HITACHI
Inspire the Next

Hitachi IT Operations Analyzer

入门指南：设备配置补充

快速查找链接

Hitachi Data Systems

MK-90IOS006SC-12

目录

前言

本指南是对《Hitachi IT Operations Analyzer 入门指南》的补充。它将协助您完成在工作场所希望监控的网络组件的预安装设置任务。

本前言包含以下信息：

适合的读者

本文档专供系统管理员以及负责配置和操作 Hitachi IT Operations Analyzer 的其他用户使用。

产品版本

本文档修订版适用于 IT Operations Analyzer 版本 3.3.1。

文档修订级别

本节提供了本文档的修订历史记录。

修订版	日期	描述
MK-90IOS006SC-00	2010 年 3 月	初版
MK-90IOS006SC-01	2010 年 10 月	修订版 1，用于取代 MK-90IOS006SC-00
MK-90IOS006SC-02	2011 年 4 月	修订版 2，用于取代 MK-90IOS006SC-01
MK-90IOS006SC-03	2012 年 1 月	修订版 3，用于取代 MK-90IOS006SC-02
MK-90IOS006SC-04	2013 年 3 月	修订版 4，用于取代 MK-90IOS006SC-03
MK-90IOS006SC-12	2013 年 7 月	修订版 12，用于取代 MK-90IOS006SC-04

相关文档

- *Hitachi IT Operations Analyzer 入门指南：设备配置补充，*MK-90IOS006
- Hitachi IT Operations Analyzer 帮助
- 发行通告，RN-99IOS004

文档惯例

以下符号用于提示重要信息。

符号	含意	描述
	提示	“提示”提供了有助于您更有效地执行任务的信息、指导或建议。
	注释	“注释”强调或补充了正文中的要点。

本文档中使用了以下印刷惯例。

惯例	描述
粗体	表示窗口中除窗口标题之外的文本，包括菜单、菜单选项、按钮、字段和标签。例如单击**确定**。
斜体	表示作为占位符的变量，代表由用户或系统提供的实际文本。如果是版本信息，则斜体 x 代表所有后续版本。例如： • 复制 *source-file target-file*。 • 内核版本 2.6.*x*。 **注**：尖括号 (< >) 也用于表示变量。
屏幕 / 代码	表示显示在屏幕上或由用户输入的文本。例如 `# pairdisplay -g oradb`
尖括号	表示作为占位符的变量，代表由用户或系统提供的实际文本。 例如 `# pairdisplay -g` < 组 > **注**：斜体字体也用于表示变量。

产品引用

在本手册中引用了 VMware® 产品。此类引用的处理方法如下：

- 在类型 / 版本明确的情况下引用产品：VMware ESX 3、VMware ESX 3i、VMware ESX 4.0 等。
- 在服务器类型 / 版本不明确的情况下引用产品服务器：ESX 服务器。

获取帮助

如果您已购买本产品并拥有当前产品支持协议，请收集以下信息：

- 产品名称和版本号
- 操作系统名称以及版本或服务包编号
- 您请求帮助所针对的许可序列号
- 显示的任何错误消息内容
- 出现错误或故障的环境
- 对问题的描述以及已尝试的纠正措施

收集此数据之后，请联系 Hitachi Data Systems 支持中心。

以下是 Hitachi Data Systems 网站的链接，您可以在其中获得 Hitachi Data Systems 支持中心的最新电话号码和其它联系信息：

https://portal.hds.com

注：如果您正在使用产品的试用版，请参阅 IT Operations 软件门户上的自助式材料：http://www.itoperations.com

意见

对本文档如有意见，请发送给我们：doc.comments@hds.com。请附上文档标题、编号和修订版，并尽可能指明章节和段落。

非常感谢！（所有意见均将成为 Hitachi Data Systems Corporation 的财产。）

1

概述

在安装IT Operations Analyzer或使用“发现向导”之前，切记检查和准备您的环境。这涉及验证在您的环境中使用的设置，并且在设置过程中收集以后需要使用的信息。

