 如果您选择了“更改端口”选项，则会打开“更改端口”屏幕。



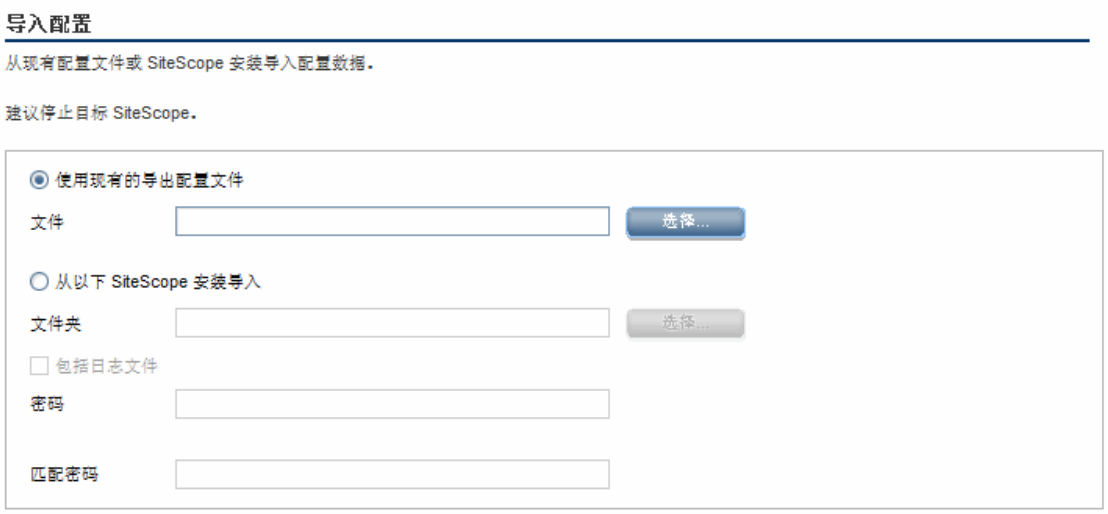
根据需要修改由 SiteScope 服务器使用的端口。端口号必须为 1 到 65534 之间的数字。除经典用户界面之外，所有其他组件都必须具有端口号。

备注: 建议使用范围在 28000-28100 之间的端口号，以避免和其他 Business Service Management 产品使用的端口发生冲突。

单击“下一步”完成更改端口的操作。

备注: 完成端口更改操作后，会在“开始”>“所有程序”>“HP SiteScope”>“打开 HP SiteScope”链接中更新端口。

5. 如果您选择了“导入配置”选项，则会打开“导入配置”屏幕。



备注: 您必须在导入数据之前停止 SiteScope 服务，并在导入数据之后重新启动该服务。有关详细信息，请参阅在 Windows 平台上启动和停止 SiteScope 服务 (第 165 页)。

- 如果选择“使用现有的导出配置文件”，请输入要导入的用户数据文件名。
- 如果选择“从以下 SiteScope 安装导入”，请输入要从中导入用户数据文件的 SiteScope 安装目录。如果还需要导入日志文件，请选择“包括日志文件”。
- 如果 SiteScope 已配置为使用密钥管理数据加密运行，则在“密码短语”框中输入 SiteScope 服务器密钥库的密码短语。在“匹配密码短语”框中输入相同密码短语，确认此密码短语。有关详细信息，请参阅将 SiteScope 配置为使用自定义密钥加密数据 (第 144 页)。使用默认 SiteScope 加密时，这些框处于禁用状态。

单击“下一步”完成导入操作。

6. 如果您选择了“导出配置”选项，则会打开“导出配置”屏幕。

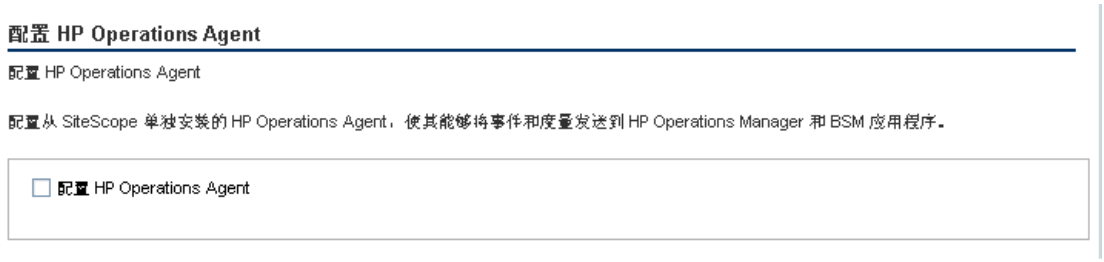
- 在“从 SiteScope 文件夹”中，保留框中已给定的默认目录，或输入 SiteScope 安装目录的完整路径。例如，如果您不使用所列出的目录路径，而要使用安装目录路径 D:\SiteScope11_0\SiteScope，则输入 D:\SiteScope11_0\SiteScope。
- 在“到文件”框中，输入要向其导出用户数据文件的目录（该目录必须已经存在）和已导出的用户数据文件的名称。该文件名必须以 **.zip** 结尾。如果还需要导出日志文件，请选择“包括日志文件”。
- 如果 SiteScope 已配置为使用密钥管理的加密运行，则在“密码短语”框中输入用于 SiteScope 服务器密钥库的密码短语。有关详细信息，请参阅将 SiteScope 配置为使用自定义密钥加密数据 (第 144 页)。使用默认 SiteScope 加密时，此框处于禁用状态。

备注:

- 您必须在导出数据之前停止 SiteScope 服务，并在导出数据之后重新启动该服务。有关详细信息，请参阅在 Windows 平台上启动和停止 SiteScope 服务 (第 165 页)。
- 由于导出 SiteScope 数据时不会复制 **\htdocs** 目录，因此需要备份此目录，并在升级后将其复制到 SiteScope 11.30 目录中，以便查看旧报告。

单击“下一步”完成导出操作。

7. 如果选择了“配置单独安装的 HP Operations Agent”选项，则会打开“配置 HP Operations Agent”屏幕。



选择“配置 HP Operations Agent”。这需要完成 HP Operations Agent 的安装。当 SiteScope 与 HP Operations Manager 或 BSM 网关服务器集成时，该代理支持 SiteScope 发送事件并充当度量数据的数据存储设备。

有关发送事件和报告度量数据的详细信息，请参阅《Integrating SiteScope with HP Operations Manager Products Guide》，该文档在 SiteScope 帮助中或 HP 软件集成网站上提供。

单击“下一步”完成安装操作。

8. 此时将打开“概要”屏幕，其中会显示配置状态。

单击“完成”关闭向导。

升级完成后，可以通过运行 **<SiteScope 根目录>\bin** 目录下的 **go.bat** 文件来启动 SiteScope。这可防止在监控器运行时间超过 15 分钟时 SiteScope 自行重新启动。

在 Linux 平台上运行配置工具

配置工具是一个非常方便的实用程序，可用于将配置数据从一个 SiteScope 安装移动到另一个 SiteScope 安装。您可以将模板、日志、监控器配置文件、脚本、服务器证书等 SiteScope 数据从当前 SiteScope 导出，以便将来导入 SiteScope。您还可以使用向导来更改 SiteScope 服务器所使用的任何端口，以及完成 HP Operations Agent 的安装。

如果在安装过程中导出了 SiteScope 数据，则可以使用配置工具将这些数据导入。另外，您也可以使用配置工具从当前的 SiteScope 单独导出数据。如果您在先前版本的 SiteScope 中创建或修改了监控器配置文件，则可能需要将它们导入到当前的 SiteScope 目录。

备注:

- 也可以通过控制台模式在 Linux 平台上运行配置工具。有关详细信息，请参阅使用控制台模式运行配置工具 (第 116 页)。
- 配置工具中已删除直接从 SiteScope 安装和卸载 HP Operations Agent 的选项。必须手动安装并配置该代理。如果 SiteScope 与 HPOM 或 BSM 集成，则需要使用该代理发送事件和存储度量数据（使用 BSM 中的配置文件数据库将度量数据绘制到性能图的情况除外）。有关安装和配置代理的详细信息，请参阅《Integrating SiteScope with HP Operations Manager Products Guide》，该文档在 SiteScope 帮助中或 HP 软件集成网站上提供。
- 将配置数据从一个 SiteScope 安装移动到另一个 SiteScope 安装时，请确保您从中获取配置数据的源 SiteScope 服务器与要向其导入数据的目标 SiteScope 服务器位于相同的时区中。
- 如果导入的配置包含过期证书，过期证书将在配置导入的默认 SiteScope 密钥库内进行合并。这种情况可导致 SSL 证书监控器处于错误状态。要避免这种情况的发生，应在导出配置数据之前删除所有过期证书。
- 导入配置数据时不能覆盖以下文件夹中的文件：**templates.os**、**templates.post**、**templates.health**、**templates.applications** 和 **conf\ems**。
- SiteScope 配置工具支持在导出数据时包含服务器证书和脚本。有关从 SiteScope 的早期版本导出数据时如何包括服务器证书和脚本的详细信息，请参阅升级现有 SiteScope 安装 (第 63 页)。
- 在需要大于 4GB 内存的负载环境中使用 SiteScope 时，应手动增加服务器上的 JVM 堆大小：
  a. 打开 **SiteScope/bin/start-service** 文件进行编辑。
  b. 在最后一行，根据需要增加 **-Xmx4096m** 参数的值，最大可增加到 **-Xmx8192m**（适用于 8GB）。

要运行 SiteScope 配置工具，请执行以下操作：

1. 在 SiteScope 服务器上，执行以下任一操作：
   a. 在图形模式下运行 <SiteScope 安装目录>/bin/config_tool.sh
   b. 在控制台模式下运行 <SiteScope 安装目录>/bin/config_tool.sh -i console

   此时将打开“SiteScope 配置向导”。

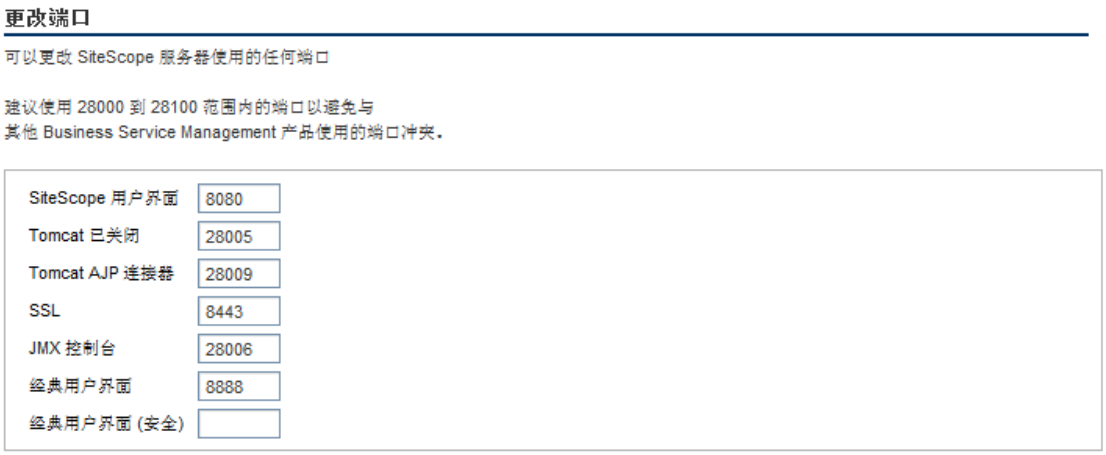
   单击“下一步”。

2. 在“简介”屏幕上选择要执行的操作，然后单击“下一步”。

- **更改端口。**允许更改 SiteScope 服务器所使用的任何端口。有关详细信息，请参阅步骤 3。
- **导入配置。**允许从导出的配置数据 (**.zip**) 文件或从现有 SiteScope 安装导入配置数据。有关详细信息，请参阅步骤 5。
- **导出配置。**允许将模板、日志、监控器配置文件等 SiteScope 数据从当前 SiteScope 导出，以便将来导入 SiteScope。有关详细信息，请参阅步骤 4。
- **配置单独安装的 HP Operations Agent。**需要完成 HP Operations Agent 的安装。当 SiteScope 与 HP Operations Manager 或 BSM 网关服务器集成时，该代理支持 SiteScope 发送事件并充当度量数据的数据存储设备。有关详细信息，请参阅步骤 6。

> **备注:** 如果 SiteScope 服务器上未安装 HP Operations Agent 11.14，则此选项处于禁用状态。有关安装和配置代理的详细信息，请参阅《Integrating SiteScope with HP Operations Manager Products Guide》，该文档在 SiteScope 帮助中或 HP 软件集成网站上提供。

3. 如果您选择了“更改端口”选项，则会打开“更改端口”屏幕。



根据需要修改由 SiteScope 服务器使用的端口。端口号必须为 1 到 65534 之间的数字。除经典用户界面之外，所有其他组件都必须具有端口号。

备注: 建议使用范围在 28000-28100 之间的端口号，以避免和其他 Business Service Management 产品使用的端口发生冲突。

单击“下一步”完成更改端口的操作。

4. 如果您选择了“导出配置”选项，则会打开“导出配置”屏幕。

备注: 您必须在导出数据之前停止 SiteScope 服务，并在导出数据之后重新启动该服务。有关详细信息，请参阅在 Linux 平台上启动和停止 SiteScope 进程 (第 166 页)。

- 在“从 **SiteScope** 文件夹”中，保留框中已给定的默认目录，或输入 SiteScope 安装目录的完整路径。例如，如果您不使用所列出的目录路径，而要使用安装目录路径 /opt/9_0/SiteScope，则输入 /opt/9_0/SiteScope。
- 在“到文件”框中，输入要向其导出用户数据文件的目录（该目录必须已经存在）和已导出的用户数据文件的名称。该文件名必须以 **.zip** 结尾。
- 如果 SiteScope 已配置为使用密钥管理数据加密运行，则在“密码短语”框中输入用于 SiteScope 服务器密钥库的密码短语。有关详细信息，请参阅将 SiteScope 配置为使用自定义密钥加密数据 (第 144 页)。使用默认 SiteScope 加密时，此框处于禁用状态。
- 如果还需要导出日志文件，请选择“包括日志文件”。

单击“下一步”完成导出操作。

5. 如果您选择了“导入配置”选项，则会打开“导入配置”屏幕。

备注: 您必须在导入数据之前停止 SiteScope 服务，并在导入数据之后重新启动该服务。有关详细信息，请参阅在 Linux 平台上启动和停止 SiteScope 进程 (第 166 页)。

- 如果选择“使用现有的导出配置文件”，请输入要导入的用户数据文件名。
- 如果选择“从以下 **SiteScope** 安装导入”，请输入要导入用户数据文件的 SiteScope 安装目录。
- 如果还需要导入日志文件，请选择“包括日志文件”。
- 如果 SiteScope 已配置为使用密钥管理数据加密运行，则在“密码短语”框中输入 SiteScope 服务器密钥库的密码短语。在“匹配密码短语”框中输入相同密码短语，确认此密码短语。有关详细信息，请参阅将 SiteScope 配置为使用自定义密钥加密数据 (第 144 页)。使用默认 SiteScope 加密时，这些框处于禁用状态。

单击“下一步”完成导入操作。

6. 如果选择了“配置单独安装的 HP Operations Agent”选项，则会打开“配置 HP Operations Agent”屏幕。

   选择“配置 HP Operations Agent”。这需要完成 HP Operations Agent 的安装。当 SiteScope 与 HP Operations Manager 或 BSM 网关服务器集成时，该代理支持 SiteScope 发送事件并充当度量数据的数据存储设备。

   有关发送事件和报告度量数据的详细信息，请参阅《Integrating SiteScope with HP Operations Manager Products Guide》，该文档在 SiteScope 帮助中或 HP 软件集成网站上提供。

   单击“下一步”完成配置操作。

7. 此时将打开“概要”屏幕。

单击“完成”关闭向导。

使用控制台模式运行配置工具

可以使用命令行或控制台模式安装配置工具。当在远程服务器上配置 SiteScope 时，或者因为任何其他原因导致无法使用用户界面时，可使用此选项。

备注:

- 配置工具中已删除直接从 SiteScope 安装和卸载 HP Operations Agent 的选项。必须手动安装并配置该代理。如果 SiteScope 与 HPOM 或 BSM 集成，则需要使用该代理发送事件和存储度量数据（使用 BSM 中的配置文件数据库将度量数据绘制到性能图的情况除外）。有关安装和配置代理的详细信息，请参阅《Integrating SiteScope with HP Operations Manager Products Guide》，该文档在 SiteScope 帮助中或 HP 软件集成网站上提供。
- 导入配置数据时不能覆盖以下文件夹中的文件：**templates.os**、**templates.post**、**templates.health**、**templates.applications** 和 **conf\ems**。
- 在需要大于 4GB 内存的负载环境中使用 SiteScope 时，应手动增加服务器上的 JVM 堆大小：
  a. 打开 **SiteScope/bin/start-service** 文件进行编辑。
  b. 在最后一行，根据需要增加 **-Xmx4096m** 参数的值，最大可增加到 **-Xmx8192m**（适用于 8GB）。

要使用控制台模式运行配置工具，请执行以下操作：

备注: 以下步骤显示了如何在 Linux 环境中运行配置工具的屏幕捕获。

1. 运行以下命令：

   在 Linux 上运行 /bin/config_tool.sh -i console，或在 Windows 上运行 <SiteScope 根目录>\bin\config_tool.bat -i console。

2. 此时将显示配置选择屏幕。

```
[root@myd-vm05763 bin]# ./config_tool.sh -i console
This wizard enables you you to change the ports assigned to SiteScope,move confi
guration data from one SiteScope installation to another.You can also configure
an external agent for integration with HP Operations Manager and BSM.

Select the actions that you want to perform.
-------------------------------------------------------------
-------------------------------------------------------------
Please select one of the options

->1 - Export: ()
  2 - Import: ()
  3 - Change ports: ()
  4 - HP Operations Agent: ()

: 4
```

   选择要执行的配置操作。

- 输入数字 1 可导出 SiteScope 数据。
- 输入数字 2 可从导出的配置数据 (.zip) 文件，或从现有 SiteScope 安装中导入配置数据。
- 输入数字 3 可更改 SiteScope 服务器所使用的任何端口。
- 输入数字 4 完成 HP Operations Agent 的安装（该代理支持 SiteScope 将度量和事件发送到 HP Operations Manager 和 BSM 应用程序）。

按 ENTER 键继续。

3. 如果您选择了“导出”选项，则会打开“导出配置”屏幕。

```
-------------------------------------------------------------------
请选择下列选项之一

->1 - 导出: ()
  2 - 导入: ()
  3 - 更改端口: ()
  4 - HP Operations Agent: ()

: 1
-------------------------------------------------------------------
SiteScope 源文件夹
文件夹名称 []
PRESS <1> to accept the value [], or <2> to change the value
2
文件夹名称:
/opt/HP/SiteScope
文件夹名称 [/opt/HP/SiteScope]:
PRESS <1> to accept the value [/opt/HP/SiteScope], or <2> to change the value
1
-------------------------------------------------------------------
导出的配置目标文件名
文件名 [SiteScope.zip]
PRESS <1> to accept the value [SiteScope.zip], or <2> to change the value
1

配置完成
```

- 对于“SiteScope 源文件夹”：
  - 输入数字 1 可接受 [ ] 中给定的默认目录。
  - 输入数字 2 可更改值，然后输入 SiteScope 安装目录的完整路径。例如，如果您不使用所列出的目录路径，而要使用安装目录路径 /opt/HP/SiteScope，则输入 /opt/HP/SiteScope。

  按 ENTER 键继续安装。

- 对于“导出的配置目标文件名”：
  - 输入数字 1 可将数据导出到名为 **SiteScope.zip** 的文件中。
  - 输入数字 2 可更改导出的用户数据文件的名称。该文件名必须以 **.zip** 结尾。

  按 ENTER 键完成导出操作。

4. 如果您选择了“导入”选项，则会打开“导入配置”屏幕。

```
请选择下列选项之一

->1 - 导出: ()
  2 - 导入: ()
  3 - 更改端口: ()
  4 - HP Operations Agent: ()

: 2
------------------------------------------------------------------
从现有配置文件或 SiteScope 安装导入配置数据

->1 - 请勿导入: ()
  2 - 从文件导入: ()
  3 - 从文件夹导入: ()

: 2
------------------------------------------------------------------
输入导入的配置文件的名称
文件名 []
PRESS <1> to accept the value [], or <2> to change the value
2
文件名:
SiteScope.zip
文件名 [SiteScope.zip]:
PRESS <1> to accept the value [SiteScope.zip], or <2> to change the value
1

配置完成
```

选择配置数据选项:

- 如果不需要导入配置数据，则输入数字 1。
- 输入数字 2 可从文件导入配置数据。如果选择此选项:
  - 输入数字 1 可接受 [ ] 中给定的默认文件名。
  - 输入数字 2 可更改值，然后输入要从中导入配置数据的文件名。输入数字 1 可接受名称。
- 输入数字 3 可从 SiteScope 安装目录导入配置数据。如果选择此选项:
  - 输入数字 1 可接受 [ ] 中给定的默认目录。
  - 输入数字 2 可更改值，然后输入要从中导入用户数据文件的 SiteScope 安装目录。输入数字 1 可接受名称。

按 ENTER 键完成导入操作。

备注: 如果导入的配置包含过期证书，过期证书将在配置导入的默认 SiteScope 密钥库内进行合并。这种情况可导致 SSL 证书监控器处于错误状态。要避免这种情况的发生，应在导出配置数据之前删除所有过期证书。

5. 如果您选择了“更改端口”选项，则会打开“更改端口”屏幕。

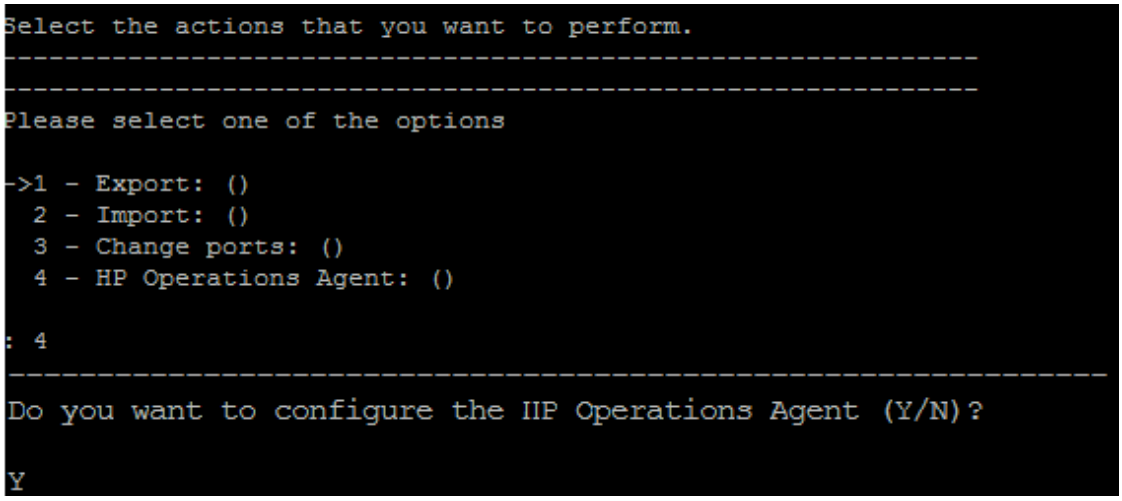
```
: 3
---------------------------------------------------------------
SiteScope 用户界面端口
端口 [8080]
PRESS <1> to accept the value [8080], or <2> to change the value
1
---------------------------------------------------------------
Tomcat 关闭端口
端口 [28005]
PRESS <1> to accept the value [28005], or <2> to change the value
1
---------------------------------------------------------------
Tomcat AJP 连接器端口
端口 [28009]
PRESS <1> to accept the value [28009], or <2> to change the value
1
---------------------------------------------------------------
SSL 端口
端口 [8443]
PRESS <1> to accept the value [8443], or <2> to change the value
1
---------------------------------------------------------------
JMX 控制台端口
端口 [28006]
PRESS <1> to accept the value [28006], or <2> to change the value
1
---------------------------------------------------------------
经典用户界面端口
端口 [8888]
PRESS <1> to accept the value [8888], or <2> to change the value
1
---------------------------------------------------------------
经典用户界面 (安全) 端口
端口 []
PRESS <1> to accept the value [], or <2> to change the value
1

配置完成
```