- 准备好您的环境

准备好您的环境

表 1-1 介绍了必要的任务以及建议或可选的任务，具体取决于您的环境和监控目的。

对于每项任务，都有引用包含详情的章节。

表 1-1：环境准备

必要任务	
任务	**详情**
在管理服务器上（IT Operations Analyzer 安装所在的机器），检查 WMI 的 DCOM 设置。	防止由于不允许远程执行 DCOM 而出现 WMI 远程连接错误。 请参阅第 2 章，准备将 WMI 用于 Windows 服务器。
如果您的工作场所使用以下任何监控目标，则必须对其进行设置： • IP 交换机	监控目标是您的工作场所希望监控的服务器、存储设备和交换机。 IT Operations Analyzer 使用 SNMP 来监控 IP 交换机。 • 启用 SNMP • 获取 SNMP 社区字符串 • 获取 IP 地址 请参阅第 5 章，准备将 SNMP 用于 IP 交换机。
• Hitachi 9500V	IT Operations Analyzer 通过设备管理器的 SMI-S 代理来监控 Hitachi 9500V。不会对性能进行监控。安装设备管理器 5.9 或更高版本并启用 SMI-S。 请参阅第 6 章，准备 Hitachi 存储设备。
• Hitachi USP VM	IT Operations Analyzer通过设备管理器的SMI-S Agent代理来监控Hitachi USP VM。安装设备管理器 6.2 或更高版本并启用 SMI-S。请参阅第 6 章，准备 Hitachi 存储设备。

• 其它存储设备、FC 交换机	IT Operations Analyzer使用SMI-S来发现和监控其它存储设备和FC交换机。安装 SMI-S 代理，然后获取以下信息：
	• IP 地址
	  • SMI-S 代理 (proxy)：将 SMI-S 服务器的 IP 地址用于交换机。
	  • SMI-S 代理 (嵌入式)：将相同的 IP 地址用于 FC 交换机。
	• 用户 ID 和密码
	• 端口号
	• 名称空间
	此外，请检查 SSL 状态。
	请参阅第 7 章，复查 SMI-S 准备。
	在为 NetApp FAS 系列指定凭证或使用 SMI-S 代理管理 Linux 版本时，我们建议您在**添加凭证**对话框中为 **SSL** 指定 **http**。

表 1-1：环境准备

建议的任务	
任务	**详情**
检查监控目标： • Windows 服务器	IT Operations Analyzer 使用 WMI 来监控 Windows 服务器。对于远程访问 WMI，必须在 Windows 服务器和管理服务器上启用 DCOM。如果不启用 DCOM，软件可能无法发现或监控 Windows 服务器。 同时，如果您的工作场所将监控Hyper-V虚拟机，也要在虚拟机上安装“集成服务”。 请参阅第 2 章，准备将 WMI 用于 Windows 服务器。
• Linux/Solaris 服务器	IT Operations Analyzer 使用 SSH 来发现 Linux 和 Solaris 服务器。它还使用密码验证（不是证书验证）来监控这些服务器。验证： • SSH 服务已安装并正在运行。 • SSH2 连接已启用。 • 允许使用密码验证。 请参阅第 3 章，准备将 SSH 用于 Linux/Solaris 服务器。
• VMware ESX 服务器	如果不安装 VMware 工具，IT Operations Analyzer 将无法在虚拟机上正确地监控 Windows 或 Linux 服务器。验证支持的版本： • VMware ESX 3 • VMware ESX 3.5 • VMware ESX 3i • VMware ESX 3.5i • VMware ESX 4 • VMware ESX 4i • VMware ESX 4.1 • VMware ESX 4.1i • VMware ESX 5 • VMware ESX 5i • VMware ESX 5.1 • VMware ESX 5.1i 此外，在虚拟机上安装 VMware 工具。请参阅第 4 章，准备 VMWare ESX 服务器。
• Hitachi AMS/WMS/SMS 系列和 Hitachi Unified Storage 系列	检查是否已启用了帐户验证或密码保护。如果已启用帐户验证或密码保护，则 IT Operations Analyzer 需要用户 ID 和密码。 请参阅第 6 章，准备 Hitachi 存储设备。
• Dell 服务器	使用内置 Dell Chassis 插件，您可以获取 Dell 服务器特定的信息。“Dell Chassis (Windows)”作为Windows的插件安装，“Dell Chassis (Linux)”作为 Linux 的插件安装。以下是 IT Operations Analyzer 监控的 Dell 服务器的系统要求： • 受监控Dell服务器必须正在运行Dell OpenManage Server Administrator (OMSA) 版本 6.1.0 或 6.2.0。 • 受监控 Dell 服务器上已安装 SNMP 代理且正在运行该代理。 • “Dell Chassis (Windows)”要求 Microsoft Windows Server 上正在运行 DSM SA Data Manager 服务。 • “Dell Chassis (Linux)”要求 Red Hat Enterprise Linux Server 上正在运行 dsm_sa_datamgrd 或 dsm_sa_datamgr32d 进程。 有关基于Linux和基于Windows的Dell服务器的操作系统要求，请参阅Linux服务器和 Microsoft Windows 服务器设置任务。