根据需要修改由 SiteScope 服务器使用的端口。端口号必须为 1 到 65534 之间的数字。除经典用户界面之外，所有其他组件都必须具有端口号。

备注: 建议使用范围在 28000-28100 之间的端口号，以避免和其他 BSM 产品使用的端口发生冲突。

按 ENTER 键完成更改端口的操作。

6. 如果选择了 **HP Operations Agent** 选项，则会打开 HP Operations Agent 屏幕。



输入 Y 完成 HP Operations Agent 的安装。

完成代理安装后，建议重新启动 SiteScope 服务器。

有关使用 HP Operations Agent 报告度量数据的详细信息，请参阅《Integrating SiteScope with HP Operations Manager Products Guide》，该文档在 SiteScope 帮助中或 HP 软件集成网站上提供。

备注: 使用 BSM 中的配置文件数据库将度量数据绘制到性能图时，不需要使用 HP Operations Agent。建议使用配置文件数据库选项，因为此为更稳定、更具伸缩性的数据源，且不需要配置 HP Operations 集成。

在静默模式下运行配置工具

可以在静默模式下运行 SiteScope 配置工具。此功能支持您从 SiteScope 的当前版本备份 SiteScope 配置数据，而无需在配置工具屏幕中进行导航，也无需输入选择项。所有配置参数将按照您在响应文件中定义的值进行分配。

运行静默配置之前的注意事项

在运行静默配置之前，请考虑以下问题：

- 在静默模式下运行配置时将不会显示任何消息。但是，您可以在日志文件中查看配置是否成功等配置信息。可以在下列目录中找到配置日志文件：
  - Windows 平台：**%tmp%\HPSiteScope_config_tool.log**
  - Linux 平台：**/tmp/HPSiteScope_config_tool.log**
- 将配置数据从一个 SiteScope 安装移动到另一个时，请确保从中获取配置数据的源 SiteScope 服务器与要向其导入数据的目标 SiteScope 服务器位于同一个时区中。
- 如果导入的配置包含过期证书，过期证书将在配置导入的默认 SiteScope 密钥库内进行合并。这种情况可导致 SSL 证书监控器处于错误状态。要避免这种情况的发生，应在导出配置数据之前删除所有过期证书。
- 将配置导入到相同版本的 SiteScope 中时，必须重命名或删除所有模板示例容器，以便导入新的模板示例。
- 您必须在导出或导入数据之前停止 SiteScope 服务，并在导出或导入数据之后重新启动该服务。有关详细信息，请参阅在 Windows 平台上启动和停止 SiteScope 服务 (第 165 页)和在 Linux 平台上启动和停止 SiteScope 进程 (第 166 页)。
- 导入配置数据时不能覆盖以下文件夹中的文件：**templates.os**、**templates.post**、**templates.health**、**templates.applications** 和 **conf\ems**。
- 如果选择了导出配置选项：
  - 由于导出 SiteScope 数据时不会复制 **\htdocs** 目录，因此需要备份此目录，并在升级后将其复制到 SiteScope 目录，以便查看旧报告。
  - 配置工具支持在导出数据时包含服务器证书和脚本。有关从 SiteScope 的早期版本导出数据时如何包括服务器证书和脚本的详细信息，请参阅升级现有 SiteScope 安装 (第 63 页)。
- 如果选择了调整大小选项（仅适用于 Windows 平台）：
  - 仅当 SiteScope 服务器的物理内存大于配置工具配置的最大 JVM 堆大小（Xmx，4GB）时，才可以更改大小。
  - 如果通过运行 **<SiteScope 安装>\bin** 目录中的 **go.bat** 文件来启动 SiteScope，请打开 **go.bat** 文件，并根据需要增加 **– Xmx4096m** 参数，最大可增加到 **– Xmx8192m**（适用于 8GB）。
- 如果选择了更改端口选项，则建议使用范围在 28000-28100 之间的端口号，以避免和其他 Business Service Management 产品使用的端口发生冲突。
- 在需要大于 4GB 内存的负载环境中使用 SiteScope 时，应手动增加服务器上的 JVM 堆大小：

a. 打开 **SiteScope/bin/start-service** 文件进行编辑。
b. 在最后一行，根据需要增加 **-Xmx4096m** 参数的值，最大可增加到 **-Xmx8192m**（适用于 8GB）。

- 配置工具中已删除直接从 SiteScope 安装和卸载 HP Operations Agent 的选项。必须手动安装并配置该代理。如果 SiteScope 与 HPOM 或 BSM 集成，则需要使用该代理发送事件和存储度量数据（使用 BSM 中的配置文件数据库将度量数据绘制到性能图的情况除外）。有关安装和配置代理的详细信息，请参阅《Integrating SiteScope with HP Operations Manager Products Guide》，该文档在 SiteScope 帮助中或 HP 软件集成网站上提供。

运行静默配置

使用 **configtoolparams.txt** 文件运行静默配置。由于此文件具有特定的格式，所以应使用 **<SiteScope 安装目录>\examples\silent_config_tool** 文件夹中的示例文件创建静默配置文件。

要运行 SiteScope 的静默配置，请执行以下操作：

1. 导航到位于 **<SiteScope 安装目录>\examples\silent_config_tool** 文件夹中的 **configtoolparams.txt** 文件。
2. 复制该文件，并将其保存到选择的位置。
3. 打开文件，根据配置需要进行修改（遵循示例文件的说明），然后保存文件。
4. 从命令行使用 **-i silent** 和 **-f <应答文件>** 标志运行配置。

   例如：

   config_tool -i silent -f c:\configtoolparams.txt (Windows)

   或

   ./config_tool.sh -i silent -f /opt/configtoolparams.txt (Linux)

第 16 章: 卸载 SiteScope

本章包括:

在 Windows 平台上卸载 SiteScope

您可以从服务器计算机上卸载 SiteScope 11.30 以及在其基础上安装的任何次次版本（修补程序），或仅卸载 SiteScope 次次版本。对于在 Windows 平台上运行的 SiteScope，安装 SiteScope 时将包含一个用于从计算机中卸载 SiteScope 软件的程序。

如何卸载 SiteScope 以及在其基础上安装的任何次次版本

1. 停止 SiteScope 服务。
   a. 选择“开始”>“所有程序”>“管理工具”>“服务”。此时将打开“服务”对话框。
   b. 从服务列表中选择“SiteScope”服务。如果 SiteScope 正在运行，则右键单击此服务以显示操作菜单，并选择“停止”。等待服务的“状态”显示为已停止，关闭“服务”窗口。
2. 卸载 SiteScope。
   a. 选择“开始”>“所有程序”>“HP SiteScope”>“卸载 HP SiteScope”。
   b. 在“选择区域设置”屏幕上，选择要显示的语言，然后单击“确定”。
   c. 在“应用程序维护”屏幕上，选择“卸载”并单击“下一步”。
   d. 在“安装前摘要”屏幕中，单击“卸载”。

      在卸载操作期间，会在屏幕上显示各个软件组件及其卸载进度。

      卸载过程完成后，将打开“卸载完成”窗口，并显示卸载过程的概要信息。
   e. 在“卸载完成”窗口中，单击“完成”，关闭卸载程序。

      通过“查看日志文件”链接，可以在 Web 浏览器中访问卸载日志文件。有关已删除的程序包的详细信息，请单击“详细信息”选项卡。
3. 取消配置并卸载 HP Operations Agent

   如果要删除 SiteScope 服务器上安装的 HP Operations Agent，您需要先取消配置，然后再将其卸载。
   a. 要手动取消配置 HP Operations Agent，请运行以下命令:
      i. msiexec /x <SiteScope 根目录>\installation\components\oa_policy_signing_tool\win64\HPOprIAPA-09.00.111-Win5.2_64-release.msi /quiet
      ii. <SiteScope 根目录>\installation\components\oa_template_management\all\install.bat -remove windows64
   b. 要卸载安装在 SiteScope 服务器上的代理，请参阅《HP Operations Agent 11.14 Installation Guide》(https://softwaresupport.hp.com/group/softwaresupport/search-result/-

/facetsearch/document/KM01001255) 中的说明。

4. 完成卸载后，请重新启动计算机（如果系统要求）。

在 Linux 平台上卸载 SiteScope

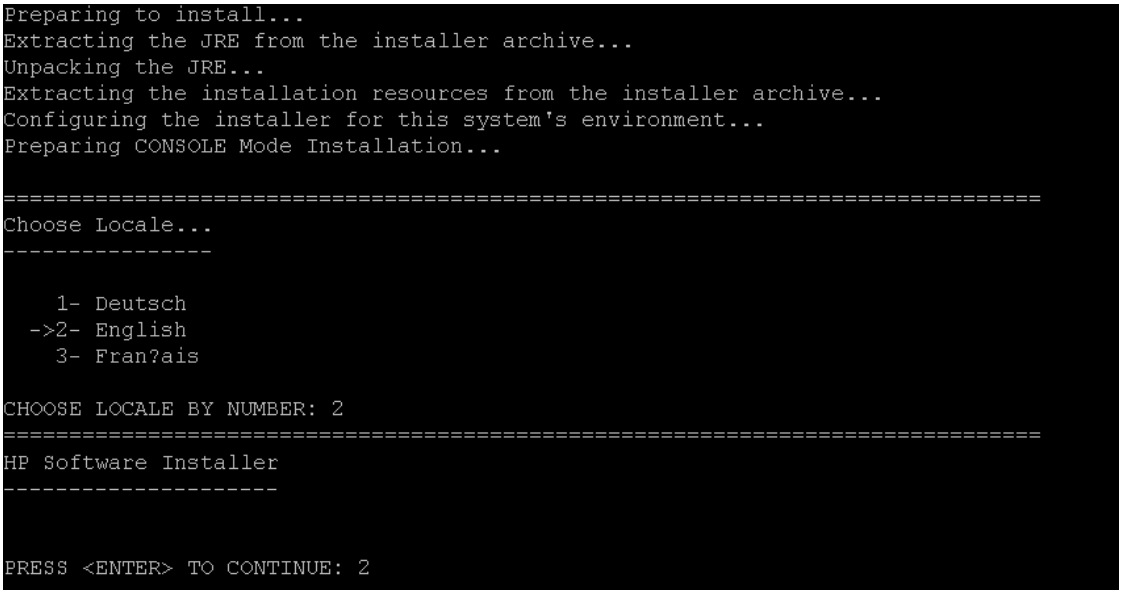
您可以从服务器计算机上卸载 SiteScope 11.30 以及在其基础上安装的任何次次版本（修补程序），或仅卸载 SiteScope 次次版本。对于在 Linux 平台上运行的 SiteScope，安装 SiteScope 时将包含一个用于从计算机中卸载 SiteScope 软件的脚本。如果无法运行该脚本，可以手动删除 SiteScope 文件和目录。

如何卸载 SiteScope 以及在其基础上安装的任何次次版本

1. 使用获得授权的帐户登录到运行 SiteScope 的计算机，执行 SiteScope 目录中的脚本。通常情况下，此帐户应是运行 SiteScope 的帐户。
2. 通过运行 **<安装路径>/SiteScope** 目录中的 **stop** shell 脚本，停止 SiteScope。以下是一个用于运行该脚本的命令行示例：**SiteScope/stop**。

   此时会显示一条消息，指示 SiteScope 已停止。

3. 如果在 X Windows 模式下工作，请运行以下命令：**/opt/HP/SiteScope/installation/bin/uninstall.sh**
4. 如果在控制台模式下工作，则需要通过运行以下命令卸载 SiteScope 11.30：**/opt/HP/SiteScope/installation/bin/uninstall.sh –i console**。
5. HP Software 安装程序将启动。指定区域设置并按 ENTER 键。



6. 键入 1 并按 ENTER 键，确认要卸载 SiteScope。

```
================================================================================
Maintenance Selection
---------------------

Modify, repair or uninstall the application
If you want to change something on a previous step, type 'back'.
You may cancel this installation at any time by typing 'quit'.



  ->1- Uninstall        Uninstall the application from your computer.

Please select one of the options...: 1
```

7. 此时将显示关于包的卸载状态的消息，然后卸载过程将完成：

```
================================================================================
Uninstallation Complete
-----------------------


The uninstallation has been successfully completed.
```

8. 取消配置并卸载 HP Operations Agent

   如果要删除 SiteScope 服务器上安装的 HP Operations Agent，您需要先取消配置，然后再将其卸载。

   a. 要手动取消配置 HP Operations Agent，请在 Linux 终端上运行以下命令：

      i. rpm -e HPOprIAPA

      ii. <SiteScope 根目录>\installation\components\oa_template_management\all\install.sh -remove linux64

   b. 要卸载安装在 SiteScope 服务器上的代理，请参阅《HP Operations Agent 11.14 Installation Guide》(https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM01001255) 中的说明。

第 4 部分: 安全运行 SiteScope

第 17 章: 强化 SiteScope 平台

本章包括:

概述

本章描述了可用于强化 SiteScope 平台的多个配置及设置选项。

作为一款系统可用性监控工具，SiteScope 可以访问系统信息，如果没有采取安全措施，这些信息可能会危及系统安全。您应当借助本节中介绍的配置和设置选项来保护 SiteScope 平台。

警告: 应有两台 Web 服务器处于活动状态，为两个版本的 SiteScope 产品界面提供服务：SiteScope Web 服务器和 SiteScope 附带的 Apache Tomcat 服务器。要限制对 SiteScope 的所有访问，必须对上述两种服务器应用适当的设置。

设置 SiteScope 用户首选项

SiteScope 用户配置文件用于要求用户在访问 SiteScope 界面时提供用户名和密码。安装后，所有对运行 SiteScope 的服务器拥有 HTTP 访问权限的用户均可正常访问 SiteScope。

默认情况下，将仅使用一个用户帐户来安装 SiteScope，并且不会为此帐户定义默认的用户名或密码。此帐户即是管理员帐户。

在安装并访问产品后，您应当为此帐户定义用户名和密码。您还可以创建其他用户帐户配置文件，以控制其他用户访问产品的方式以及可以执行的操作。有关创建用户帐户的详细信息，请参阅 SiteScope 帮助中《使用 SiteScope》中的“用户管理首选项”部分。

密码加密

所有 SiteScope 密码均使用名为“三重数据加密标准”(TDES) 的方法进行加密。TDES 在每个 64 位文本块上连续使用三次数据加密算法，其用到的两个或三个密钥均不相同。因此，未授权用户复制原始密码的难度极大。

使用传输层安全性 (TLS) 访问 SiteScope

可将 SiteScope 配置为使用 TLS 来控制对产品界面的访问。有关详细信息，请参阅将 SiteScope 配置为通过安全连接通信 (第 132 页)。

备注: 传输层安全性 (TLS) 是安全套接字层 (SSL) 的新名称。SiteScope 用户界面仍然包含对 SSL 的引用。这两个术语在 SiteScope 中可以通用。

智能卡身份验证

智能卡是用于在安全系统中标识用户的物理设备。这些智能卡可用于存储验证用户身份并允许用户访问安全环境的证书。

SiteScope 支持使用智能卡进行用户身份验证。如果配置了智能卡身份验证，就必须使用有效的智能卡才可登录到 SiteScope。SiteScope 可使用各种类型的智能卡，包括:

- **CAC。**通用访问卡（通常称为 CAC 卡），是美国国防部使用的一种智能卡。对军事政府系统执行任何操作都必须使用这种智能卡。
- **PIV。**与军事机构一样，民用机构的联邦职员和承包商也需要智能卡。他们使用类似的标准 PIV（个人身份认证）卡。这些卡与 CAC 卡略有不同，卡上印有各种信息，具体内容取决于其发行机构。这些卡使用的 CA（证书颁发机构）服务器集与 CAC 所使用的 CA 服务器集不同。PIV 卡包括 PIV 系统所需的各种个人专用数据，授予订户访问联邦设施和信息系统的权限；确保所有适用的联邦应用程序具有合适的安全级别；并在使用该标准的联邦组织间实现互操作性。

有关配置智能卡身份验证的详细信息，请参阅配置智能卡身份验证 (第 132 页)。

备注: 市场上有各种智能卡供应商。要支持所有不同排列组合使用客户端证书，可以在 **<SiteScope 根目录>\groups\master.config** 文件中使用以下参数:

- _clientCertificateAuthJITCComplianceEnforcementEnabled
- _clientCertificateAuthSmartCardEnforcementEnabled
- _clientCertificateAuthIsGetUidFromSubject
- _clientCertificateAuthAllowLocalUsers
- _clientCertificateSubjectAlternativeNamesGeneralName
- _clientCertificateAuthEnabled

联合互操作性测试司令部 (JITC) 认证

JITC 是一个美国军事组织，负责测试涉及军队和政府多个分支机构的技术。JITC 为获取和部署全球“以网络为中心的”军事能力提供测试、评估和认证服务。

SiteScope 目前正在接受 JITC 的测试和评估。JITC 认证是支持 CAC 和智能卡身份验证登录所需的通用标准认证之一。

备注: 完成评估后将对本节进行更新。

通用标准认证

HP SiteScope 致力于提供业界领先的符合全球行业标准和政府认证计划的监控软件。

HP SiteScope 正在进行评估保证级别 (EAL) 2+ 的通用标准认证。通用标准之类的认证对联邦政府的安全措施而言至关重要。这些安全认证不仅可以保护政府客户免遭现今的高级攻击和数据窃取，还可以满足 HP 全球业务客户的需求。

信息技术安全评估通用标准（简称通用标准）是计算机安全认证的一项国际标准。该通用标准验证了产品的功能是否符合承诺，以及产品是否是使用保证安全性和稳定性的方式构建的。认证结果会经由独立测试实验室进行验证和评估。该项认证也是美国政府采购安全产品的必需要求。

FIPS 140-2 符合性

作为通用标准认证的一部分，SiteScope 可配置为以 FIPS 140-2 兼容模式运行。FIPS 140-2（联邦信息处理标准 140-2）是一系列针对密码模块的安全要求。FIPS 140-2 受 CMVP（密码模块验证体系）监督，后者是美加两国政府共同努力的结果。

SiteScope 11.30 是目前唯一可以配置为以 FIPS 140-2 兼容模式运行的 SiteScope 版本。

有关 FIPS 140-2 以及将 SiteScope 配置为以 FIPS 140-2 兼容模式运行的详细信息，请参阅将 SiteScope 配置为在 FIPS 140-2 兼容模式下运行 (第 137 页)。

使用自定义密钥加密数据

默认情况下，SiteScope 使用标准加密算法来加密持久性数据（包括所有已定义监控器、组、警报和模板的配置数据以及许多其他 SiteScope 实体）。可以在强化工具中使用密钥管理来更改用于加密持久性数据的加密密钥。

有关详细信息，请参阅将 SiteScope 配置为使用自定义密钥加密数据 (第 144 页)。

保障用户帐户安全的建议

下表列出了 SiteScope 中的各种可用帐户，以及保障这些帐户安全可采取的步骤。

用户帐户	描述	强化步骤
默认（管理员）	默认情况下，将仅使用一个用户帐户来安装 SiteScope，并且不会为此帐户定义默认的用户名或密码。	要限制帐户及其权限的访问，我们建议在安装和访问产品后编辑管理员帐户配置文件，以在其中包含用户登录名和登录密码。SiteScope 随后会显示一个登录页面，登录之后才能访问 SiteScope。 您应创建其他用户帐户配置文件，以控制其他用户访问产品的方式以及可以执行的操作。有关详细信息，请参阅 SiteScope 帮助中《使用 SiteScope》的“用户管理首选项”部分。

用户帐户	描述	强化步骤
		注意：要创建其他帐户，必须首先编辑管理员帐户配置文件，以包括用户登录名和密码。
集成查看器	默认情况下，SiteScope 提供从 HPOM 事件进行向下搜索所使用的“集成查看器”用户。这是已被授予查看权限以及刷新组和监控器权限的一般用户。有关详细信息，请参阅《与 HP Operations Manager 产品集成》。	如果具有 HPOM 或 BSM 集成，我们建议更改集成查看器帐户配置文件的预定义登录密码。 如果没有 HPOM/BSM 集成，则可以禁用或删除此用户。
SiteScope 服务用户	**对于 Windows：** 默认情况下，将 SiteScope 作为本地系统帐户安装并运行（不适用于 Linux 安装）。此帐户在本地计算机上具有多种权限，并可以访问大多数系统对象。在本地系统帐户下运行时，SiteScope 会尝试使用 SiteScope 中配置的服务器凭据连接到远程服务器。 **对于 Linux：** 您必须使用 root 用户将 SiteScope 安装到 Linux 环境中。	**对于 Windows：** 我们建议将 SiteScope 服务设置为以具有域管理权限的用户身份登录。 这能让 SiteScope 有权访问域中的监控器服务器数据。输入可以访问远程服务器的帐户和密码（并确认密码）。在域环境中，使用域管理员用户；在非域环境中，使用内置管理员用户。 可以在安装期间（请参阅“安装”）或安装后更改此设置。 有关详细信息，请参阅使用安装向导进行安装 (第 80 页)。 **对于 Linux：** 在安装 SiteScope 之后，您可以创建有权运行 SiteScope 的非 root 用户帐户（除非 SiteScope Web 服务器在特权端口上运行，这种情况下需要由 root 用户运行）。有关如何配置非 root 用户以使其有权运行 SiteScope 的详细信息，请参阅保障用户帐户安全的建议 (第 129 页)。
JMX 用户	默认情况下，JMX 可以远程访问 SiteScope 服务器（可使用强化工具配置使用 JMX 协议的连接）。	要全方位保障 SiteScope 的安全，建议使用强化工具禁用 JMX 远程访问。有关详细信息，请参阅如何使用强化工具配置 JMX 远程访问 (第 155 页)。
API 用户	通常情况下没有这种用户（SiteScope 有许多 API 不需要身份验证）。	如果需要禁用旧的未用 API 用户，可以通过将“首选项”>“基础结构首选项”>“自定义设置”中的“禁用旧 API”设置为 true 来实现。

配置登录时显示的警告横幅

您可使 SiteScope 在用户登录到 SiteScope 时显示一条警告消息，告知用户将要登录到安全系统。

要配置在登录时显示的消息，请执行以下操作：

1. 在文本编辑器中打开 **<SiteScope 根目录>\templates.fips\banner.txt** 文件，然后输入希望显示在登录屏幕上的文本。
2. 在文本编辑器中打开 **<SiteScope 根目录>\groups\master.config** 文件，然后将 **_ isLogonWarningBannerDisplayed=** 属性的值更改为 **true**。

   当用户登录到 SiteScope 时，将会显示通知消息。用户必须在使用 SiteScope 前先确认该消息。

第 18 章: 将 SiteScope 配置为通过安全连接通信

本章包括:

将 SiteScope 配置为需要安全连接

可将 SiteScope 配置为需要通过安全连接访问其界面和接口（UI 和 API）。可通过以下步骤执行此操作:

1. 获取颁发给 SiteScope 服务器的 FQDN 的服务器证书。
2. 将 SiteScope 配置为仅响应通过安全通道发送的请求。

可通过以下任一方法执行此操作:

- 使用强化工具配置 SiteScope 来执行此配置（建议方法）。有关详细信息，请参阅如何使用强化工具将 SiteScope 配置为需要安全连接 (第 150 页)。
- 手动将 SiteScope 配置为使用 TLS。有关详细信息，请参阅手动将 SiteScope 配置为使用安全连接 (第 183 页)。

配置智能卡身份验证

智能卡是用于在安全系统中标识用户的物理设备。这些智能卡可用于存储验证用户身份并允许用户访问安全环境的证书。

SiteScope 支持使用智能卡进行用户身份验证。如果配置了智能卡身份验证，就必须使用有效的智能卡才可登录到 SiteScope。

可将 SiteScope 配置为使用这些证书替代用户各自手动输入用户名和密码的标准模型。您需要定义从每张智能卡上存储的证书中提取用户名的方法。

如果 SiteScope 已配置为使用智能卡身份验证，则用户只能使用有效的智能卡登录 SiteScope。通过手动输入用户名和密码进行登录的选项将对所有用户锁定，除非禁用智能卡配置。

如果在 BSM 中配置了智能卡身份验证，要想将 SiteScope 与 BSM 集成，则必须配置 SiteScope 智能卡身份验证以验证 BSM 客户端证书。有关详细信息，请参阅将 SiteScope 配置为连接到需要安全连接的 BSM 服务器 (第 147 页)。

类似地，在 SiteScope 已配置为使用智能卡身份验证的情况下，如果要允许 BSM 与 SiteScope 通信，则必须先将 BSM 配置为在 SiteScope 中使用客户端证书进行身份验证。有关详细信息，请参阅将 SiteScope 配置为连接到需要安全连接的 BSM 服务器 (第 147 页)。

注意: 如果已启用智能卡强制执行，那么运行在 Windows 操作系统上的 Internet Explorer 将成为

唯一支持的浏览器。

如果已禁用智能卡强制执行，但启用了客户端证书身份验证，那么如果要在 Firefox 中使用 SiteScope，请参阅**在客户端认证启用的情况下使用 Firefox (第 134 页)****。**

提示: **有关智能卡的详细信息，请参阅《Smart Card Authentication Configuration Guide》(**https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM01134341**)。**

将 SiteScope 配置为需要客户端证书身份验证

如果将 SiteScope 配置为在 TLS 上工作（请参阅**将 SiteScope 配置为需要安全连接 (第 132 页)****），则可以将 SiteScope 和 SiteScope 公共 API 客户端配置为需要客户端证书身份验证。**

可通过强化工具执行此操作。有关详细信息，请参阅**如何使用强化工具配置 SiteScope 和 SiteScope 公共 API 客户端证书身份验证 (第 155 页)****。**

第 19 章: 高级强化配置

本章包括:

将 SiteScope 配置为验证证书吊销

可使用强化工具将 SiteScope 配置为验证客户端证书是否已被吊销。有关详细信息，请参阅如何使用强化工具将 SiteScope 配置为验证证书吊销 (第 151 页)。

在客户端认证启用的情况下使用 Firefox

如果已禁用智能卡强制执行，但启用了客户端证书身份验证，那么如果要在 Firefox 中打开 SiteScope 用户界面，就必须执行以下操作:

1. 将您的个人证书导入 Firefox 中，步骤如下:
   a. 在 Firefox 中，转至“工具”>“选项”>“高级”>“证书”>“查看证书”。将打开“证书管理器”对话框。
   b. 单击“导入”，然后打开 **.pfx**（或 **.p12**）文件格式的个人证书。此时将打开“密码输入”对话框。
   c. 输入用于加密此备份证书的密码，然后单击“确定”。此证书将出现在“证书管理器”对话框中，表明证书已经添加到 Firefox。
2. 将您的个人证书导入客户端 JRE 中，步骤如下:
   a. 在 JRE 中，打开“Java 控制面板”。
   b. 转至“安全”>“证书”并在“证书类型”中选择“客户机验证”。
   c. 单击“导入”，然后打开先前导入 Firefox 中的客户端证书。
   d. 单击“确定”。个人证书将出现在 JRE 中。
3. 在 Firefox 中输入 SiteScope URL。此时将打开“用户标识请求”对话框。选择您在第 1 步中创建的个人证书，以将其作为标识。

将证书颁发机构证书导入 SiteScope 信任库

要使 SiteScope 信任客户端证书，SiteScope 必须信任颁发该客户端证书的证书颁发机构。要使 SiteScope 信任证书颁发机构，必须将该证书颁发机构的证书存储到 SiteScope 服务器信任库和主信任库中。

SiteScope 服务器信任库负责对来自客户端（API 和浏览器）的所有传入连接请求进行身份验证。

SiteScope 主信任库是位于 SiteScope 安装目录下 Java 目录中的证书颁发机构 Java 信任库。该信任库负责管理 SiteScope 证书。

可使用强化工具将证书颁发机构的证书导入 SiteScope 服务器信任库和主信任库。有关详细信息，请参阅如何使用强化工具将证书颁发机构证书导入到 SiteScope 信任库中 (第 152 页)。

禁用 JMX 远程访问

JMX 默认情况下可以远程访问 SiteScope 服务器。您可以禁用该访问。

备注: 要完全确保 SiteScope 的安全性，建议禁用 JMX 远程访问。

可使用强化工具配置 JMX 远程访问。有关详细信息，请参阅如何使用强化工具配置 JMX 远程访问 (第 155 页)。

恢复已备份的配置

运行强化工具时，将自动备份现有的 SiteScope 配置。要恢复已备份的配置，请参阅如何使用强化工具恢复备份的配置 (第 155 页)。

在 SiteScope 中配置搭建框架筛选器

备注: 此主题仅在您已安装 SiteScope 11.30 IP1 时有效。

框架是独立于容器显示内容的网页或浏览器窗口的一部分，可单独加载内容。默认情况下，启用 SiteScope 的搭建框架功能。

如果您不希望其他站点搭建 SiteScope 的框架，或希望只允许搭建部分框架，则必须执行以下步骤：

1. 打开 **<SiteScope 根目录>\groups** 中的 **master.config** 文件，然后根据需要配置 **_disableFramingFiltering** 属性：
   - **True**。已禁用筛选器，将允许从每个网页搭建 SiteScope 框架。（这是默认设置。）
   - **False**。已启用筛选器，将阻止从网页搭建 SiteScope 框架，包括 BSM、HPOM 和 Performance Center 等 HP 产品。例如，BSM 的托管用户界面将不起作用。
   - **Smart**。根据 **_framingFilteringPlugsClasses** 属性中列出的插件，支持搭建部分 SiteScope 框架。
2. 使用搭建部分框架时，创建要按筛选器应用的插件，然后将这些插件添加到 **_framingFilteringPlugsClasses** 属性中。
   a. 导航到 **master.config** 文件中的 **_framingFilteringPlugsClasses** 属性。默认情况下，此属性包含以下预置插件：
      - com.mercury.sitescope.web.request.framing.plugs.LWSSOPlug。允许通过轻量单一登录 (LW-SSO) 令牌发送的请求。

- com.mercury.sitescope.web.request.framing.plugs.BSMPlug。允许从 BSM 的 SAM 管理程序发送的请求。
- com.mercury.sitescope.web.request.framing.plugs.PerformanceCenterPlug。允许来自 Performance Center 的请求。

从属性中删除任意预置插件可禁用该插件。

b. 要添加您自己的插件，请执行以下操作：

i. 编写必须实现以下接口的插件：com.mercury.sitescope.web.request.framing.IFramingPlug。

此接口位于 **<SiteScope 根目录>\WEB-INF\lib\ss_webaccess.jar** 中。此 jar 必须位于类路径中才能编译插件。

下面是一个插件示例，该插件在将请求名称为 *exampleParameter* 的参数设置为 true 时允许为该参数搭建框架：

```
package com.company.sitescope.examples.plug
import javax.servlet.ServletRequest;
import com.mercury.sitescope.web.request.framing.IFramingPlug;
public class ExamplePlug implements IFramingPlug{
   @Override
     public boolean isAuthorized(ServletRequest request) {
       //Add the code that will determine whether this request comes from an authorized product.
       if (request == null){
           return false;
        }
        HttpServletRequest httpServletRequest = (HttpServletRequest)request;
        if (httpServletRequest.getParameter("exampleParameter") == null){
        return false;
        }

        return "true".equalsIgnoreCase((String)httpServletRequest.getParameter
("exampleParameter"));
        }
}
```

ii. 向 **master.config** 文件中的 **_framingFilteringPlugsClasses** 属性添加类完全限定名称，用逗号分隔。

例如，应将 com.company.sitescope.examples.plug.ExamplePlug 附加到列表。

iii. 创建一个包含您自己所有插件的 jar，然后将其添加到 **<SiteScope 根目录>\WEB-INF\lib** 文件夹中。

3. 重新启动 SiteScope（对 **master.config** 文件进行任何更改后需要进行）。

第 20 章: 将 SiteScope 配置为在 FIPS 140-2 兼容模式下运行

本章包括:

FIPS 140-2 符合性概述

FIPS 140-2（联邦信息处理标准）是美国和加拿大政府的一项针对加密和密码模块的认证标准，组成完整解决方案的每一项单独的加密组件都需要独立进行认证。该认证标准旨在定义计算机系统中使用的加密过程、加密体系结构、加密算法和其他加密技术。完整的 FIPS 文本可从美国国家标准与技术研究院 (NIST) 联机得到。

要在 FIPS 140-2 兼容模式下运行，SiteScope 管理员必须使用 SiteScope 强化工具启用 FIPS 140-2 模式。SiteScope 会在启动时运行自我测试，执行密码模块完整性检查，然后重新生成密钥材料。此时，SiteScope 即在 FIPS 140-2 模式下运行。

启用 FIPS 模式的理由:

如果您的组织符合以下情况，可能需要以 FIPS 模式运行 SiteScope:

- 联邦政府部门或承包商。
- 希望通过改善安全性来保护您的业务免受高级攻击和数据窃取带来的损失。

软件要求

您的操作系统和浏览器需要满足特定的版本和设置要求才能实现 FIPS 兼容。

虽然 FIPS 模式支持 SiteScope 支持的所有浏览器，但并非所有版本的操作系统均可满足 FIPS 所需的密码要求。因此，FIPS 模式不支持 SiteScope 通常支持的部分操作系统。

要以 FIPS 模式运行，必须将 SiteScope 安装到以下操作系统之一上:

· Windows Server 2008 R2（64 位）

· Windows Server 2012 R2（64 位）

JDBC 驱动程序

以 FIPS 模式运行 SiteScope 时，应考虑使用您的 JDBC 驱动程序，而非随 SiteScope 提供的默认驱动程序。

与不兼容 FIPS 的应用程序连接的 SiteScope

如果 SiteScope 连接到的应用程序使用未得到 FIPS 审批的加密算法，则 SiteScope 与该应用程序的连接不是 FIPS 兼容的（即便已在 SiteScope 上启用 FIPS-140-2 模式）。

启用 FIPS 140-2 兼容模式

要在使用安全连接时启用 SiteScope 以按 FIPS 140-2 兼容模式运行，必须执行以下步骤：

- 第 1 步：配置 LDAP 集成 (第 138 页)
- 第 2 步：配置 Windows 操作系统以使用 FIPS 140-2 兼容模式 (第 138 页)
- 第 3 步：运行 SiteScopeHardeningToolRuntime (第 140 页)
- 第 4 步：禁用 JMX 远程访问 SiteScope 服务器 (第 140 页)
- 第 5 步：配置 SSL (第 140 页)
- 第 6 步：配置客户端身份验证 (第 141 页)

备注: 如果计划启用密钥管理数据加密（提供比常规加密更强的加密），则必须在启用或禁用 FIPS 140-2 模式之后执行此操作。如果已配置密钥管理数据加密，则必须执行如何在更改加密密钥之后启用或禁用 FIPS 兼容模式 (第 145 页)中所述的步骤。

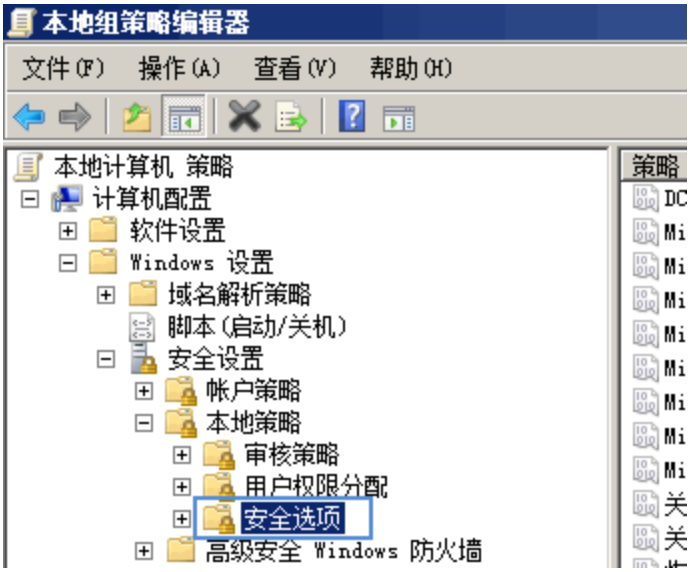
第 1 步：配置 LDAP 集成

要使用客户端证书登录 SiteScope，需要启用 LDAP 用户身份验证。

1. 在 SiteScope 上配置 LDAP 服务器。有关详细信息，请参阅 SiteScope 帮助众《使用 SiteScope》指南中的“如何将 SiteScope 设置为使用 LDAP 身份验证”。
2. 在 SiteScope 用户管理中为 LDAP 用户创建新角色。
3. 将 SiteScope 管理员登录名更改为 LDAP 中的用户电子邮件地址。这应当与客户端证书中的用户相同（在第 6 步：配置客户端身份验证 (第 141 页)的第 3 步输入）。不要输入密码。

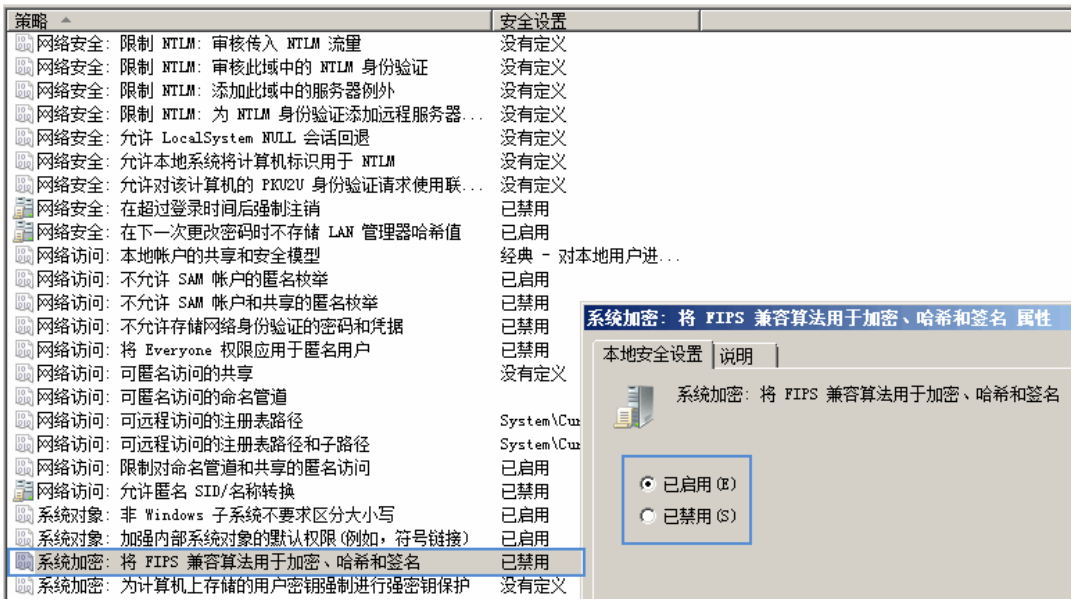
第 2 步：配置 Windows 操作系统以使用 FIPS 140-2 兼容模式

1. 配置 Windows 操作系统以使用 FIPS 140-2 模式。
   a. 使用管理凭据登录到计算机。
   b. 单击“开始”，然后单击“运行”，键入 gpedit.msc，然后按 ENTER 键。此时将打开“本地组策略编辑器”。
   c. 在本地组策略编辑器中，双击“计算机配置”下的“Windows 设置”，然后双击“安全设置”。
   d. 在“安全设置”节点下，双击“本地策略”，然后单击“安全选项”。



e. 在详细信息窗格中，双击“系统加密：使用 FIPS 兼容算法用于加密、哈希和签名”。

f. 在“系统加密：使用 FIPS 兼容算法用于加密、哈希和签名”对话框中，单击“已启用”，然后单击“确定”关闭对话框。



g. 关闭本地组策略编辑器。

h. 确保该安全选项已启用。

i. 打开注册表编辑器。单击“开始”，然后单击“运行”，键入 regedit，然后按 ENTER 键。此时将打开“注册表编辑器”。

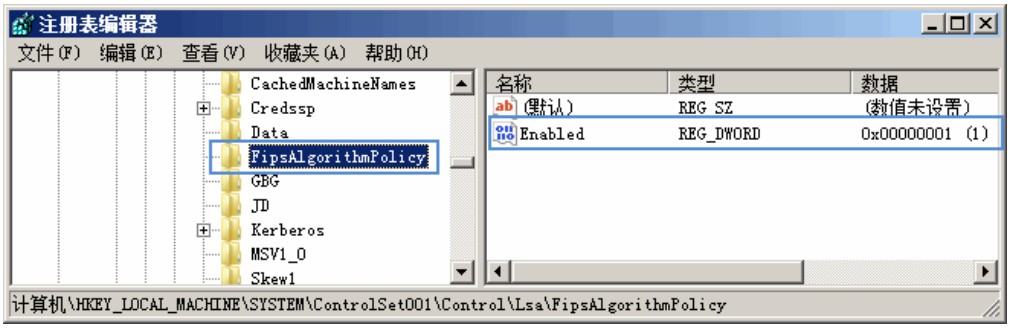
ii. 查找以下键并验证值。

- 键：**HKLM\System\CurrentControlSet\Control\Lsa\FIPSAlgorithmPolicy\Enabled**。

  该注册表值反映了当前的 FIPS 设置。如果启用了此设置，则该键的值为 1。如果禁用了此设置，则该键的值为 0。

- **值：1。**

iii.



提示: 有关其他信息，请参阅：

- http://technet.microsoft.com/en-us/library/cc750357.aspx
- http://support.microsoft.com/kb/811833

第 3 步：运行 SiteScopeHardeningToolRuntime

1. 将 SiteScope 安装包 **\Tools** 文件夹中的 **SiteScopeHardeningToolRuntime.zip** 文件复制到 SiteScope 服务器。
   a. 将该文件的内容提取到 **<SiteScope 根目录>\tools\SiteScopeHardeningTool** 文件夹。
   b. 通过运行以下命令行启动强化工具：
      <SiteScope 主目录>\tools\SiteScopeHardeningTool\runSSLConfiguration.bat

第 4 步：禁用 JMX 远程访问 SiteScope 服务器

使用强化工具禁用 JMX 远程访问 SiteScope 服务器：

1. 运行强化工具。有关详细信息，请参阅如何运行强化工具 (第 149 页)。
2. 选择选项“Configure JMX remote access”。
3. 按照工具中的说明禁用 JMX 远程访问。

提示: 只有退出强化工具后，配置中的变更才会生效。

第 5 步：配置 SSL

1. 通过运行以下命令行启动强化工具：
   <SiteScope 主目录>\tools\SiteScopeHardeningTool\runSSLConfiguration.bat
2. 输入 1 选择“SiteScope hardening configuration”选项。
3. 输入创建的备份文件使用的名称。如果需要禁用 FIPS 140-2 模式并恢复运行强化工具之前原有的 SiteScope 配置，则需要此备份。有关详细信息，请参阅禁用 FIPS 140-2 兼容模式 (第 142 页)。
4. 输入 2 选择“Configure SiteScope Standalone to work over SSL (https)”选项。
5. 输入 Y 确认您希望将 SiteScope 配置为在 SSL 上工作。
6. 输入 Y 确认是否要将 SiteScope 配置为与 FIPS 140-2 兼容。

7. 成功配置 FIPS 140-2 兼容模式后，请选择以下方法之一，以创建用于保存 SiteScope 服务器证书的 SiteScope 服务器密钥库：
   - **导入 .pkcs12 格式的服务器密钥库**

     工具将提示您选择一个别名，其中包含 SiteScope SSL 身份验证的密钥。

     备注: 如果稍后配置 SiteScope 和 SiteScope 公共 API 客户端进行客户端证书身份验证（请参阅将 SiteScope 配置为需要客户端证书身份验证 (第 133 页)），SiteScope 将使用此别名将密钥导出到 SiteScope API 的客户端信任库中。

     按照工具中的说明执行操作。

   - **通过对已认证证书颁发机构服务器上的请求进行签名，创建服务器密钥库。**

     选择此选项创建新密钥库并对签名证书的证书颁发机构生成密钥请求。生成的证书稍后将导入到密钥库中。

     工具将提示您输入服务器密钥库参数。对于“公用名称”，必须输入与计算机上所使用相同的 URL，如果使用了 FQDN，也应将其包括在内（例如 yourserver.domain.com）；对于别名，请输入您的计算机名（例如 yourserver）。

8. 复制已签名的 SiteScope 服务器证书，以创建由您的证书颁发机构签名的证书。
9. 输入从证书颁发机构服务器接收的已签名证书的完整路径。
10. 输入用于颁发以上证书的根 CA 证书的完整路径。
11. 键入 yes 以信任从证书颁发机构服务器接收的证书。此时证书即已添加到 SiteScope 服务器密钥库。

第 6 步：配置客户端身份验证

1. 输入用于客户端证书身份验证的 SiteScope 服务器信任库的密码。该密码必须至少包含 6 个字符，并且不应包含任何特殊字符。默认密码是 changeit。
2. 输入 Y 确认您希望启用客户端证书身份验证。

   启用客户端身份验证后，SiteScope 将在握手时执行完整的身份验证并提取客户端证书。SiteScope 用户管理 (LDAP) 系统将会对该客户端证书进行检查。有关详细信息，请参阅第 1 步：配置 LDAP 集成 (第 138 页)。
3. 在客户端证书的 AlternativeSubjectName 字段中输入客户端证书的用户名属性。默认用户名是 Other Name。
4. 输入 Y 确认您希望启用智能卡强制执行。

   如果启用智能卡强制执行，则 SiteScope 将验证客户端证书是否来源于硬件设备，然后将该证书添加到 SiteScope 信任库。

   有关智能卡强制执行的详细信息，请参阅配置智能卡身份验证 (第 132 页)。
5. 输入 Y 确认您想要将 CA 证书添加到 SiteScope 信任库。

   备注: 要使 SiteScope 信任客户端证书，SiteScope 必须信任颁发该客户端证书的证书颁发机构。要使 SiteScope 信任证书颁发机构，必须将该证书颁发机构的证书导入到 SiteScope 服务器信任库中。
6. 输入 CER 格式的 CA 根证书文件的完整路径。

7. 此时 CA 证书即已添加到 SiteScope 信任库。

   如果证书已存在于密钥库中，则会显示一条消息。键入 yes 确认您仍然想要将该证书添加到 SiteScope 信任库。
8. （可选）要向 SiteScope 服务器信任库添加其他 CA 证书，请输入 Y，然后重复第 1-3 步。

   备注: 无需其他 CA 证书。
9. 输入 Q 完成强化工具进程。

禁用 FIPS 140-2 兼容模式

如果启用了 FIPS 140-2 兼容模式，并且使用了安全连接，则无法使用强化工具中禁用 FIPS 的选项来禁用 FIPS 140-2 兼容模式。因此，必须恢复启用 FIPS 模式之前原有的 SiteScope 配置。

如果启用了 FIPS 140-2 兼容模式，并且使用的是非安全连接，则可以使用强化工具中禁用 FIPS 140-2 兼容模式的选项。

禁用安全连接的 FIPS 140-2 兼容模式

1. 通过运行以下命令行启动强化工具：

   <SiteScope 主目录>\tools\SiteScopeHardeningTool\runSSLConfiguration.bat
2. 输入 2 选择“Restore SiteScope configuration from backup”选项。
3. 输入可用备份列表中您希望恢复的备份配置的编号。
4. 输入 y 确认您希望恢复选定备份配置。
5. 输入 Q 完成强化工具进程。

禁用非安全连接的 FIPS 140-2 兼容模式

1. 通过运行以下命令行启动强化工具：

   <SiteScope 主目录>\tools\SiteScopeHardeningTool\runSSLConfiguration.bat
2. 输入 1 选择“SiteScope hardening configuration”选项。
3. 工具中出现提示时，选择“Configure FIPS 140-2 compliancy for a non-secure connection”选项。
4. 输入 2 禁用 FIPS 140-2 兼容模式。
5. 输入 y 确认您希望禁用 FIPS 140-2 兼容模式。
6. 输入 Q 完成强化工具进程。

疑难解答和限制

限制:

- 以 FIPS 140-2 模式运行 SiteScope 时，SSH 连接仅支持使用 SSH2。
- 当 SiteScope 以 FIPS 140-2 模式运行时，“URL 监控器”、“URL 工具”和“新建/编辑 HTTP 接收方”对话框中的“与 TLS 相比，首选 SSL”会被忽略（FIPS 140-2 模式下强制使用 TLS 进行身份验证）。

疑难解答：

- **问题：** 启用 FIPS 140-2 模式时，无法使用证书管理将证书从远程主机导入 SiteScope。

  解决方法： 通过 SiteScope 用户界面中的“证书管理”页面从文件导入证书，或者通过以下命令手动从文件导入证书：

```
keytool -import -file <信任证书文件> -alias <信任证书名称> -keypass <密码> -keystore <信任库文件 (SiteScope\java\lib\security\cacerts)>
-storepass <密码> -providername JsafeJCE –storetype PKCS12
```

第 21 章: 将 SiteScope 配置为使用自定义密钥加密数据

本章包括:

密钥管理概述

默认情况下，SiteScope 使用标准加密算法加密持久性数据（持久性数据包括所有已定义的监控器、组、警报和模板的配置数据，以及在 **<SiteScope 根>\persistency** 目录中找到的许多其他 SiteScope 实体）。

可以在强化工具中使用密钥管理数据加密选项来更改用于加密 SiteScope 持久性数据的加密密钥。与标准 SiteScope 加密相比，更改加密密钥提供了更强的加密性。

以下 SiteScope 工具支持使用密钥管理加密数据：强化工具、持久性查看器和持久性记录程序。也可以将密钥管理数据加密配置为在 SiteScope 处于 FIPS 140-2 兼容模式时运行。

当启用密钥管理时，将 SiteScope 配置为使用自定义密钥加密数据。要执行此操作，请输入 SiteScope 用于生成新密钥并加密持久性数据的密码短语。在从当前 SiteScope 导出 SiteScope 持久性数据以供稍后导入 SiteScope 时，必须输入此密码短语。在导入持久性数据（安装期间或使用 SiteScope 配置工具安装后）时，必须为 SiteScope 服务器密钥输入相同的密码短语。请注意，密钥不会保存到持久性数据。

- 如果计划启用或禁用 FIPS 140-2 兼容模式（请参阅将 SiteScope 配置为在 FIPS 140-2 兼容模式下运行 (第 137 页)），则必须在启用密钥管理数据加密之前执行此操作，否则将需要先禁用再重新启用密钥管理数据加密。
- 如果在更改用于加密 SiteScope 数据的加密密钥之后需要启用或禁用 FIPS 140-2 符合性模式，请按照如何在更改加密密钥之后启用或禁用 FIPS 兼容模式 (第 145 页)中描述的步骤操作。

疑难解答和限制

- 安装在 Linux 平台上的 SiteScope 不支持密钥管理数据加密。
- 当使用 SiteScope 故障转移为主 SiteScope 提供备份基础结构监控时，不支持密钥管理数据加密（在主 SiteScope 和 SiteScope 故障转移服务器上都不支持）。如果将 SiteScope 故障转移与使用默认密钥加密的 SiteScope 结合使用，然后使用强化工具将 SiteScope 转换到密钥管理数据加密，则在镜像配置时 **high_availability.log** 中将出现 UNEXPECTED_SHUTDOWN 错误。

如何将 SiteScope 配置为使用自定义密钥加密数据

使用密钥管理，您可以管理和更改用于加密 SiteScope 配置数据（持久性）的加密密钥。

备注: 如果计划以 FIPS 140-2 兼容模式使用 SiteScope（请参阅FIPS 140-2 符合性概述 (第 137 页)），则必须在更改加密密钥之前配置 FIPS 兼容模式，否则将需要先禁用再重新启用密钥管理数据加密。如果在自定义加密密钥后需要更改 FIPS 模式，请按照如何在更改加密密钥之后启用或禁用 FIPS 兼容模式 (第 145 页)中描述的步骤操作。

1. 安装 SiteScope。

   有关详细信息，请参阅安装工作流 (第 72 页)。
2. 启动 SiteScope（以便生成 SiteScope 持久性数据）。
3. 停止 SiteScope。
4. 运行强化工具。
   a. 工具提示时，请选择选项“Enable or re-encrypt key management data encryption”。
   b. 输入 1 使用自定义密钥加密或重新加密持久性数据。与标准 SiteScope 加密相比，更改用于加密配置的加密密钥提供了更强的加密性。

      要将持久性数据恢复为标准密钥加密，请输入 2。
   c. 确认要使用自定义密钥加密或重新加密持久性数据。
   d. 输入用于自定义密钥的新密码短语（此密码短语不是已使用中的密码短语，而是用于新的加密迭代）。密码短语不能包含空格或转义字符。

      SiteScope 生成新密钥，并用其加密持久性数据。

      备注: 当使用 SiteScope 配置向导或 SiteScope 配置工具导出或导入使用此自定义密钥加密的 SiteScope 配置数据时，必须输入此密码短语。请注意，密码短语不随 zip 文件存储在已导出的配置中。
5. 启动 SiteScope。

如何在更改加密密钥之后启用或禁用 FIPS 兼容模式

如果要在更改用于加密数据的 SiteScope 服务器密钥之后启用或禁用 FIPS 140-2 兼容模式，则必须执行以下操作：

备注: 不按下表所列顺序执行步骤可能导致 SiteScope 数据丢失。

1. 禁用密钥管理数据加密（请参阅如何将 SiteScope 配置为使用自定义密钥加密数据 (第 145 页)的步骤 4，然后输入 2 恢复标准加密）。
2. 启用/禁用 FIPS 140-2 兼容模式。有关详细信息，请参阅启用 FIPS 140-2 兼容模式 (第 138 页)。
3. 启用密钥管理数据加密（从如何将 SiteScope 配置为使用自定义密钥加密数据 (第 145 页)的步骤 4 继续，然后输入 1 使用自定义密钥加密持久性数据）。

如何在使用自定义密钥加密数据时导出和导入配置数据

当 SiteScope 配置为使用密钥管理加密数据时，请输入 SiteScope 用于生成新密钥的密码短语。SiteScope 将使用此密钥来加密持久性数据。之后将此加密数据导出或导入 SiteScope 时，必须为 SiteScope 服务器密钥输入相同的密码短语。

1. 从当前 SiteScope 导出 SiteScope 配置数据，以便稍后导入 SiteScope。
   - 使用 SiteScope 配置工具时，请执行以下操作：
     i. 在“导出配置”屏幕中，在“密码短语”框中输入用于 SiteScope 服务器密钥库的密码短语。使用默认 SiteScope 加密时，此框处于禁用状态。
     ii. 单击“下一步”完成导出操作。将使用自定义密钥加密并导出配置数据。

     备注: 使用默认 SiteScope 加密时，这些输入字段处于禁用状态。

   - 当以控制台模式运行配置工具时，要使用配置工具，请执行以下操作：在“导出配置”屏幕中，出现提示时输入用于 SiteScope 服务器密钥库的密码短语，然后按 Enter 完成导出操作。
   - 当使用静默模式时：在 **ovinstallparams.ini** 文件的相关部分输入密钥管理数据加密密码短语。
2. 导入 SiteScope 配置数据。
   - 用户界面（使用 SiteScope 配置向导安装期间，或使用 SiteScope 配置工具安装后）：
     i. 在“导入配置”屏幕中，输入要导入的用户数据 (zip) 文件的名称，或输入要从中导入用户数据文件的 SiteScope 安装目录。
     ii. 在“密码短语”框中，输入用于 SiteScope 服务器密钥库的密码短语。在“匹配密码短语”框中输入相同密码短语，确认此密码短语。

     备注: 使用默认 SiteScope 加密时，这些框处于禁用状态。

     iii. 单击“下一步”完成导入操作。
   - 控制台模式（安装期间或使用配置工具安装后）：在“导入配置”屏幕中，出现提示时输入用于 SiteScope 服务器密钥的密码短语，然后按 Enter 完成导入操作。
   - 静默安装：在 **ovinstallparams.ini** 文件的相关部分输入用于数据加密的自定义密钥的密码短语。

   将使用自定义密钥加密已导入的配置数据。

第 22 章: 将 SiteScope 配置为通过安全连接与 BSM 通信

本章包括:

将 SiteScope 配置为连接到需要安全连接的 BSM 服务器

要将 SiteScope 配置为连接到需要安全连接的 BSM 服务器，必须在 SiteScope 和 BSM 之间建立信任关系以启用安全通信。这意味着 SiteScope 必须信任颁发 BSM 服务器证书的证书颁发机构。要使 SiteScope 信任证书颁发机构，必须将该证书颁发机构的证书存储到 SiteScope 服务器信任库和主信任库中。有关详细信息，请参阅将证书颁发机构证书导入 SiteScope 信任库 (第 134 页)。

将 SiteScope 配置为连接到需要客户端证书的 BSM 服务器

可以将 SiteScope 配置为连接到需要客户端证书的 BSM 服务器。为此，需要将 BSM 服务器证书导入到 SiteScope 密钥库中。

我们建议使用强化工具执行此操作。有关详细信息，请参阅如何使用强化工具将 SiteScope 配置为连接到需要客户端证书的 BSM 服务器 (第 153 页)。

还可以使用将 SiteScope 配置为连接到需要客户端证书的 BSM 服务器 (第 189 页)中的手动步骤完成此操作。

将 BSM 配置为在 SiteScope 需要客户端证书时连接到 SiteScope

在 BSM 中，在网关服务器和数据处理服务器上执行以下步骤:

1. 将文件 **<SiteScope 主目录>\templates.certificates\BSMClientKeystore** 从 SiteScope 计算机文件复制到 BSM 计算机上的任意文件夹中。
2. 停止 BSM。
3. 编辑 **<HP BSM 根目录>\EjbContainer\bin\product_run.bat** 并添加以下内容:

```
set SECURITY_OPTS=-Djavax.net.ssl.keyStore=FULL_PATH_TO_COPIED_BSMClientKeyStore_
File -Djavax.net.ssl.keyStorePassword=PASSWORD_FOR_BSMClientKeyStore_File -
Djavax.net.ssl.keyStoreType=JKS

set JAVA_OPTS=%JAVA_OPTS% %SECURITY_OPTS%
```

其中 FULL_PATH_TO_COPIED_BSMClientKeyStore_File **是密钥库路径，** PASSWORD_FOR_BSMClientKeyStore_File **是密钥库密码。**

4. **重新启动 BSM。**
5. **在 系统可用性管理 (SAM) 管理中配置 BSM 和 SiteScope。**
6. **将“SAM 管理”>“新建/编辑 SiteScope”>“分布式设置”中的“网关服务器名称/IP 地址”属性更改为安全反向代理的完全限定域名 (FQDN)。**

第 23 章: 使用强化工具

强化工具是一种命令行工具，可使用该工具配置 SiteScope 以执行 SiteScope 的全部或部分强化操作。

备注: 每次运行此工具时，都会对现有 SiteScope 配置执行完整备份，以便您可以回滚到备份的配置。有关详细信息，请参阅如何使用强化工具恢复备份的配置 (第 155 页)。

可以使用强化工具执行以下任务:

如何运行强化工具

本主题描述如何打开和运行强化工具。要执行本章主题中描述的其他任务，必须先执行本主题中的步骤。

1. 如果要启用 LDAP 用户身份验证（仅在计划使用客户端证书登录 SiteScope 时才需要），请先配置 LDAP 集成，然后再运行此工具:
   a. 在 SiteScope 上配置 LDAP 服务器。有关详细信息，请参阅 SiteScope 帮助中《使用 SiteScope》指南的“如何将 SiteScope 设置为使用 LDAP 身份验证”。
   b. 在 SiteScope 用户管理中为 LDAP 用户创建新角色。
   c. 将 SiteScope 管理员登录名更改为 LDAP 中的用户电子邮件地址。不要输入密码。
2. 停止 SiteScope 服务:

   Windows:

   - 如果要从 **go.bat** 运行 SiteScope，请关闭命令行终端或按 **CTRL+C**。
   - 如果要将 SiteScope 作为服务运行，请执行以下操作:
     i. 在 Windows 资源管理器中，搜索“服务”。此时将打开“组件服务”窗口。
     ii. 在左窗格中，选择“服务(本地)”。
     iii. 在中心窗格的服务列表中，选择“HP SiteScope”。
     iv. 在服务列表的左侧区域中，单击“停止服务”。

Linux:

运行以下命令行:

```
cd /opt/HP/SiteScope/
./stop
```

警告: 不要在 SiteScope 运行时运行强化工具。

3. 通过运行以下命令行启动此工具:

   Windows:

   <SiteScope 主目录>\tools\SiteScopeHardeningTool\runSSLConfiguration.bat

   Linux:

   ./opt/HP/SiteScope/tools/SiteScopeHardeningTool/runSSLConfiguration.sh

   此时将打开强化工具。
4. 工具提示时，请选择选项“SiteScope hardening configuration”。此时将自动备份现有的 SiteScope 配置。
5. 系统提示时，请输入将来恢复该备份时易于识别的备份描述。要恢复备份的配置，请参阅如何使用强化工具恢复备份的配置 (第 155 页)。

   备注: 使用强化工具时，将覆盖 **/opt/HP/SiteScope/Tomcat/conf** 目录中的 Tomcat 配置文件 **server.xml**，并将删除在运行该工具之前对该文件所做的任何修改。要恢复这些修改，必须在运行工具之后重新将修改应用到此文件。
6. 选择工具中列出的一个任务或任务组合。

   有关使用强化工具执行配置任务的详细信息，请参阅本章中的其他主题。

备注: 只有退出强化工具后，配置中的变更才会生效。

如何使用强化工具将 SiteScope 配置为需要安全连接

备注: 如果您计划允许 SiteScope 在 FIPS 140-2 兼容模式下运行，请按照启用 FIPS 140-2 兼容模式 (第 138 页)中的步骤执行操作。

可以使用强化工具将 SiteScope 配置为需要安全连接 (https)。

1. 运行强化工具。有关详细信息，请参阅如何运行强化工具 (第 149 页)。
2. 工具提示时，请选择选项“Configure SiteScope Standalone to work over SSL (https)”。

   或者，如果要执行工具中可用的所有强化配置任务，请选择选项“Full SiteScope hardening configuration (all of the configuration options)”。
3. 确认将 SiteScope 配置为通过 SSL 运行。
4. 确认是否要将 SiteScope 配置为与 FIPS 140-2 兼容。有关详细信息，请参阅启用 FIPS 140-2 兼容模式 (第 138 页)。
5. 选择以下方法之一创建用于保存 SiteScope 服务器证书的 SiteScope 服务器密钥库:

- **导入 .jks 格式的服务器密钥库。**

  工具将提示您选择一个别名，其中包含 SiteScope SSL 身份验证的密钥。

  备注: 如果稍后配置 SiteScope 和 SiteScope 公共 API 客户端进行客户端证书身份验证（请参阅将 SiteScope 配置为需要客户端证书身份验证 (第 133 页)），SiteScope 将使用此别名将密钥导出到 SiteScope API 的客户端信任库中。

  按照工具中的说明执行操作。

- **通过对已认证证书颁发机构服务器上的请求进行签名，创建服务器密钥库。**

  选择此选项创建新密钥库并对签名证书的证书颁发机构生成密钥请求。生成的证书稍后将导入到密钥库中。

  工具将提示您输入服务器密钥库参数。我们建议，对于公用名称，请输入计算机的 URL（例如 yourserver.domain.com），对于别名，请输入计算机名称（例如 yourserver）。

- **从 .pfx 格式的服务器证书导入服务器密钥库。**

  选择此选项从 **.pfx** 格式的证书创建密钥库。此证书必须包含其私钥。

  每次创建密钥库时，强化工具都将自动确认密钥库密码和私钥是否相同。

6. 输入客户端证书的用户名属性。默认用户名是 Other Name。

   服务器证书将导入到服务器密钥库中。工具中将显示该证书别名。
7. 确认是否要启用 SiteScope 客户端身份验证。

   如果启用客户端 TLS 身份验证，则 SiteScope 将在 TLS 握手时执行完整客户端 TLS 身份验证并提取客户端证书。将对照 SiteScope 用户管理系统检查此客户端证书。
8. 确认是否要启用智能卡强制执行。

   如果启用智能卡强制执行，则 SiteScope 将验证客户端证书是否来源于硬件设备。有关智能卡强制执行的详细信息，请参阅配置智能卡身份验证 (第 132 页)。
9. 输入 SiteScope 服务器信任库的密码。默认密码是 changeit。

   要使 SiteScope 信任客户端证书，SiteScope 必须信任颁发该客户端证书的证书颁发机构。要使 SiteScope 信任证书颁发机构，必须将该证书颁发机构的证书存储到 SiteScope 服务器信任库和主信任库中。要将证书颁发机构证书导入到 SiteScope 信任库，请参阅如何使用强化工具将证书颁发机构证书导入到 SiteScope 信任库中 (第 152 页)。
10. 输入 Q 完成强化工具进程。

如何使用强化工具将 SiteScope 配置为验证证书吊销

可以使用强化工具将 SiteScope 配置为验证客户端证书是否已被吊销，方法如下:

- **证书吊销列表 (CRL)**

  支持您通过 CRL 列表验证客户端证书是否已被吊销。CRL 列表的 URL 位于客户端证书属性中。将此列表下载到本地服务器中。系统将提示您输入 CRL 列表在本地服务器上缓存的生存时间。

  下表描述了 CRL 的生存时间:

CRL 值	描述
-1	CRL 将在本地缓存，且仅在服务器上有变更时重新加载。这是建议值，使用此值可获得更好的性能。
0	每次验证请求时重新加载 CRL。
⩾ 1	CRL 的生存时间只有几秒钟。时间到期后，将重新加载 CRL。

- **联机证书状态协议 (OCSP)**

  支持您通过与远程服务器的连接验证客户端证书是否已被吊销。SiteScope 将客户端证书的序列号传输到远程服务器并等待响应。默认 OCSP 响应程序的 URL 位于客户端证书属性中，但您可以覆盖该 URL。

可以通过 CRL 或 CRL 和 OCSP 的组合验证客户端证书是否已被吊销。

要验证客户端证书是否已被吊销，请执行以下操作：

1. 运行强化工具。有关详细信息，请参阅如何运行强化工具 (第 149 页)。
2. 选择选项“Configure SiteScope SSL certificate revocation verification via CRL and OCSP”。
3. 按照工具中的说明执行操作。

   工具将提示您激活转发 HTTP 代理服务器。

   如果激活转发 HTTP 代理服务器，则所有证书吊销请求都将通过代理服务器重定向到 CRL 和 OCSP URL。

   如有需要，还可以将 SiteScope 配置为符合美国联邦信息处理标准 (FIPS) 出版物 140-2 的要求。有关详细信息，请参阅将 SiteScope 配置为在 FIPS 140-2 兼容模式下运行 (第 137 页)。

   只有退出强化工具后，配置中的变更才会生效。

如何使用强化工具将证书颁发机构证书导入到 SiteScope 信任库中

有关将证书颁发机构证书导入到 SiteScope 信任库中的详细信息，请参阅将证书颁发机构证书导入 SiteScope 信任库 (第 134 页)。

要将证书颁发机构证书导入到 SiteScope 信任库，请执行以下操作：

1. 先决条件（如果将 SiteScope 配置为需要安全连接）

   在将证书颁发机构证书导入到 SiteScope 信任库之前，必须通过将 SiteScope 服务器证书导入 SiteScope 服务器密钥库，将 SiteScope 配置为通过 TLS 运行。有关详细信息，请参阅如何使用强化工具将 SiteScope 配置为需要安全连接 (第 150 页)。
2. 运行强化工具。有关详细信息，请参阅如何运行强化工具 (第 149 页)。
3. 工具提示时，请选择选项“Import CA certificates into SiteScope main and server trustStores”。
4. 按照工具中的说明执行操作。

提示：

- 此工具仅接受常规 Windows 格式的文件路径。在 UNIX 格式中，如果文件路径中有空格，则会在空格前添加反斜线（ “\” ）表示后跟空格，应删除该反斜线。

格式	文件路径
Windows	**/user/temp dir/certificate.cer**
UNIX	**/user/temp\ dir/certificate.cer** 更改为: **/user/temp dir/certificate.cer**

- 只有退出强化工具后，配置中的变更才会生效。

如何使用强化工具将 SiteScope 配置为连接到需要客户端证书的 BSM 服务器

使用强化工具为 BSM 集成配置客户端 TLS 身份验证。使用此工具，您可以将 SiteScope 配置为允许 BSM 与 SiteScope 集成。还可以使用此工具将 SiteScope 故障转移配置为使用 TLS 客户端证书身份验证。在这两种情况下，都必须按照下面描述的步骤执行操作。

备注: 为 BSM 集成配置 TLS 客户端身份验证之前，必须通过将 SiteScope 服务器证书导入到 SiteScope 服务器密钥库，将 SiteScope 配置为通过 TLS 运行。有关详细信息，请参阅如何使用强化工具将 SiteScope 配置为需要安全连接 (第 150 页)。

如果您尚未执行此操作，强化工具将提示您执行完整的 SiteScope 强化配置。

要为 BSM 集成配置 TLS 客户端身份验证，请执行以下操作:

1. 运行强化工具。有关详细信息，请参阅使用强化工具 (第 149 页)。
2. 选择选项“Configure SiteScope client certificate authentication for BSM Integration”。
3. 按照工具中的说明执行操作。
   a. 系统提示时，输入颁发 BSM 服务器证书的证书颁发机构所颁发的 **.cer** 格式的证书的完整路径。BSM 服务器证书将导入到 SiteScope 信任库中。
   b. 系统提示时，请确认信任该 BSM 服务器证书。该 BSM 服务器证书将导入到密钥库中。
   c. 系统提示时，请选择以下方法之一创建用于保存 SiteScope 服务器证书的 SiteScope 服务器密钥库:
      - **导入 .jks 格式的服务器密钥库。**

        工具将提示您选择一个别名，其中包含 SiteScope TLS 身份验证的密钥。

        备注: 如果稍后配置 SiteScope 和 SiteScope 公共 API 客户端进行客户端证书身份验证（请参阅将 SiteScope 配置为需要客户端证书身份验证 (第 133 页)），SiteScope 将使用此别名将密钥导出到 SiteScope API 的客户端信任库中。

      - **通过对已认证证书颁发机构服务器上的请求进行签名，创建服务器密钥库。**

        选择此选项创建新密钥库并对签名证书的证书颁发机构生成密钥请求。生成的证书稍后将导入到密钥库中。

工具将提示您输入服务器密钥库参数。我们建议，对于公用名称，请输入计算机的 URL（例如 anyserver.domain.com），对于别名，请输入计算机名称（例如 anyserver）。

- **从 .pfx 格式的服务器证书导入服务器密钥库。**

  选择此选项从 **.pfx** 格式的证书创建密钥库。此证书必须包含其私钥。

  每次创建密钥库时，强化工具都将自动确认密钥库密码和私钥是否相同。

d. 系统提示时，请输入用于 BSM 身份验证的客户端密钥库的密码。SiteScope 将创建 BSM 客户端证书密钥库。

e. 系统提示时，请输入搜寻代理 **TrustStore MAMTrustStoreExp.jks** 的密码。默认密码是 logomania。我们强烈建议不要更改此默认密码。

   配置过程中，SiteScope 会自动将 BSM 服务器证书导入到 SiteScope 信任库中。

f. 系统提示时，请确认信任该 BSM 服务器证书。

   该 BSM 服务器证书将导入到 SiteScope 密钥库中。

提示：

- 此工具仅接受常规 Windows 格式的文件路径。在 UNIX 格式中，如果文件路径中有空格，则会在空格前添加反斜线（“\”）表示后跟空格，应删除该反斜线。

格式	文件路径
Windows	**/user/temp dir/certificate.cer**
UNIX	**/user/temp\ dir/certificate.cer** 更改为： **/user/temp dir/certificate.cer**

- 只有退出强化工具后，配置中的变更才会生效。

如何使用强化工具启用 FIPS 140-2 兼容模式

可以使用强化工具将 SiteScope 配置为与 FIPS 140-2 兼容。FIPS 140-2 是一个由美国国家标准与技术研究院 (NIST) 管理的密码模块验证计划，其指定了密码模块的安全要求。

有关详细信息，请参阅启用 FIPS 140-2 兼容模式 (第 138 页)。

如何使用强化工具启用密钥管理数据加密

可以在强化工具中使用密钥管理来更改用于加密 SiteScope 中的持久性数据的加密密钥。这种加密方法比 SiteScope 中使用的标准方法更强。

有关详细信息，请参阅如何将 SiteScope 配置为使用自定义密钥加密数据 (第 145 页)。

如何使用强化工具配置 SiteScope 和 SiteScope 公共 API 客户端证书身份验证

使用强化工具配置 SiteScope 和 SiteScope 公共 API 客户端进行客户端证书身份验证，步骤如下：

1. 运行强化工具。有关详细信息，请参阅如何运行强化工具 (第 149 页)。
2. 选择选项“Configure SiteScope and SiteScope public API client for client certificate authentication”。
3. 按照工具中的说明执行操作。

提示：

- 如果为 SiteScope 公共 API 启用 LDAP 用户身份验证，则从 API 客户端证书提取的用户名通过 LDAP 服务器进行身份验证。
- 系统提示将客户端证书签名机构添加到 SiteScope 服务器信任库中后，该证书将导入到 SiteScope 服务器信任库和主信任库中。创建的 API 配置文件将放置在 **API_Configuration** 目录的脚本目录下。
- 此工具仅接受常规 Windows 格式的文件路径。在 UNIX 格式中，如果文件路径中有空格，则会在空格前添加反斜线（“\”）表示后跟空格，应删除该反斜线。

格式	文件路径
Windows	**/user/temp dir/certificate.cer**
UNIX	**/user/temp\ dir/certificate.cer** 更改为： **/user/temp dir/certificate.cer**

- 只有退出强化工具后，配置中的变更才会生效。

如何使用强化工具配置 JMX 远程访问

可以使用强化工具启用或禁用对 SiteScope 服务器的 JMX 远程访问，步骤如下：

1. 运行强化工具。有关详细信息，请参阅如何运行强化工具 (第 149 页)。
2. 选择选项“Configure JMX remote access”。
3. 按照工具中的说明执行操作。

提示: 只有退出强化工具后，配置中的变更才会生效。

如何使用强化工具恢复备份的配置

运行强化工具时，将自动备份现有的 SiteScope 配置。可以使用强化工具恢复备份的配置，步骤如下：

1. 运行强化工具。有关详细信息，请参阅如何运行强化工具 (第 149 页)。
2. 选择选项“Restore SiteScope configuration from backup”。
3. 按照工具中的说明执行操作。

提示:

- 备份名称包含备份的时间和日期。
- 只有退出强化工具后，配置中的变更才会生效。

强化工具限制/疑难解答

本节描述有关使用强化工具的疑难解答和限制。

限制

如果 SiteScope 安装在非英语操作系统中，则无法使用强化工具将 SiteScope 配置为使用 TLS。在这种情况下，可使用《HP SiteScope 部署指南》的附录部分中所述的手动步骤。

疑难解答

- **强化工具不接受 UNIX 格式的文件路径。**

  原因: 此工具仅接受常规 Windows 格式的文件路径。

  解决方案: 在 UNIX 格式中，如果文件路径中有空格，则会在空格前添加反斜线（ “\” ）表示后跟空格，应删除该反斜线。

格式	文件路径
Windows	**/user/temp dir/certificate.cer**
UNIX	**/user/temp\ dir/certificate.cer** 更改为: **/user/temp dir/certificate.cer**

- **退出工具时，显示错误消息，通知用户复制到文件时出现错误。**

  原因: 当配置工具找不到某个创建的配置文件时，会出现这种错误。如果不是从命令行运行此工具，就会出现这种情况。在这种情况下，创建的文件不会放置在配置工具目录中。

  解决方案:

  a. 在配置工具目录中，删除创建的所有库（例如，**API_Configuration**、**tmp_<数字>**、**BSM_Int** ）。
  b. 打开命令行终端。
  c. 通过命令行转到配置工具目录。
  d. 从命令行运行配置工具。有关详细信息，请参阅使用强化工具 (第 149 页)。

- **配置 SiteScope 身份验证后，在通过 Web 浏览器访问 SiteScope 时，SiteScope 将不提**

供身份验证证书选项，导致登录失败。

原因： SiteScope 信任库不包含证书签名机构的证书（CA 证书）。这会导致 SiteScope 不对这些证书签名机构签名的客户端证书发起请求。

解决方案： 将 CA 证书导入 SiteScope 主信任库和服务器信任库，并添加所需的 CA 证书。有关详细信息，请参阅将证书颁发机构证书导入 SiteScope 信任库 (第 134 页)。

- **SiteScope 公共 API 调用退出，错误为 NumberFormatException。**

  原因： 执行 API 调用时 –useSSL 参数设置为 false。

  解决方案： 在 –useSSL 参数设置为 true 时运行 API 调用。

- **SiteScope 公共 API 调用退出，错误为 ConnectException:Connection refused。**

  原因： API 调用尝试连接的端口不是 TLS 端口。

  解决方案： 将 –port参数设置为 TLS 身份验证端口 8443。

- **SiteScope 公共 API 调用失败，错误为 (500) 内部服务器错误。**

  原因： –login 参数未设置为正确的 TLS 用户名。

  解决方案： 将 –login 参数设置为 SITESCOPE_CERTIFICATE_AUTHENTICATED_USER。

- **尝试通过浏览器访问 SiteScope 时，SiteScope 显示以下消息：“The user is not valid SiteScope user.Please contact SiteScope administrator”。**

  原因： 配置 SiteScope 使用 TLS 身份验证时启用了客户端 TLS 身份验证和智能卡强制执行，但未在 SiteScope 用户管理中设置 LDAP 服务器。

  解决方案 1：

  a. 运行强化工具。

  > **备注:** 如果打算仅使用客户端证书登录 SiteScope，则在执行强化步骤之前，必须首先在 SiteScope 上配置 LDAP 服务器。强化 SiteScope 后，将从客户端证书提取用于登录的用户名，并对照 LDAP 服务器进行检查，然后将以下属性添加到 **<SiteScope 根目录>\groups\master.config** 文件中（不要修改这些属性）：
  >
  > - **_clientCertificateAuthIdentityPropertyName**。指示 SiteScope 在客户端证书属性中找到用于连接的用户名。
  > - **_clientCertificateAuthIsAPIRealLDAPUserRequired**。指示 SiteScope 在调用 SiteScope API 时，应通过 LDAP 完成用户名身份验证。
  > - **_clientCertificateAuthUsernamePropertyNameInSubjectField**。可在客户端证书中找到的用于 API 调用的用户名的属性。

  b. 恢复运行工具之前备份的 SiteScope 配置（有关详细信息，请参阅恢复已备份的配置 (第 135 页)）。

  c. 配置 LDAP 服务器。

  d. 再次运行强化工具。

  解决方案 2：

  a. 打开 **<SiteScope 根目录>\groups** 中的 **master.config** 文件，然后将以下属性值更改为 false：
  - _clientCertificateAuthEnabled
  - _clientCertificateAuthIsAPIRealLDAPUserRequired
  - _clientCertificateAuthSmartCardEnforcementEnabled

  b. 重新启动 SiteScope。

c. 配置 LDAP 服务器。
d. 打开 **master.config** 文件。
e. 将上述属性更改为其原始值。
f. 重新启动 SiteScope。

第 24 章: 配置符合 USGCB (FDCC) 的桌面

美国政府配置基准 (USGCB) 原称联邦桌面核心配置 (FDCC)，是一项旨在为改善并维持以安全性为重点的高效配置设置提供指导的桌面配置标准。

SiteScope 通过了符合 USGCB (FDCC) 客户端的认证。要启用这项符合性，必须将 SiteScope URL 添加到可信站点安全区域和弹出窗口允许列表中。此外，还建议允许文件下载。

有关 USGCB (FDCC) 的详细信息，请参阅:

- http://usgcb.nist.gov/usgcb/microsoft_content.html
- http://nvd.nist.gov/fdcc/index.cfm

先决条件:

安装客户端系统要求 (第 54 页)中列出的 SiteScope 支持的最新 JRE 版本。

如何在 Windows 7 中启用组策略编辑器 (gpedit.msc):

1. 将 SiteScope URL 添加到“可信站点”安全区域:
   a. 通过运行以下命令打开组策略编辑器: run gpedit.msc。
   b. 导航到: “计算机配置”>“管理模板”>“Windows 组件”>“Internet Explorer”>“Internet 控制面板”>“安全页”:
      i. 在右侧的设置面板中，双击“站点到区域分配列表”，选择“已启用”选项，然后单击“显示”。在“显示内容”对话框中，单击“添加”。
      ii. 在“输入要添加的项目的名称”框中，输入 SiteScope 服务器的名称。例如，http://MySiteScope.com。如果要通过 HTTPS 使用 SiteScope，则输入 https://MySiteScope.com。
      iii. 在“输入要添加的项目的值”框中，输入表示区域类型的数值:

值	区域类型	描述
1	Intranet 区域	本地网络上的站点
2	受信任的站点区域	添加到可信站点中的站点
3	Internet 区域	Internet 上的站点
4	受限制站点区域	专门添加到受限制站点中的站点

2. 将 SiteScope URL 添加到弹出窗口允许列表。
   a. 通过运行以下命令打开组策略编辑器: run gpedit.msc。
   b. 导航到: “计算机配置”>“管理模板”>“Windows 组件”>“Internet Explorer”:
      i. 在右侧的设置面板中，双击“弹出窗口允许列表”，选择“已启用”选项，然后单击“显示”。在“显示内容”对话框中，单击“添加”。
      ii. 在“输入要添加的项目的名称”框中，输入 SiteScope 服务器的名称。例如，http://MySiteScope.com。如果要通过 HTTPS 使用 SiteScope，则输入 https://MySiteScope.com。
3. 允许文件下载（可选，用于日志抓取程序和发行说明）。

a. 通过运行以下命令打开组策略编辑器：run gpedit.msc。

b. 导航到：“计算机配置”>“管理模板”>“Windows 组件”>“Internet Explorer”>“安全功能”>“限制文件下载”，然后在右侧的设置面板中，双击“Internet Explorer 进程”，选择“已禁用”选项。

第 5 部分: 开始使用和访问 SiteScope

第 25 章: 安装之后的管理任务

本章包括建议在安装 SiteScope 之后执行的步骤。

✓	步骤
	注册以获取 SiteScope 支持。有关详细信息，请参阅入门指导 (第 31 页)。
	为了改进 SiteScope 的扩展性和性能，我们建议安装 Microsoft 修补程序。有关详细信息，请参阅安装 Microsoft 修补程序 (第 164 页)。
	如果要从较早版本的 SiteScope 升级，请使用配置工具将监控器和组配置数据从较早的 SiteScope 安装传输到新安装。有关使用配置工具的详细信息，请参阅使用 SiteScope 配置工具 (第 107 页)。
	使用 Web 浏览器登录 SiteScope Web 界面。有关详细信息，请参阅连接到 SiteScope (第 166 页)。
	新安装可自动激活社区许可证，社区许可证支持无限期使用 SiteScope 的部分功能。如果要将 SiteScope 版本升级到提供 SiteScope 全部功能的版本，可在安装期间或安装后在“常规首选项”页面输入 SiteScope 许可证信息，如 SiteScope 帮助中《使用 SiteScope》的“常规首选项”部分所述。有关许可证的详细信息，请参阅SiteScope 许可证 (第 21 页)。
	创建 SiteScope 管理员帐户的用户名和密码。该帐户是产品安装后的默认活动帐户。该帐户拥有 SiteScope 的全部管理权限，同时也是访问此产品的所有用户使用的帐户，除非您对其进行了限制。 可以根据组织的需求创建和配置其他用户帐户。有关详细信息，请参阅 SiteScope 帮助中《使用 SiteScope》的“用户管理首选项”部分。如果没有为管理员用户定义用户名和密码，则 SiteScope 会跳过登录页并自动登录。
	使用管理员电子邮件地址来配置 SiteScope 电子邮件首选项电子邮件服务器，并指定 SiteScope 可用于向用户转发电子邮件和警报的邮件服务器。有关详细信息，请参阅 SiteScope 帮助中《使用 SiteScope》的“电子邮件首选项”部分。
	配置要监控的远程服务器的连接配置文件。根据安全要求指定要使用的连接方法。有关详细信息，请参阅 SiteScope 帮助中《使用 SiteScope》的“远程服务器”部分。
	必要时，可调整“日志首选项”以设置监控器数据在 SiteScope 服务器上保留的时间（以天为单位）。默认情况下，SiteScope 会删除早于 40 天的日志。如果计划将监控器数据导出到外部数据库，则需准备好数据库、必需的驱动程序，并适当配置“日志首选项”。有关详细信息，请参阅 SiteScope 帮助中《使用 SiteScope》的“日志首选项”部分。
	为需要驱动程序的监控器安装中间件驱动程序，以便与远程数据库和应用程序建立连接。

✓	步骤
	使用 SiteScope 作为 Business Service Management (BSM) 的数据收集器时，需要配置 BSM 集成。有关详细信息，请参阅 SiteScope 帮助中《使用 SiteScope》的“使用 BSM”部分。
	使用 SiteScope 在 HP Operations Manager (HPOM) 或 BSM 的操作管理中发送事件或报告度量时，需要配置 HP Operations Manager 集成。有关详细信息，请参阅 HP 软件集成网站中的“将 SiteScope 与 HP Operations Manager 产品集成”： • HPOM for Windows: http://support.openview.hp.com/sc/solutions/integrations.jsp?intid=39 • HPOM for UNIX: http://support.openview.hp.com/sc/solutions/integrations.jsp?intid=628
	根据业务系统基础架构评估中确定的要求和限制，概述组并监控组织。
	创建和开发模板，以使用标准化组结构、命名约定和配置设置加快监控部署速度。有关详细信息，请参阅 SiteScope 帮助中《使用 SiteScope》的“用户定义模板和解决方案模板”部分。
	在组和关键监控器之间建立相关性，以便更好地控制冗余警报。有关详细信息，请参阅 SiteScope 帮助中《使用 SiteScope》的“使用 SiteScope 组”部分。
	向业务利益相关者和系统管理员推广 SiteScope。

SiteScope 系统使用已定义的用户和传入的监控数据启动并运行后，需要培训业务和系统用户，指导他们如何访问并使用 SiteScope 报告和警报功能。

第 26 章: 安装 Microsoft 修补程序

为了提升 SiteScope 的扩展性和性能，建议在安装 SiteScope 后安装以下 Microsoft 修补程序:

修补程序下载	描述
http://support.microsoft.com/kb/2847018 http://support.microsoft.com/kb/2775511	在 SiteScope 服务器上安装最新的 Microsoft mrxsmb.sys 和 mrxsmb10.sys 或 mrxsmb20.sys 修补程序文件以防止针对同一主机运行多个基于 perfex 的监控器时出现性能问题和监控器跳过。
http://support.microsoft.com/?scid=kb;en-us;942589	安装该 Microsoft 修补程序以在 64 位版本的 Windows 2003、Windows 2008 或 Windows XP 上运行 Microsoft Exchange（因为 32 位应用程序无法在运行 64 位版本的 Windows Server 2003 或 2008 的计算机上访问 system32 文件夹）。
http://support.microsoft.com/kb/961435	在目标 Windows 系统上安装此 Microsoft 修补程序以启用通过 WMI 监控 Microsoft Windows Server 2008。

此外，建议执行以下 Microsoft 知识库文章中的步骤以避免出现权限问题以及缺少或损坏的计数器值:

Microsoft 知识库文章	问题/说明
http://support.microsoft.com/kb/300702/en-us http://support.microsoft.com/kb/164018/en-us	**无法连接到计算机**：用户必须拥有特定访问权限才能监控 Windows 远程服务器中的性能对象，如 Microsoft 知识库文章 300702 和 164018 中所述。
http://support.microsoft.com/kb/295292	**WMI 权限**：要配置 WMI 服务用于远程监控，在 WMI 远程服务器上输入的用户必须具有从 WMI 命名空间 root\CIMV2 远程读取统计信息的权限。
http://support.microsoft.com/kb/300956/en-us	**缺少/损坏的性能计数器库值**：如果必需的性能计数器库值缺少或存坏，请按照 Microsoft 知识库文章 KB300956 中的说明手动重新构建这些值。

第 27 章: 开始使用 SiteScope

本章包括:

启动 SiteScope 服务概述

安装时会在所有平台上启动 SiteScope 进程。

- 在 Windows 平台上，会将 SiteScope 作为一个服务添加，并会将该服务设置为在服务器重新启动时自动重启。
- 在 Linux 平台上，每次重新启动安装 SiteScope 的服务器时，都必须重新启动 SiteScope 进程。

可以执行本节中所描述的步骤，根据需要手动启动和停止 SiteScope 进程。

在 Windows 平台上启动和停止 SiteScope 服务

SiteScope 在 Microsoft Windows 平台作为服务安装。默认情况下，SiteScope 服务设置为在服务器重新启动时自动重启。您可以使用“服务”控制面板手动启动和停止 SiteScope 服务。

要使用“服务”控制面板启动或停止 SiteScope 服务，请执行以下操作:

1. 通过选择“开始”>“设置”>“控制面板”>“管理工具”>“服务”，打开“服务”控制面板。
2. 在服务列表中选择 **SiteScope**，并右键单击以显示操作菜单。
3. 根据需要从操作菜单中选择“启动”或“停止”。

Netstart 和 Netstop 命令

您还可以使用 netstart 和 netstop 命令来启动和停止 SiteScope 服务。

要使用 netstart 启动 SiteScope 服务，请执行以下操作:

1. 在装有 SiteScope 的服务器上打开命令行窗口。
2. 使用以下语法运行 netstart 实用程序:

   net start SiteScope

要使用 netstop 停止 SiteScope 服务，请执行以下操作:

1. 在运行 SiteScope 的服务器上打开命令行窗口。
2. 使用以下语法运行 netstop 实用程序:

net stop SiteScope

在 Linux 平台上启动和停止 SiteScope 进程

SiteScope 具有自动启动进程，在系统启动时自动启动 SiteScope，并在系统停止时自动停止 SiteScope。请注意，如果要更改 SiteScope 可执行程序（启动、停止）的权限，必须也在 **/etc/init.d/sitescope** 文件中更改权限。

还可以使用产品附带的 shell 脚本手动启动和停止 SiteScope。也可使用 init.d 脚本在重新启动服务器时自动重启 SiteScope。

备注: 虽然必须通过 root 用户帐户在 Linux 上安装 SiteScope，但是在安装后，可以使用非 root 用户帐户运行。有关详细信息，请参阅配置有权运行 SiteScope 的非 root 用户帐户 (第 35 页)。

要在 Linux 上手动启动 SiteScope 进程，请执行以下操作：

1. 在安装 SiteScope 的服务器上打开终端窗口。
2. 使用以下语法运行 start 命令 shell 脚本：

   <安装路径>/SiteScope/start

   （在 Linux/UNIX 计算机上，可以在任何目录中运行 service sitescope start。）

要在 Linux 上手动停止 SiteScope 进程，请执行以下操作：

1. 在运行 SiteScope 的服务器上打开终端窗口。
2. 使用以下语法运行 stop 命令 shell 脚本：

   <安装路径>/SiteScope/stop

   （在 Linux/UNIX 计算机上，可以在任何目录中运行 service sitescope stop。）

在上述各个命令中，用安装 SiteScope 的路径替代 <安装路径>。例如，如果您将 SiteScope 安装在 /usr 目录中，则要停止 SiteScope 的命令为：

/usr/SiteScope/stop

连接到 SiteScope

SiteScope 被设计为 Web 应用程序的形式，这意味着您可以使用可访问 SiteScope 服务器的 Web 浏览器来查看和管理 SiteScope。

SiteScope 安装为在两个端口上进行响应：8080 和 8888。如果有其他服务被配置为要使用这两个端口，则安装进程会尝试配置 SiteScope 在其他端口上响应。

在 Windows 平台上，安装进程还会在“开始”>“所有程序”菜单中为 SiteScope 添加 SiteScope 链接。“开始”菜单文件夹可在安装过程中选择。

要访问 SiteScope，请执行以下操作：

在 Web 浏览器中输入 SiteScope 地址。默认地址为：http://localhost:8080/SiteScope。

在 Windows 平台上，您还可以通过单击“开始”>“所有程序”>“HP **SiteScope**”>“打开 HP **SiteScope**”，来访问 SiteScope。如果在安装 SiteScope 后更改了 SiteScope 端口，则会在“打开 HP SiteScope”链接中更新端口。

第一次部署 SiteScope 时，会因为初始化界面元素而出现延迟。SiteScope 打开后进入“控制面板”视图。

备注:

- 要限制对此帐户及其权限的访问，必须编辑管理员帐户配置文件，以在其中包含用户登录名和密码。随后，SiteScope 会在用户可以访问 SiteScope 之前显示一个登录对话框。有关如何编辑管理员帐户配置文件的信息，请参阅 SiteScope帮助中《使用 SiteScope》中的“用户管理首选项”部分。
- 从其他计算机查看 SiteScope 时，建议您使用已安装最新支持版本的 Java Runtime Environment 的计算机。

SiteScope 经典界面

可在先前版本的 SiteScope 中使用的 SiteScope 经典界面（使用 URL：http://<sitescope 主机>:8888）现已不再用于管理 SiteScope。

如果 **master.config** 文件中的 **_serverFilter** 属性中列出了经典界面中的某些特定页面，则您仍可访问它们。默认情况下，列出的页面包括“监控器概要”和“警报报告”页。

备注: 请不要删除默认情况下启用的 SiteScope 经典界面页面，因为这会导致某些功能故障。

疑难解答和限制

本节提供了有关在登录 SiteScope 时出现的以下问题的疑难解答和限制：

特定启动问题：

SiteScope 不启动并显示错误消息

如果在启动 SiteScope applet 时遇到如“无法加载 Java Runtime Environment”这样的错误消息或者任何其他未知错误，请执行下列步骤。

在每个步骤之后，尝试重新打开 SiteScope。如果 SiteScope 仍然失败，则继续执行下一个步骤。

1. 关闭所有浏览器窗口。
2. 使用“Windows 任务管理器”结束所有其他浏览器进程（如果尚存在这类进程）。
3. 清除本地 Java applet 缓存。选择“开始”>“控制面板”>“Java”。在“常规”选项卡中，单击“设置”>“删除文件”，然后单击“确定”。
4. 通过删除以下文件夹的内容，清除本地 Java applet 缓存：C:\Documents and Settings\<用户名>\Application Data\Sun\Java\Deployment\cache。

SiteScope applet 加载失败，出现“NoClassDefFound”异常

如果 applet 加载失败并出现“NoClassDefFound”异常，请在客户端的 Java 配置中选择“将临时文件保存在我的计算机上”选项（“控制面板”>“Java”>“常规”选项卡 >“临时 Internet 文件”>“设置”）。

如果出于安全问题的考虑，您可以在 SiteScope applet 使用完成后手动删除临时文件：

1. 关闭 SiteScope applet。
2. 选择“开始”>“控制面板”>“Java”>“常规”选项卡。
3. 在“临时 Internet 文件”部分中，单击“设置”，然后单击“删除文件”。

从 64 位计算机加载 applet 时出现问题

在 64 位计算机上运行 SiteScope 时，请确保所使用的浏览器版本与 JRE 相匹配：

JRE	浏览器
64 位 JRE	Internet Explorer（64 位）
32 位 JRE	Internet Explorer（32 位）

在浏览器窗口的多个选项卡上打开同一个 SiteScope 服务器时，SiteScope 挂起

如果在浏览器窗口的多个选项卡中打开同一个 SiteScope 服务器用户界面，然后尝试在多个 SiteScope 服务器选项卡之间进行浏览时，SiteScope 挂起。

可能的解决方案：

- 关闭多余的选项卡，确保对同一个 SiteScope 服务器用户界面只打开了一个选项卡。
- 另外，也可以打开一个新的浏览器窗口。

SiteScope 菜单栏打开，但 applet 未能启动，并显示一个空白屏幕、一条错误消息或一个带有“x”标记的图像

如果 Java 控制面板未配置为使用 Web 浏览器，则可能会发生这种情况。

可能的解决方案：

1. 单击“开始”>“控制面板”>“Java”。在“常规”选项卡中，单击“网络设置”，选择“直接连接”选项，然后单击“确定”。
2. 在“高级”选项卡中，展开“浏览器的默认 Java”文件夹（如果您正在使用 Java 5，则展开“<APPLET> 标记支持”）。确保选中 **Microsoft Internet Explorer** 和 **Mozilla 系列**。单击“应用”，然后单击“确定”。
3. 重新启动浏览器。

在无法启动 SiteScope 时备份和恢复 SiteScope 安装

要在 SiteScope 发生故障并且无法重新启动时恢复 SiteScope 配置数据，请在安装新版本的 SiteScope 之前，对当前的 SiteScope 安装目录及其所有子目录进行备份。您可以使用配置工具备份当前的 SiteScope 安装，将 SiteScope 数据导出为 **.zip** 文件，或者手动备份所需文件。

在重新安装 SiteScope 之后，可以使用配置工具（如果您使用该工具对安装目录进行了备份）将监控器配置数据复制到 SiteScope 中，或者从新安装目录删除您已备份的所有文件夹和文件，然后将备份的文件夹和文件复制到安装目录。

要对 SiteScope 安装进行备份，请执行以下操作：

1. 停止 SiteScope。

   备注: 尽管并不一定要停止 SiteScope，但仍然建议您在进行备份之前执行此操作。

2. 采用以下方式之一，对当前 SiteScope 安装目录进行备份：
   - 使用配置工具将配置导出到 **.zip** 文件中。有关详细信息，请参阅使用 SiteScope 配置工具 (第 107 页)。
   - 将以下文件夹和文件从 SiteScope 安装复制到备份目标位置：

目录	描述
\cache	包含 Business Service Management 发生故障时没有报告给 Business Service Management 的数据样本。
\conf\ems	包含用于“集成”监控器类型的关键配置和控制文件。只有在您将 SiteScope 用作向其他 Business Service Management 应用程序进行报告的代理时，这些文件才适用。
\conf\integration	包含用于与 Business Service Management 进行集成的拓扑文件。
\discovery\scripts\custom	包含自定义搜寻脚本。
\groups	包含 SiteScope 操作所需的监控器、警报、报告和其他关键配置数据。
\htdocs	包含用于 SiteScope 界面的计划报告和用户定义的样式表。备份此目录，并将它复制到 SiteScope 目录（在同一个 SiteScope 版本中）中，以避免损坏报告页，并查看旧报告。在将配置导入到新的 SiteScope 版本中时，此文件夹无法备份。

目录	描述
\logs	包含许多日志，它们包含按日期编码的监控数据日志。您可以有选择地备份最新监控数据日志文件以及此目录中的其他日志类型。您可能还要备份 **error.log**、**RunMonitor.log**、**access.log**、**alert.log** 和 **monitorCount.log** 日志，以保证历史记录的连续性。
\persistency	这是产品的主要持久性目录，可在此目录中找到所有定义的监控器、组、警报、模板和许多其他 SiteScope 实体。
\scripts	包含由脚本监控器使用的脚本。
\scripts.remote	包含脚本监控器用来触发远程服务器上其他脚本的命令脚本。
\templates.*	包括用于对监控器功能、警报内容和其他功能进行自定义的数据和模板。子目录组均以名称 templates 开头。 **示例：** templates.mail、templates.os、templates.webscripts
\WEB-INF\lib\peregrine.jar	在配置 HP Service Manager 集成时可能已更改（已重新生成）的文件。

要恢复 SiteScope 安装，请执行以下操作：

1. 请执行新的 SiteScope 安装。有关详细信息，请参阅安装工作流 (第 72 页)。
2. 安装 SiteScope 之后：
   - 如果已使用配置工具对当前 SiteScope 安装目录进行了备份，请使用配置工具导入先前创建的 **.zip** 文件。有关详细信息，请参阅使用 SiteScope 配置工具 (第 107 页)。
   - 如果您手动创建了备份，请从新安装目录中删除上面列出的所有文件夹和文件，然后将备份的文件夹和目录复制到安装目录中。

无法在 Firefox 中打开 SiteScope

问题： 在禁用智能卡强制执行，但启用了客户端证书身份验证的情况下，无法在 Firefox 浏览器中打开 SiteScope。

解决方案： 要在禁用智能卡强制执行，但启用了客户端证书身份验证的情况下，在 Firefox 浏览器中打开 SiteScope，请参阅在客户端认证启用的情况下使用 Firefox (第 134 页)。

附录

附录 A: 将 IIS 与 SiteScope 中的 Tomcat 服务器集成

要将 Internet 信息服务器 (IIS) 与 SiteScope 中包含的 Apache Tomcat 服务器进行集成，需要更改 Apache Tomcat 服务器所使用的配置文件，并在 IIS 配置中的对应网站对象中创建虚拟目录。

本节包括：

配置 Apache Tomcat 服务器文件

要集成 IIS 与 Apache Tomcat 服务器，您必须编辑 SiteScope 中包含的 Apache Tomcat 服务器的配置文件。

要配置 Apache Tomcat 服务器文件，请执行以下操作：

1. 从 Apache 下载地址下载连接器文件的最新 Java Connector jk 版本：

   http://tomcat.apache.org/download-connectors.cgi
2. 将 **isapi_redirect.dll** 文件复制到 **<Tomcat 安装>\bin\win32** 目录。默认情况下，将在安装 SiteScope 时在 **C:\SiteScope\Tomcat** 目录下安装 Tomcat 服务器。如果 **win32** 目录不存在，则创建该目录。
3. 执行下列其中一个操作：
   - 在 **isapi_redirect.dll** 文件所在的目录中创建一个名为 **isapi_redirect.properties** 的配置文件。

     isapi_redirect.properties 文件示例：

     ```
     # Configuration file for the Jakarta ISAPI Redirector

     # The path to the ISAPI Redirector Extension, relative to the website
     # This must be in a virtual directory with execute privileges
     extension_uri=/jakarta/isapi_redirect.dll

     # Full path to the log file for the ISAPI Redirector
     log_file=C:\SiteScope\Tomcat\logs\isapi.log

     # Log level (debug, info, warn, error or trace)
     log_level=info

     # Full path to the workers.properties file
     worker_file=C:\SiteScope\Tomcat\conf\workers.properties.minimal
     ```

```
# Full path to the uriworkermap.properties file
worker_mount_file=C:\SiteScope\Tomcat\conf\uriworkermap.properties
```

此配置指向日志文件（建议将此文件放置在 **<SiteScope 根目录>\Tomcat\logs** 目录下）以及工作程序和工作程序安装文件（应存储在 **<SiteScope 根目录>\Tomcat\conf** 目录下）。

- 将相同的配置条目（请参阅以上内容）添加到以下路径的注册表中：HKEY_LOCAL_MACHINE\SOFTWARE\Apache Software Foundation\Jakarta Isapi Redirector\1.0

4. 在 **<SiteScope 根目录>\Tomcat\conf** 目录下创建一个名为 **workers.properties.minimal** 的 SiteScope 工作程序文件。

SiteScope 工作程序文件示例：

```
# workers.properties.minimal -
#
# This file provides minimal jk configuration
# properties needed to
# connect to Tomcat.
#
# Defining a worker named ajp13w and of type ajp13
# Note that the name and the type do not have to
# match.
worker.list=ajp13w
worker.ajp13w.type=ajp13
worker.ajp13w.host=localhost
worker.ajp13w.port=8009
#END
```

注意：

- **worker.ajp13w.port** 取决于所使用的 Tomcat 版本。打开 **<SiteScope 根目录>\Tomcat\conf\server.xml**，搜索字符串 <Connector port=，确定此 Tomcat 版本所使用的端口。
- 如果将 SiteScope 配置为与 SiteMinder 集成，则在 **server.xml** 文件中将 <!-- Define an AJP 1.3 Connector on port 8009 --> 部分的重定向端口从：

  ```
  <!--   <Connector port="18009"
  URIEncoding="UTF-8" enableLookups="false" redirectPort="8443" protocol="AJP/1.3" /> -->
  ```

  更改为

  ```
  <Connector port="18009"
  URIEncoding="UTF-8" enableLookups="false" redirectPort="80" protocol="AJP/1.3" />
  ```

- 如果 IIS 和 Tomcat 不在同一台计算机上，请将 **workers.properties.minimal** 中的主机属性更改为指向其他计算机。

5. 在 **<SiteScope 根目录>\Tomcat\conf** 目录下创建一个 SiteScope 工作程序安装文件。

名为 uriworkermap.properties 的 SiteScope 工作程序文件示例（如前面的配置示例中所示）：

```
# uriworkermap.properties - IIS
#
# This file provides sample mappings for example:
# ajp13w worker defined in workermap.properties.minimal
# The general syntax for this file is:
# [URL]=[Worker name]
/SiteScope=ajp13w
/SiteScope/*=ajp13w
#END
```

新语法将 SiteScope 的两个规则合并为一个规则：/SiteScope/*=ajp13w

Tomcat 日志输出被写入 **<SiteScope 根目录>\logs\tomcat.log** 文件。可在 **<SiteScope 根目录>\Tomcat\common\classes\log4j.properties** 文件中配置日志文件的设置。

疑难解答

问题：从 SiteScope 的较早版本升级时，将覆盖 **<SiteScope 根目录>\Tomcat\conf** 目录中的 **server.xml** Tomcat 配置文件，对该文件所做的任何修改都将删除（例如将 SiteScope 配置为使用 SSL 时所做的更改）。

解决方案：要恢复这些修改，必须在执行升级后将它们重新应用到 **server.xml** 文件。

a. 停止 SiteScope。

b. 替换以下文件：

要替换的文件	替换为的文件
<SiteScope 根目录>\java\lib\security\cacerts	**<SiteScope 根目录>\installation\HPSiS1122\backup\java\lib\security\cacerts**
<SiteScope 根目录>\java\lib\security\java.security	**<SiteScope 根目录>\installation\HPSiS1122\backup\java\lib\security\java.security**
<SiteScope 根目录>\java\lib\security\javaws.policy	**<SiteScope 根目录>\installation\HPSiS1122\backup\java\lib\security\javaws.policy**
<SiteScope 根目录>\java\lib\security\java.policy	**<SiteScope 根目录>\installation\HPSiS1122\backup\java\lib\security\java.policy**

c. 通过将所有强化和其他自定义更改从 **<SiteScope 根目录>\installation\HPSiS1122\backup\Tomcat\conf\server.xml** 复制到 **<SiteScope 根目录>\Tomcat\conf\server.xml** 以手动应用这些更改。

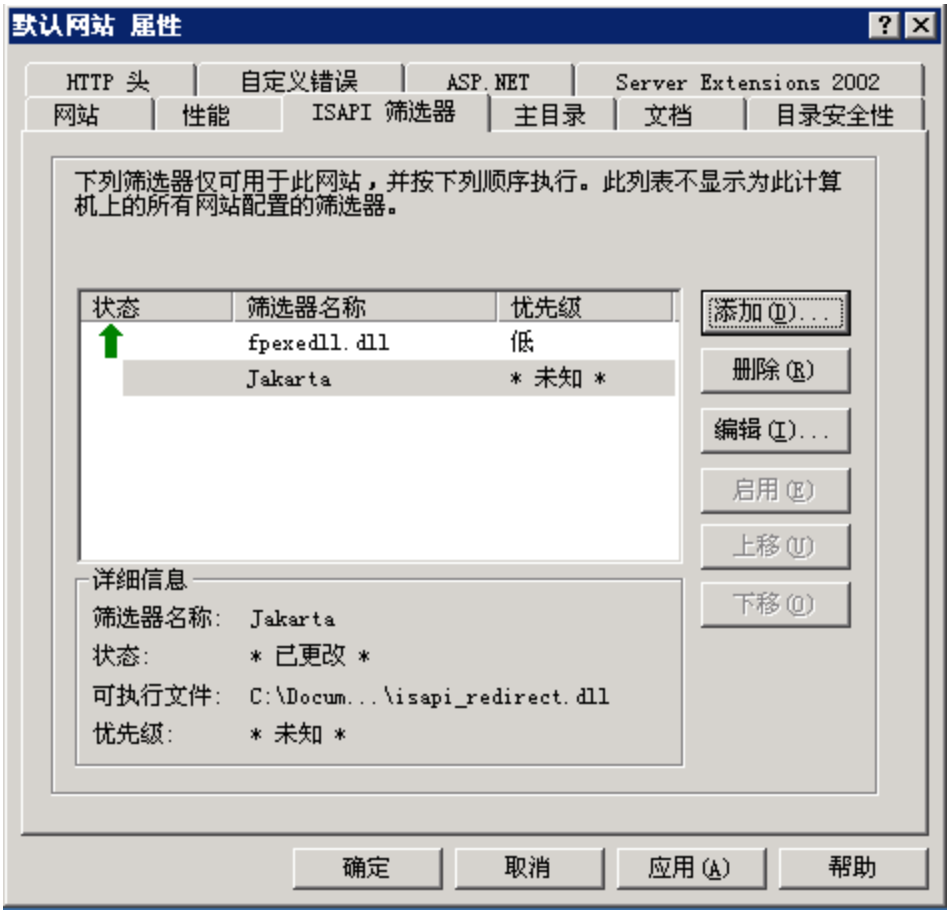
配置 IIS

更改 Tomcat 服务器所使用的配置文件之后，需要在 IIS 配置中的对应网站对象中创建虚拟目录。

要配置 IIS，请执行以下操作：

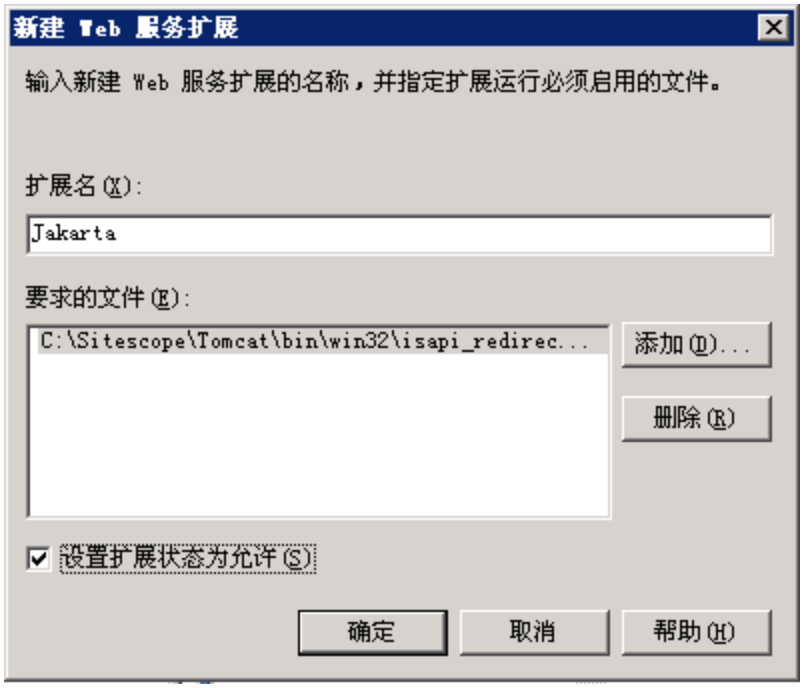
1. 在 Windows 的“开始”菜单上单击“设置”>“控制面板”>“管理工具”>“Internet 信息服务(IIS)管理器”。
2. 在右窗格中，右键单击 **<本地计算机名称>\Web Sites\<网站名称>**，然后单击“新建\虚拟目录”。将其重命名为 **Jakarta**，并将“本地路径”设置为 **isapi_redirect.dll** 所在的目录。

3. 右键单击 **<网站名称>**，然后单击“属性”。
4. 单击“ISAPI 筛选器”选项卡，然后单击“添加”。在“筛选器名称”列中，选择 **Jakarta**，并浏览到 **isapi_redirect.dll**。此时已添加筛选器，但目前该筛选器仍处于非活动状态。



单击“应用”。

5. 右键单击 **<本地计算机名称>\Web Service extensions**，然后单击“添加新的 Web 服务扩展”。此时将打开“新建 Web 服务扩展”对话框。
6. 在“扩展名”框中，输入名称 Jakarta，然后在“要求的文件”下浏览到 **isapi_redirect.dll** 文件。选择“设置扩展状态为允许”。



单击“确定”。

7. 重新启动 IIS Web 服务器，然后尝试通过 Web 服务访问应用程序。

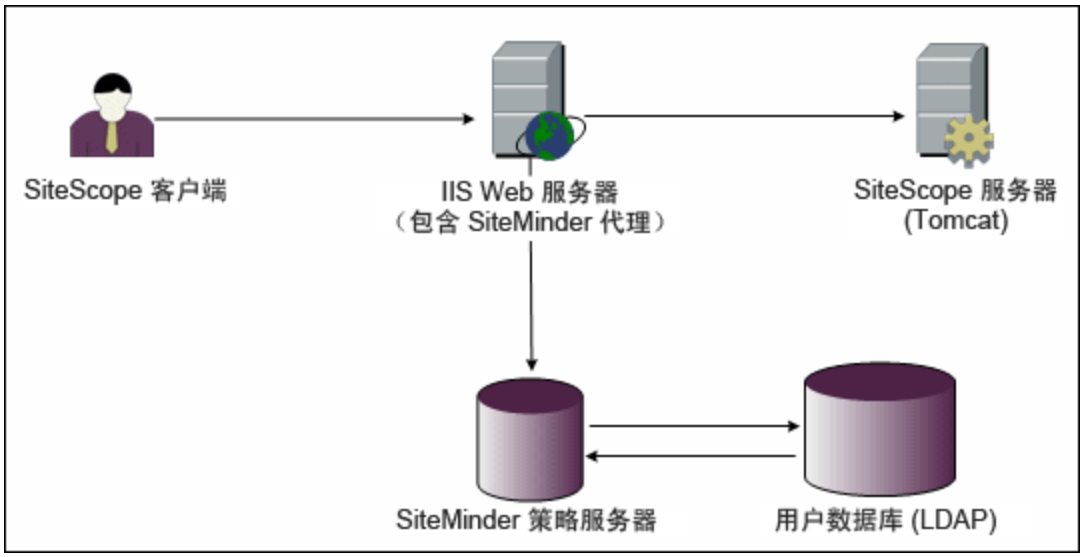
附录 B: 将 SiteScope 与 SiteMinder 集成

SiteScope 可与安全访问管理解决方案 SiteMinder 集成，以利用客户的用户和访问管理配置。

本节包括：

了解与 SiteMinder 的集成

下图演示了 SiteScope 如何与 SiteMinder 集成，以对 SiteScope 用户进行身份验证和授权。



在此体系结构中，在位于 SiteScope 的 Tomcat 应用程序服务器前的 IIS Web 服务器上配置了一个 SiteMinder 代理。SiteMinder 代理必须位于 Web 服务器上。IIS Web 服务器连接到管理 LDAP 或任何其他类似库中的所有 SiteScope 用户的 SiteMinder 策略服务器。

SiteMinder 代理会拦截所有与 SiteScope 相关的流量，并检查用户的凭据。用户的凭据会发送到 SiteMinder 策略服务器，进行身份验证和授权。如果 SiteMinder 对用户进行身份验证，则它会向 SiteScope 发送一个标记（使用特殊的 HTTP 标头），用于描述已成功登录并通过 SiteMinder 授权的用户。

备注: 建议在同一台计算机上配置 SiteScope 客户端、IIS Web 服务器以及 SiteScope 的 Tomcat 应用程序服务器。

集成要求

本节说明将 SiteScope 与 SiteMinder 集成时所需的最低系统要求。

操作系统	Windows 2003 Standard/Enterprise SP1
Web 服务器	IIS 5.0、IIS 6.0
应用程序服务器	Tomcat 5.0.x
Java 连接器	Java Connector jk-1.2.21

集成过程

本节描述 SiteMinder 集成过程。

要集成 SiteScope 与 SiteMinder，请执行以下操作:

1. **准备和配置 SiteMinder 策略服务器。**

   SiteMinder 管理员需要准备用于安装 Web 代理的 SiteMinder 策略服务器，在 IIS Web 服务器上安装 Web 代理，并配置 Web 代理。

   此外，SiteMinder 管理员还需要配置 SiteMinder 策略服务器。有关建议的 SiteMinder 配置的详细信息，请参阅配置 SiteMinder 策略服务器 (第 179 页)。
2. **配置 SiteScope 以使用 SiteMinder。**

   要使 SiteScope 可与 SiteMinder 集成，您需要对 Tomcat 服务器所使用的配置文件进行更改。有关详细信息，请参阅配置 Apache Tomcat 服务器文件 (第 172 页)。
3. **配置 IIS。**

   需要在 IIS 配置中的对应网站对象中创建虚拟目录。有关详细信息，请参阅配置 IIS (第 175 页)。
4. **为不同 SiteScope 角色定义权限。**

   启用 SiteMinder 集成之后，必须为 SiteScope 中的不同角色定义权限。有关详细信息，请参阅定义不同 SiteScope 角色的权限 (第 181 页)。

配置 SiteMinder 策略服务器

您可以对 SiteMinder 策略服务器进行配置，方法是：创建一个 SiteScope 领域对象、两个用于身份验证和转发 Cookie 与其他属性的 SiteScope 规则对象、一个将其他 LDAP 属性传输到 SiteScope 的 SiteScope 响应对象，以及向安全策略对象添加一些 SiteScope 规则和响应。

在策略服务器上创建 SiteScope 领域对象之前，请确保:

- 已在域（绑定到一个或多个用户目录）上配置特殊管理员。
- 已配置一个或多个用户目录对象。这些对象代表 LDAP 目录或任何其他库中的用户。
- 已定义身份验证方案。

  域已连接到一个或多个用户目录对象。不必为领域创建特殊域，使用现有域即可。

要配置 SiteMinder 策略服务器，请执行以下操作：

1. 登录到“SiteMinder Administration”。
2. 创建领域，并输入以下信息：
   - **名称。**输入领域的名称。例如，**SiteScope realm**。
   - **资源筛选器。**输入 **/SiteScope**。SiteScope 下的所有内容将成为领域的一部分。
3. 右键单击新领域，然后单击“Create rule under realm”。
   - 创建用于身份验证的规则。为规则输入有意义的名称，例如 **SiteScope rule**。在“Action”部分中，选择“Web Agent Action”选项并选择所有 HTTP 请求方案（**Get**、**Post** 和 **Put**）。
   - 创建用于将 Cookie 和其他属性转发到 SiteScope 的第二个规则。为规则输入有意义的名称，例如 **Users role**。在“Action”部分中，选择“Authentication events”选项，并从下拉列表中选择“OnAuthAccept”。
4. 创建 SiteScope 响应对象，以将其他 LDAP 属性与相关身份验证信息传输到 SiteScope。
   a. 右键单击“Responses”，打开“Response Properties”窗口。
   b. 为“Response”输入有意义的名称。例如，**SiteScope Role**。
   c. 在“Attribute List”部分下，单击“Create”按钮打开一个新窗口，在其中对属性列表进行配置。
   d. 在“Attribute Kind”部分中，选择“User Attribute”选项。
   e. 在“Attribute Fields”部分中，选择“SITESCOPE_ROLE”作为变量名，并从在标头中发送到 SiteScope 的预定义用户目录中选择要作为所选字段的属性名。这是要在身份验证时发送的“用户目录”属性。

   备注: 如果使用 LDAP 组对象或嵌套的组对象来定义 SiteScope 角色，则应对“Attribute Name”字段使用特殊 SiteMinder 变量。应将“SM_USERGROUPS”变量用于常规组；如果要让 **SITESCOPE_ROLE** HTTP 标头包含嵌套组的信息，则使用“SM_USERNESTEDGROUPS”变量。
5. 将 SiteScope 规则和响应添加到安全策略对象中。
   a. 单击“Policies”选项，创建新的安全策略。
   b. 为策略输入有意义的名称。例如，**SiteScope Policy**。
   c. 单击“Users”选项卡，然后添加或删除要应用策略的实体。（只能从领域的同一个域的用户目录中选择实体。）
   d. 单击“Rules”选项卡，并选择在步骤 3 中描述的“Users Role”和“**SiteScope** Rule”。此外，还需添加“**SiteScope** Role”响应，该响应已在先前的步骤 4 中定义为“Users Role”的响应。

配置 SiteScope 以使用 SiteMinder

要使 SiteScope 可与 SiteMinder 集成，您需要对 Tomcat 服务器所使用的配置文件进行更改。有关配置 Tomcat 服务器文件的信息，请参阅配置 Apache Tomcat 服务器文件 (第 172 页)。

配置 IIS

对 Tomcat 服务器使用的配置文件进行更改之后，需要配置 IIS。有关如何配置 IIS 的信息，请参阅配置 IIS (第 175 页)。

定义不同 SiteScope 角色的权限

启用 SiteMinder 集成后，必须在 SiteScope 中定义不同角色的权限（使用 SiteScope 常规用户权限模型）。这些角色的用户关联将在 SiteScope 的外部完成，例如在 LDAP 组中完成。添加新 SiteScope 用户时，只须在 SiteMinder 中定义它，原因是用户会从相关 SiteScope 角色自动继承权限。

备注: 必须确保 SiteMinder 所使用的 SiteScope 用户帐户不需要密码，否则 SiteMinder 无法登录。有关创建用户帐户的详细信息，请参阅 SiteScope 帮助中《使用 SiteScope》的“用户管理首选项”部分。

登录 SiteScope

用户尝试登录 SiteScope 时，SiteMinder 会拦截请求。如果它验证用户的凭据有效，则会将分配的 SiteScope 用户名和角色（组）发送到 SiteScope（例如，User:Fred, Role:Accounting）。如果 SiteScope 未能将名称识别为有效的用户名称，但识别出角色，则用户将使用角色登录到 SiteScope（在此示例中，User:Accounting）。

要登录 SiteScope，请执行以下操作:

打开 Web 浏览器，并键入以下 URL:

http://<IIS 计算机名称>/SiteScope。

备注: 如果 IIS 和 SiteScope 位于同一台计算机上，则应当连接到默认端口 80，而不是端口 8080。

在 SiteMinder 成功对用户进行身份验证且用户登录到 SiteScope 后，SiteScope 会直接打开到“控制面板”视图。

注意事项和指导原则

- 登录到 SiteScope 的所有用户的名称均列在审核日志中，此日志位于 **<SiteScope 根目录>\logs** 目录中。即使用户以角色名称登录，也会列出名称。例如，如果因为 SiteScope 未将 Fred 识别为有效用户但识别出角色，则用户 Fred 以角色登录，而在审核日志中，所有操作仍会列在用户名 Fred 下。
- 可以指定在注销 SiteMinder 环境后，浏览器将重定向到的页面（这是在 SiteScope 中单击“注销”

按钮后打开的页面）。要启用注销页面，请打开位于 **<SiteScope 根目录>\groups** 中的 **master.config** 文件，并添加以下行：

_siteMinderRedirectPageLogout=<url_to_go_to_after_logout>

- SiteMinder 用于登录 SiteScope 的用户账户不能有密码，否则 SiteMinder 无法登录。有关如何在 SiteScope 中设置用户帐户的详细信息，请参阅 SiteScope 帮助中《使用 SiteScope》的“用户管理首选项”部分。
- 要阻止用户尝试直接使用 SiteScope URL 访问 SiteScope，应考虑在 SiteScope 安装期间在 Tomcat 服务器上禁用 HTTP 端口 8080 和 8888。
- 要防止用户在 Web 浏览器处于非活动状态 30 分钟后从 SiteScope 中注销，请将 **master.config** 文件中的“_keepAliveFromJSP=”属性更改为“=true”。

附录 C: 手动将 SiteScope 配置为使用安全连接

您可以手动将 SiteScope 配置为使用安全连接，以限制对 SiteScope 界面的访问。

建议使用强化工具将 SiteScope 配置为使用 SSL。有关详细信息，请参阅使用强化工具 (第 149 页)。

本节包括：

为 SiteScope 使用 TLS 做准备

SiteScope 附带了 **Keytool.exe**。Keytool 是一个密钥和证书管理实用程序。该实用程序允许用户管理自己的公/私钥对以及关联的证书，以便使用数据签名进行身份验证。同时，它还允许用户对与其通信的其他人员和组织的公钥进行缓存操作。该实用程序安装在 **<SiteScope 安装路径>\SiteScope\java\bin** 目录下。

警告: 当创建、请求和安装数字证书时，请记录您在该过程的每个步骤中使用的参数和命令行参数。在整个过程中都使用相同的值是十分重要的。

备注:

- SiteScope 仅使用 JKS 格式的密钥库和信任库。
- 要使 SiteScope 经典界面能够与 TLS 配合使用，您必须配置 Tomcat 服务器（请参阅配置 SiteScope 以在 Tomcat 上使用 TLS (第 186 页)）和经典界面引擎（请参阅使用 HTTPS 访问 SiteScope 报告和经典用户界面 (第 195 页)中的说明）。

可以在 Oracle 网站 (http://docs.oracle.com/javase/7/docs/technotes/tools/windows/keytool.html) 上找到有关 keytool 的详细信息。

本节包括以下主题：

使用证书颁发机构的证书

您可以使用证书颁发机构颁发的数字证书。要使用此选项，需要可导入 Keytool 所使用的密钥存储文件的数字证书。如果您的组织当前没有此类数字证书，则需要请求证书颁发机构为您颁发证书。

可使用以下步骤创建密钥库文件和数字证书请求。

要使用证书颁发机构颁发的证书，请执行以下操作：

1. 从证书颁发机构获取根证书（以及其他任何中间证书）。
2. 从用户界面或通过运行以下命令将根证书（以及其他任何中间证书）导入到 **<SiteScope 根目录>\java\lib\security\cacerts**：

   keytool -import -alias yourCA -file C:\CAcertificate.cer -keystore ..\lib\security\cacerts -storepass changeit
3. 删除 **<SiteScope 根目录>\groups** 目录中的 **serverKeystore** 文件。您可以将其删除，或者移动到其他目录。
4. 通过从 **<SiteScope 根目录>\java\bin** 目录运行以下命令行创建密钥对：

   keytool -genkey -dname "CN=www.yourDomain.com, OU=yourDepartment, O=yourCompanyName, L=yourLocation, ST=yourState, C=yourCountryCode" -alias yourAlias -keypass keypass -keystore ..\..\groups\serverKeystore -storepass keypass -keyalg "RSA" -validity valdays

   备注:
   - 必须在一行中输入此命令和您所使用的其他命令。为了适于在此页面中显示，这里对行进行了划分。
   - 输入生成证书时使用的 serverKeystore 字符串时，大小写必须与文档中指定的大小写一致，否则使用通过 SSL 的 SiteScope 故障转移时操作将失败。
   - 私钥密码和密钥库密码必须相同，以避免出现 IOException:Cannot recover key 错误。

   此命令会在 **<SiteScope 根目录>\groups** 目录中创建一个名为 **serverKeystore** 的文件。SiteScope 会使用此文件存储安全会话中使用的证书。请确保在其他位置中保留此文件的备份。

   准则和限制
   - -dname 选项值必须具有如下顺序，其中的斜体值将替换为您选择的值。关键字的缩写如下：

     CN = commonName - 普通人名（如 Warren Pease）

     OU = organizationUnit - 小型组织单位（如 NetAdmin）

     O = organizationName - 大型组织名称（如 ACMe-Systems, Inc.）

     L = localityName - 地点（城市）名称（如 Palo Alto）

     ST = stateName - 州名或省名（如 California）

     C = country - 国家/地区代码（两个字母，如 US）
   - -dname（可分辨名称字符串）变量中的子组件不区分大小写且具有顺序，但您不必包含所有子组件。-dname 变量表示公司，CN 是安装 SiteScope 的 Web 服务器的域名。
   - -storepass 值是用于保护密钥库文件的密码。该密码必须至少包含 6 个字符。将证书数据导入密钥库文件和从密钥库文件中删除证书数据时需要使用此密码。
   - -alias 变量是一个别名或昵称，用于标识密钥库中的条目。
5. 通过从 **<SiteScope 根目录>\java\bin** 目录运行以下命令，为此密钥库创建一个证书请求：

keytool -certreq -alias yourAlias -file ..\..\groups\sis.csr -keystore ..\..\groups\serverKeystore -storepass passphrase

此命令将在 **<SiteScope 根目录>\groups** 目录中创建名为 **sis.csr** 的文件。可使用此文件向证书颁发机构请求证书。

接收到证书颁发机构颁发的证书后（回复消息中会包含一个名为 **cert.cer** 的文件），需要将此证书导入到通过上述步骤创建的密钥库文件中。该文件的名称应为 **serverKeystore**。使用以下步骤导入证书以用于 SiteScope。

6. 通过从 **<SiteScope 根目录>\java\bin** 目录运行以下命令，将证书数据导入到密钥库文件中：

   keytool -import -trustcacerts -alias yourAlias -file cert.cer -keystore ..\..\groups\serverKeystore

   备注: 为避免在导入证书颁发机构颁发的证书时出现 keytool error:java.lang.Exception:Failed to establish chain from reply 错误，应使用用户界面的“证书管理”或通过运行以下命令，将证书颁发机构颁发的根证书（以及其他任何中间证书）导入到 **<SiteScope 根目录>\java\lib\security\cacerts** 中：

   keytool -import -alias yourCA -file C:\CAcertificate.cer -keystore ..\lib\security\cacerts -storepass changeit

7. 要将“SiteScope”更改为使用安全连接，需要在“SiteScope”中添加或修改某些设置或配置文件。有关详细信息，请参阅配置 SiteScope 以在 Tomcat 上使用 TLS (第 186 页)。

使用自签名证书

也可使用以下方式之一生成自签名证书配置 SiteScope：

- **SSL 工具。**有关详细信息，请参阅要使用 SSL 功能，请执行以下操作：（第 185 页）。
- **手动配置。**使用 -selfcert 选项让 Keytool 实用程序生成自签名证书。有关详细信息，请参阅要手动生成自签名证书，请执行以下操作：（第 185 页）。

备注: 我们建议在大多数情况下使用 SSL 工具。但是，在以下两种情况下应手动配置 SiteScope 使用 SSL：在 Windows 平台上配置且没有 %SITESCOPE_HOME% 变量（例如，SiteScope 已使用 **go.bat** 命令从其他位置启动）；在 Linux 平台上配置且未将 SiteScope 安装在 **/opt/HP/SiteScope/** 目录中。

要使用 SSL 功能，请执行以下操作：

1. 输入以下命令停止 SiteScope 服务：

   cd /opt/HP/SiteScope/
   ./stop

2. 输入以下命令运行 SSL 工具：

   cd /opt/HP/SiteScope/tools/SSL/
   ./ssl_tool.sh

3. 按照 SSL 工具中的说明执行操作。

要手动生成自签名证书，请执行以下操作：

1. 删除 **<SiteScope 根目录>\groups** 目录中的 **serverKeystore** 文件。您可以将其删除，或者移动到其他目录。

2. 从 **<SiteScope 根目录>\java\bin** 目录运行以下命令。以斜体表示的值是需要使用特定于组织的信息填写的变量。

   keytool -genkey -dname "CN=www.yourDomain.com, OU=yourDepartment, O=yourCompanyName, L=yourLocation, ST=yourState, C=yourCountryCode" -alias yourAlias -keypass keypass -keystore ..\..\groups\serverKeystore -storepass passphrase -keyalg "RSA" -validity valdays

   备注:

   - 必须在一行中输入此命令和您所使用的其他命令。为了适于在此页面中显示，这里对行进行了划分。
   - 输入生成证书时使用的 serverKeystore 字符串时，大小写必须与文档中指定的大小写一致，否则使用通过 SSL 的 SiteScope 故障转移时操作将失败。

3. 仍从 **<SiteScope 根目录>\java\bin** 目录运行以下命令:

   keytool -selfcert -alias yourAlias -sigalg "MD5withRSA" -keypass password -dname "CN=www.yourDomain.com, OU=yourDepartment, O=yourCompanyName, L=yourLocation, ST=yourState, C=yourCountryCode" -keystore ..\..\groups\serverKeystore

4. 要更改 SiteScope 以使用安全连接，需要在 SiteScope 中添加或修改某些设置或配置文件。有关详细信息，请参阅配置 SiteScope 以在 Tomcat 上使用 TLS (第 186 页)。
5. 您可以选择运行以下命令来导出证书，以便在 BSM 中使用:

   keytool -exportcert -alias yourAlias -file <SiteScope 根目录>\certificate_name.cer -keystore ..\..\groups\serverKeystore

   导出后，输入密钥库密码。

配置 SiteScope 以在 Tomcat 上使用 TLS

要在 Tomcat 上启用 TLS，需要对 Tomcat 服务器所使用的配置文件进行更改。

1. 打开 **<SiteScope 根目录>\Tomcat\conf** 目录中的 **server.xml** 文件。
2. 找到类似于下列内容的配置文件部分:

```
<!-- Define a SSL Coyote HTTP/1.1 Connector on port 8443 -->
<!--
Connector port="8443" maxHttpHeaderSize="8192"
maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
enableLookups="false" disableUploadTimeout="true"
acceptCount="100" scheme="https" secure="true"
clientAuth="false" sslProtocol="TLS"
compression="on" compressionMinSize="2048" noCompressionUserAgents="gozilla, traviata"
compressableMimeType="text/html,text/xml,text/javascript,text/css,image/x-icon,application/json" />
->
```

3. 将以上部分更改为:

```
<!-- Define a SSL Coyote HTTP/1.1 Connector on port 8443 -->
```

```
<Connector port="8443"
maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
enableLookups="false" disableUploadTimeout="true"
acceptCount="100" debug="0" scheme="https" secure="true"
clientAuth="false" sslEnabledProtocols="TLSv1,TLSv1.1,SSLv2Hello"
keystoreFile="<SiteScope_install_path>\SiteScope\groups\serverKeystore"
keystorePass="testing"
/>
```

其中，<SiteScope_install_path> 是用于安装 SiteScope 的路径。

备注:

- 如果在安装 SiteScope 的服务器上安装了其他 HP 产品，则可能需要将 8443 端口更改为其他端口号以避免冲突。
- Tomcat 日志输出被写入 **<SiteScope 根目录>\logs\tomcat.log** 文件。可在 **<SiteScope 根目录>\Tomcat\common\classes\log4j.properties** 文件中配置日志文件的设置。
- 可通过禁用弱加密来增强 Tomcat 服务器的安全性。要执行此操作，请打开 **<SiteScope 根目录>\Tomcat\conf\server.xml**，并将现有列表更改为以下列表：

  <Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
  maxThreads="150" scheme="https" secure="true" clientAuth="false"
  sslEnabledProtocols="TLSv1,TLSv1.1,SSLv2Hello" ciphers="SSL_RSA_WITH_RC4_128_
  SHA, TLS_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_128_CBC_SHA, TLS_
  DHE_DSS_WITH_AES_128_CBC_SHA, SSL_RSA_WITH_3DES_EDE_CBC_SHA, SSL_DHE_
  RSA_WITH_3DES_EDE_CBC_SHA, SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA"/>]

默认情况下，Tomcat 会在 SiteScope 用户的主目录中查找 **.keystore** 文件。

有关为 Tomcat 服务器启用 TLS 的详细信息，请参阅 http://tomcat.apache.org/tomcat-5.5-doc/ssl-howto.html。

4. 通过此示例为 Tomcat 启用 TLS 后，即可通过语法结构如下的 URL 使用 SiteScope 接口：
   https://<SiteScope 服务器>:8443/SiteScope（链接区分大小写）

配置 SiteScope 以进行 Mutual TLS 配置

如果 SiteScope 服务器要求从客户端获取客户端证书，则执行以下步骤。

1. SiteScope 应使用 TLS 进行配置。有关详细信息，请参阅配置 SiteScope 以在 Tomcat 上使用 TLS (第 186 页)。
2. 将 Tomcat 服务器配置为请求客户端证书，方法是找到 **<SiteScope 根目录>\Tomcat\conf\server.xml** 配置文件中的以下部分：

```
<Connector port="8443"
    maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
```

```
    enableLookups="false" disableUploadTimeout="true"
    acceptCount="100" debug="0" scheme="https" secure="true"
    sslEnabledProtocols="TLSv1,TLSv1.1,SSLv2Hello"
    keystoreFile="..\groups\serverKeystore"
    keystorePass="changeit"
```

然后添加以下属性并更改 clientAuth="true":

```
    truststoreFile="..\java\lib\security\cacerts"
    truststorePass="changeit"
    truststoreType="JKS"
    clientAuth="true"
/>
```

3. 将为组织颁发客户端证书的证书颁发机构的根证书导入到 SiteScope 信任库（**<SiteScope 根目录>\java\lib\security\cacerts**），方法是运行以下命令:

   C:\SiteScope\java\>keytool -import -trustcacerts -alias <您的别名> -keystore ..\lib\security\cacerts -file <证书文件>

4. 创建客户端证书或使用现有证书将其导入到浏览器中。
5. 重新启动 SiteScope 并使用以下链接访问 SiteScope:

   https://<服务器>:8443/SiteScope（链接区分大小写）

备注:

调用 SiteScope SOAP API 也需要证书。将以下内容添加到 Java 代码可使用客户端证书进行响应:

System.setProperty("javax.net.ssl.keyStore",<客户端证书密钥库的路径名称，JKS 格式>);

System.setProperty("javax.net.ssl.keyStorePassword", <客户端证书密钥库的密码>);

（可选）System.setProperty("javax.net.ssl.trustStore", <truststore 的路径名称，JKS 格式>);

或者使用以下 JVM 参数:

-Djavax.net.ssl.keyStore=<客户端证书密钥库的路径名称，JKS 格式>

-Djavax.net.ssl.keyStorePassword=<客户端证书密钥库的密码>

（可选）-Djavax.net.ssl.trustStore=<信任库的路径名称，JKS 格式>

将 SiteScope 配置为连接到使用 TLS 部署的 BSM 服务器

要将 SiteScope 连接到使用 TLS 部署的 BSM 服务器，请执行以下操作:

1. 连接到 SiteScope 服务器。
2. 在 SiteScope 用户界面中使用证书管理将 CA 根证书或 BSM 服务器证书导入到 SiteScope。有关详细信息，请参阅 SiteScope 帮助中《使用 SiteScope》指南的“证书管理”部分。
3. 如果使用负载平衡器配置 BSM，则使用 SiteScope 用户界面中的证书管理程序将负载平衡器核心和中央 URL 的证书导入到 SiteScope 中。有关详细信息，请参阅 SiteScope 帮助中《使用 SiteScope》指南的“证书管理”部分。
4. 有关如何将证书导入到 BSM 的详细信息，请参阅 BSM 文档库的《BSM Hardening Guide》中的“Using SSL with SiteScope”部分。

将 SiteScope 配置为连接到需要客户端证书的 BSM 服务器

要将 SiteScope 连接到要求提供客户端证书的 BSM 服务器，请执行以下操作：

1. 连接到 SiteScope 服务器。
2. 在 SiteScope 用户界面中使用证书管理将 CA 根证书或 BSM 服务器证书导入到 SiteScope。有关详细信息，请参阅 SiteScope 帮助中《使用 SiteScope》指南的“证书管理”部分。
3. 如果已获得 JKS 格式的客户端证书，请将其复制到 **<SiteScope 根目录>\templates.certificates** 文件夹，然后从步骤 11 继续执行操作。

   备注:

   - 确保私钥密码至少包含 6 个字符，并确保私钥和密钥库密码相同。
   - 此外，确保上述密钥库包含签发密钥的 CA 证书。

   如果获得了其他格式的客户端证书，请执行下列步骤。
4. 通过从 **<SiteScope 根目录>\java\bin** 目录运行以下命令，在 **<SiteScope 根目录>/templates.certificates** 下创建一个密钥库：

   keytool -genkey -keyalg RSA -alias sis -keystore
   <SiteScope 根目录>\templates.certificates\.ks -storepass
   <您的密钥库密码>

   示例:

   keytool -genkey -keyalg RSA -alias sis -keystore C:\SiteScope\templates.certificates\.ks -storepass changeit
   What is your first and last name?
   [Unknown]:domain.name
   What is the name of your organizational unit?
   [Unknown]:dept
   What is the name of your organization?
   [Unknown]:XYZ Ltd
   What is the name of your City or Locality?
   [Unknown]:New York

```
What is the name of your State or Province?
[Unknown]:USA
What is the two-letter country code for this unit?
[Unknown]:US
Is CN=domain.name, OU=dept, O=XYZ Ltd, L=New York, ST=USA, C=US correct?
[no]:yes

Enter key password for <SiteScope>
```

按 ENTER 键以使用与密钥库密码相同的密码。

5. **通过从 <SiteScope 根目录>\java\bin 目录运行以下命令，为此密钥库创建一个证书请求:**

   keytool -certreq -alias sis -file c:\sis.csr -keystore
   <SiteScope 根目录>\templates.certificates\.ks -storepass
   <您的密钥库密码>

   示例:

   keytool -certreq -alias sis -file c:\sis.csr -keystore
   C:\SiteScope\templates.certificates\.ks -storepass changeit

6. **请证书颁发机构对您请求的证书进行签名。将 .csr 文件的内容复制/粘贴到证书颁发机构 Web 表格中。**
7. **以 BASE-64 格式将签名的客户端证书下载到 <SiteScope 根目录>\templates.certificates\clientcert.cer。**
8. **以 BASE-64 格式将证书颁发机构颁发的证书下载到 c:\。**
9. **运行以下命令，将证书颁发机构颁发的证书导入到 JKS 密钥库中:**

   keytool -import -alias ca -file c:\ca.cer -keystore
   <SiteScope 根目录>\templates.certificates\.ks -storepass
   <您的密钥库密码>

   示例:

   ```
   keytool -import -alias ca -file c:\ca.cer -keystore C:\SiteScope\templates.certificates\.ks -
   storepass changeit
   Owner:CN=dept-CA, DC=domain.name
   Issuer:CN=dept-CA, DC=domain.name
   Serial number:2c2721eb293d60b4424fe82e37794d2c
   Valid from:Tue Jun 17 11:49:31 IDT 2008 until:Mon Jun 17 11:57:06 IDT 2013
   Certificate fingerprints:
   MD5:14:59:8F:47:00:E8:10:93:23:1C:C6:22:6F:A6:6C:5B
   SHA1:17:2F:4E:76:83:5F:03:BB:A4:B9:96:D4:80:E3:08:94:8C:D5:4A:D5
   Trust this certificate?[no]:yes
   Certificate was added to keystore
   ```

10. **运行以下命令，将客户端证书导入密钥库中:**

    keytool -import -alias sis -file
    <SiteScope 根目录>\templates.certificates\certnew.cer -keystore

<SiteScope 根目录>\templates.certificates\.ks -storepass
<您的密钥库密码>

示例:

keytool -import -alias sis -fil c:\SiteScope\templates.certificates\certnew.cer -keystore C:\SiteScope\templates.certificates\.ks -storepass changeit

证书回复安装在密钥库 **<SiteScope 根目录>\java\bin** 目录中。

11. 通过从 **<SiteScope 根目录>\java\bin** 目录运行以下命令来检查密钥库内容，并输入密钥库密码:

    keytool -list -keystore <SiteScope 根目录>\templates.certificates\.ks

    示例:

    keytool -list -keystore C:\SiteScope\templates.certificates\.ks
    Enter keystore password:changeit

    Keystore type:jks
    Keystore provider:SUN

    Your keystore contains 2 entries
    ca, Mar 8, 2009, trustedCertEntry,
    Certificate fingerprint (MD5):14:59:8F:47:00:E8:10:93:23:1C:C6:22:6F:A6:6C:5B
    sis, Mar 8, 2009, keyEntry,
    Certificate fingerprint (MD5):C7:70:8B:3C:2D:A9:48:EB:24:8A:46:77:B0:A3:42:E1

    C:\SiteScope\java\bin>

12. 要将此密钥库用于客户端证书，请将下列行添加到 **<SiteScope 根目录>\groups\master.config** 文件中:

    _urlClientCert=<密钥库名称>

    _urlClientCertPassword=<密钥库密码>

    示例:

    _urlClientCert=.ks
    _urlClientCertPassword=changeit

13. 保存文件更改。
14. 在 **SiteScope**“首选项”>“集成首选项”>“BSM 首选项可用操作”中，单击“重置”删除 SiteScope 服务器中的所有 BSM 相关设置以及 BSM 中的所有 SiteScope 配置。
15. 重新启动 SiteScope 服务器。
16. 在 BSM 中，选择“管理”>“管理系统可用性管理”，然后单击“新建 SiteScope”按钮来添加 SiteScope 实例。

    备注: 如果 SiteScope 和 BSM 之间的连接失败，请检查 **<SiteScope 根目录>\log\bac_integration.log** 中是否有错误。

当 BSM 服务器需要客户端证书时在 SiteScope 中配置拓扑搜寻代理

在使用客户端证书将 SiteScope 配置为与 BSM 网关服务器连接后（请参阅将 SiteScope 配置为连接到需要客户端证书的 BSM 服务器 (第 189 页)），需要执行以下步骤进行搜寻，以便将拓扑报告给 BSM 服务器。

1. **在 <SiteScope 根目录>\WEB-INF\classes 中创建一个名为 security 的文件夹（如果不存在该文件夹）。**
2. **将 MAMTrustStoreExp.jks 和 ssl.properties 从 <SiteScope 根目录>\WEB-INF\classes 移到 <SiteScope 根目录>\WEB-INF\classes\security 文件夹中。**
3. **使用密码将 CA 根证书（或 BSM 服务器证书）导入搜寻信任库 (MAMTrustStoreExp.jks)，搜寻信任库的默认密码为 logomania，该密码已加密，即：[22,-8,116,-119,-107,64,49,93,-69,57,-13,-123,-32,-114,-88,-61]:**

   keytool -import -alias <您的 CA> -keystore <SiteScope 根目录>\WEB-INF\classes\security\MAMTrustStoreExp.jks -storepass <您的密钥库密码>

   示例：

   keytool -import -alias AMQA_CA -file c:\ca.cer -keystore C:\SiteScope\WEB-INF\classes\security\MAMTrustStoreExp.jks -storepass logomania

   备注：私钥密码必须至少包含 6 个字符，并且私钥密码和密钥库的密码必须相同。

4. **使用以下命令检查信任库的内容：**

   <SiteScope 根目录>\java\bin>keytool -list -keystore <SiteScope 根目录>\WEB-INF\classes\security\MAMTrustStoreExp.jks -storepass <您的密钥库密码>
   Keystore type:<密钥库类型>
   Keystore provider:<密钥库提供商>
   Your keystore contains 2 entries mam, Nov 4, 2004, trustedCertEntry,Certificate fingerprint (MD5): <证书指纹> amqa_ca, Dec 30, 2010, trustedCertEntry,Certificate fingerprint (MD5): <证书指纹>

   示例：

   C:\SiteScope\java\bin>keytool -list -keystore C:\SiteScope\WEB-INF\classes\security\MAMTrustStoreExp.jks -storepass logomania

   Keystore type:JKS
   Keystore provider:SUN

   Your keystore contains 2 entries

   mam, Nov 4, 2004, trustedCertEntry,
   Certificate fingerprint (MD5):C6:78:0F:58:32:04:DF:87:5C:8C:60:BC:58:75:6E:F7

```
amqa_ca, Dec 30, 2010, trustedCertEntry,
Certificate fingerprint (MD5):5D:47:4B:52:14:66:9A:6A:0A:90:8F:6D:7A:94:76:AB
```

5. 将 SiteScope 客户端 keyStore (.ks) 从 **<SiteScope 根目录>\templates.certificates** 复制到 **<SiteScope 根目录>SiteScope\WEB-INF\classes\security** 中。
6. 在 **ssl.properties** 文件中，将 **javax.net.ssl.keyStore** 属性更新为 keyStore 名称。例如，javax.net.ssl.keyStore=.ks。
7. 更改 SiteScope 客户 keyStore 密码，以与密钥库的搜寻密码（默认值为 logomania ）匹配。

   keytool -storepasswd -new <搜寻密钥库密码> -keystore <SiteScope 根目录>\WEB-INF\classes\security\.ks -storepass <您的密钥库密码>

   示例：

   keytool -storepasswd -new logomania -keystore C:\SiteScope\WEB-INF\classes\security\.ks -storepass changeit

8. 更改私钥密码，以与密钥库的搜寻密码匹配：

   keytool -keypasswd -alias sis -keypass <您的密钥库密码> -new <搜寻密钥库密码> -keystore <SiteScope 根目录>\WEB-INF\classes\security\.ks -storepass <您的密钥库密码>

   示例：

   keytool -keypasswd -alias sis -keypass changeit -new logomania -keystore C:\SiteScope\WEB-INF\classes\security\.ks -storepass logomania

9. 使用新密码验证密钥库：

   keytool -list -v -keystore <SiteScope 根目录>\WEB-INF\classes\security\.ks -storepass <您的密钥库密码>

   示例：

   keytool -list -v -keystore C:\SiteScope\WEB-INF\classes\security\.ks -storepass logomania

10. 重新启动 SiteScope 服务器。
11. 在 BSM 中，选择“管理”>“管理系统可用性管理”，然后单击“新建 SiteScope”按钮来添加 SiteScope 实例。在“配置文件设置”窗格中，确保选中“BSM 前端使用 HTTPS”复选框。
12. 检查是否在“BSM”>“管理”>“**RTSM** 管理”>“IT 领域管理器”>“系统监控器”视图中显示了拓扑。

疑难解答

- 检查位于 **<SiteScope 根目录>\logs\bac_integration** 下的 **bac-integration.log** 中是否存在以下错误：

  ```
  2010-12-30 11:03:06,399 [TopologyReporterSender] (TopologyReporterSender.java:364)
  ```

```
 ERROR - failed to run main topology agent. topologyCommand=TopologyCommand
{commandType=RUN_SCRIPT, ···
java.lang.IllegalArgumentException:cannot find script with name=create_monitor.py
at com.mercury.sitescope.integrations.bac.topology.dependencies.DependenciesCrawler.
findDependencies(DependenciesCrawler.java:60)
at com.mercury.sitescope.integrations.bac.topology.dependencies.
ScriptDependenciesFinder.find(ScriptDependenciesFinder.java:80)
at com.mercury.sitescope.integrations.bac.topology.TopologyReporterSender.
getDependencies(TopologyReporterSender.java:552)
at com.mercury.sitescope.integrations.bac.topology.TopologyReporterSender.
send(TopologyReporterSender.java:347)
at com.mercury.sitescope.integrations.bac.topology.TopologyReporterSender.
run(TopologyReporterSender.java:304)
at java.lang.Thread.run(Thread.java:619)
```

- **验证证书和密钥库的密码是否相同。**

附录 D: 使用 HTTPS 访问 SiteScope 报告和经典用户界面

可将 SiteScope Web 服务器设置为通过 HTTPS 协议访问，以便使用 SSL 连接。本节描述了进行此操作需要执行的步骤。

本节包括以下内容:

关于在 SiteScope 中使用证书

SiteScope 附带了 **Keytool.exe**。Keytool 是一个密钥和证书管理实用程序。该实用程序允许用户管理自己的公/私钥对以及关联的证书，以便使用数据签名进行身份验证。同时，它还允许用户对与其通信方的公钥进行缓存操作。该实用程序安装在 **<SiteScope 安装路径>\SiteScope\java\bin** 目录下。

备注: 创建、请求和安装数字证书是一个需要注重细节的过程。请记录您在该过程的每个步骤中使用的参数和命令行参数，因为在整个过程中都使用相同的值是十分重要的。

您可以在 Sun Microsystems 网站中找到关于 Keytool 的更多信息:

http://java.sun.com/j2se/1.3/docs/tooldocs/win32/keytool.html

使用证书颁发机构的证书

可通过以下步骤使用证书颁发机构颁发的数字证书。要使用此选项，需要可导入 Keytool 所使用的密钥存储文件的数字证书。如果您的组织当前没有此类数字证书，则需要请求证书颁发机构为您颁发证书。

要使用证书颁发机构颁发的证书，请执行以下操作:

1. 删除 **<SiteScope 根目录>\groups** 目录中的 **serverKeystore** 文件。您可以将其删除，或者移动到其他目录。

   备注: 执行下列步骤前，必须删除此文件。

2. 接着，您必须创建密钥对。要执行此操作，需要从 **<SiteScope 根目录>\java\bin** 目录运行下面列出的命令行。

   备注: 以斜体表示的值是需要使用特定于组织的信息填写的变量。

   必须在一行中输入此命令和您所使用的其他命令。为了适于在此页面中显示，这里对行进行了划分。

keytool -genkey -dname "CN=www.yourDomain.com, OU=yourDepartment, O=yourCompanyName, L=yourLocation, S=yourState, C=yourCountryCode" -alias yourAlias -keypass keypass -keystore ..\..\groups\serverKeystore -storepass passphrase -keyalg "RSA" -validity valdays

此命令会在 **SiteScope\groups** 目录中创建一个名为 **serverKeystore** 的文件。SiteScope 会使用此密钥库文件存储安全会话中使用的证书。请确保在其他位置中保留此文件的备份。

-dname 选项值必须具有如下顺序，其中的斜体值将替换为您选择的值。关键字的缩写如下：

CN = commonName - 普通人名（如“Warren Pease”）

OU = organizationUnit - 小型组织单位（如“NetAdmin”）

O = organizationName - 大型组织名称（如“ACMe-Systems, Inc.”）

L = localityName - 地点（城市）名称（如“Palo Alto”）

S = stateName - 州名或省名（如“California”）

C = country - 国家/地区代码（两个字母，如“US”）

- **-dname**（可分辨名称字符串）变量中的子组件不区分大小写且具有顺序，但您不必包含所有子组件。-dname 变量表示公司，CN 是安装 SiteScope 的 Web 服务器的域名。
- -storepass 值是用于保护密钥库文件的密码。该密码必须至少包含 6 个字符。将证书数据导入密钥库文件和从密钥库文件中删除证书数据时需要使用此密码。
- -alias 变量是一个别名或昵称，用于标识密钥库中的条目。

3. 创建证书请求文件。要执行此操作，请从 **<SiteScope 根目录>\java\bin** 目录运行以下命令：

   keytool -certreq -alias yourAlias -file ..\..\groups\filename.csr -keypass keypass -keystore ..\..\groups\serverKeystore -storepass passphrase -keyalg "RSA"

   此命令将生成要用作请求文件的 .csr 文件。您需要将此文件以及证书请求发送至证书颁发机构 (CA)。接收到证书颁发机构颁发的证书后（回复中会包含一个名为 **cert.cer** 的文件），需要将此证书导入到上述步骤创建的密钥库文件中。该文件的名称应为 **serverKeystore**。可使用以下步骤导入证书。

4. 要将证书数据导入到密钥库文件中，请从 **SiteScope\java\bin** 目录运行以下命令：

   keytool -import -trustcacerts -alias yourAlias -file cert.cer -keystore ..\..\groups\serverKeystore

5. 要更改 SiteScope 以使用安全连接，需要在 **<SiteScope 根目录>\groups\master.config** 文件中添加或修改以下参数：

   _httpSecurePort=8899

   用于 **_httpSecurePort** 参数的数值可设置为任何可用的端口号。建议不要使用 8888 作为端口号，因为这是使用 HTTP（非安全）访问 SiteScope 的默认端口。

   如果希望只通过 HTTPS 访问 SiteScope，则需要按如下方式修改 **master.config** 文件中的以下参数。请将以斜体表示的项替换为适用的值：

   _httpPort=

   _httpSecurePort=8899

   _httpSecureKeyPassword=passphrase

   _httpSecureKeystorePassword=keypass

备注: master.config 文件中的所有参数均区分大小写并严格遵循语法。请确保不要向该文件添加任何额外的空格或行。

6. 保存对 **master.config** 文件的更改。
7. 停止并重新启动 SiteScope 服务，以使更改生效。

现在，您应当可以使用 HTTP 访问 SiteScope，例如从防火墙内以默认地址访问：

http://服务器 IP 地址:8888

您应当还可以基于以上示例的步骤，使用 HTTPS 通过以下地址来访问 SiteScope：

https://服务器 IP 地址:8899

使用自签名证书

此外，您还可以生成自签名证书。要完成该操作，请使用 -selfcert 选项让 Keytool 实用程序生成自签名证书。

要使用自签名证书，请执行以下操作：

1. 删除 **<SiteScope 根目录>\groups** 目录中的 **serverKeystore** 文件。您可以将其删除，或者移动到其他目录。

   备注: 执行下列步骤前，必须删除此文件。

2. 接着，请从 **<SiteScope 根目录>\java\bin** 目录运行以下命令。

   备注: 以斜体表示的值是需要使用特定于组织的信息填写的变量

   必须在一行中输入此命令和您所使用的其他命令。为了适于在此页面中显示，这里对行进行了划分。

   keytool -genkey -dname "CN=www.yourDomain.com, OU=yourDepartment, O=yourCompanyName, L=yourLocation, S=yourState, C=yourCountryCode" -alias yourAlias -keypass keypass -keystore ..\..\groups\serverKeystore -storepass passphrase -keyalg "RSA" -validity valdays

3. 接着，请仍然从 **SiteScope\java\bin** 目录运行以下命令：

   keytool -selfcert -alias yourAlias -sigalg "MD5withRSA" -keypass password -dname "CN=www.yourDomain.com, OU=yourDepartment, O=yourCompanyName, L=yourLocation, S=yourState, C=yourCountryCode" -keystore ..\..\groups\serverKeystore

4. 要更改 SiteScope 以使用安全连接，需要在 **<SiteScope 根目录>\groups\master.config** 文件中添加或修改以下参数：

   _httpSecurePort=8899

   用于 **_httpSecurePort** 参数的数值可设置为任何可用的端口号。建议不要使用 8888 作为端口号，因为这是使用 HTTP（非安全）访问 SiteScope 的默认端口。

   如果希望只通过 HTTPS 访问 SiteScope，则需要按如下方式修改 master.config 文件中的以下参数。请将以斜体表示的项替换为适用的值：

   _httpPort=

_httpSecurePort=8899

_httpSecureKeyPassword=passphrase

_httpSecureKeystorePassword=keypass

备注: master.config 文件中的所有参数均区分大小写并严格遵循语法。请确保不要向该文件添加任何额外的空格或行。

5. 保存对 **master.config** 文件的更改。
6. 停止并重新启动 SiteScope 服务，以使更改生效。

现在，您应当可以使用 HTTP 访问 SiteScope，例如从防火墙内以默认地址访问：

http://服务器 IP 地址:8888

您应当还可以基于以上示例的步骤，使用 HTTPS 通过以下地址来访问 SiteScope：

https://服务器 IP 地址:8899

发送文档反馈

如果对本文档有任何意见，可以通过电子邮件与文档团队联系。如果在此系统上配置了电子邮件客户端，请单击以上链接，此时将打开一个电子邮件窗口，主题行中为以下信息：

部署指南 (SiteScope 11.30) 反馈

只需在电子邮件中添加反馈并单击“发送”即可。

如果没有可用的电子邮件客户端，请将以上信息复制到 Web 邮件客户端的新邮件中，然后将您的反馈发送至 SW-doc@hp.com。

我们感谢您提出宝贵的意见！