表 1-1：环境准备

可选任务	
任务	**详情**
检查监控目标： • Windows 服务器	IT Operations Analyzer 使用 WMI 来监控 Windows 服务器。Windows 2003 必须安装 FCInfo，才能通过 WMI 提供 FC HBA 数据。 如果您的 Windows 服务器使用 FC HBA，则安装 FCInfo。 请参阅第 2 章，准备将 WMI 用于 Windows 服务器。
• IP 交换机	启用 SNMP 陷阱发送。IT Operations Analyzer 可以接收来自 IP 交换机的 SNMP陷阱。这是可选任务，因为在没有陷阱的情况下，IT Operations Analyzer 可以通过轮询来监控IP交换机。请参阅第 5章，准备将SNMP用于IP交换机。

2

准备将 Hyper-V 和 WMI 用于 Windows 服务器

IT Operations Analyzer 使用 WMI 来监控 Windows 服务器。对于远程访问 WMI，必须在 Windows 服务器和管理服务器上启用 DCOM。如果不启用 DCOM，软件可能无法发现或监控 Windows 服务器。本章介绍了 Hyper-V 和 WMI 环境准备。

- 准备 Hyper-V
- 准备将 WMI 用于 Windows 服务器

准备 Hyper-V

如果您的工作场所计划监控安装在 Hyper-V 虚拟机上的 Windows 或 Linux 服务器，则您需要在虚拟机的OS上安装“集成服务”。否则，如果未安装“集成服务”，虚拟机的状态和主机与 guest OS 之间的关系均无法在 IT Operations Analyzer 中正确显示。

注：Hyper-V 主机设置类似于准备 Windows 服务器。有关参考信息，请参阅下面的下一个小节。
此外，对于管理目标的主机操作系统，如果未将 KB2264080 应用到 Windows Server 2008 R2，则在以下情况下无法连接到管理目标 Hyper-V 的客户机操作系统：
- Hyper-V 的虚拟机上有很多会话时。
- 向 Hyper-V 的虚拟机传输大量数据时。

准备将 WMI 用于 Windows 服务器

IT Operations Analyzer 通过 Windows 管理规范 (WMI) 来发现和监控 Windows 服务器。以下小节介绍了与启用 WMI 远程访问以及对使用 FC 主机总线适配器 (HBA) 的 Windows 2003/2003 R2 服务器进行配置相关联的任务。

注：

- 对于 Microsoft Hyper-V 节点和 Windows 服务器节点，您可通过 FC 连接、iSCSI 连接和本地连接获取有关硬盘的性能信息。无法获取有关 CD-ROM 驱动器或 USB 存储器的性能信息。如果无法获取性能信息，则在**监控**模块的**性能**选项卡中，性能指标的图标会指示 “未知”。
- 对于 Windows Server 2003，请应用 KB953955。否则，为 CPU 名称报告的值可能不正确。

准备管理服务器

要监控 Windows 计算机或存储服务器，必须在管理服务器上启用 DCOM。请参阅第 2-4 页上的允许远程执行 DCOM。

准备 Windows 计算机和 Windows 存储服务器

表 2-1 列出了监控所需的信息。

表 2-1：关于连接至 Windows 服务器的信息

项目	详情
IP 地址	要监控的 Windows 服务器的 IP 地址。
用户名	对要监控的 Windows 服务器具有管理员权限的用户帐户。
域名	用户的域名（如果以上所述的用户帐户是域用户）。
密码	与用户名相关联的密码。

要监控Windows服务器，DCOM必须进行验证，且任何WMI异常都必须添加至Windows防火墙。如果您计划使用 Windows Server 2003 或 2003 Windows Server R2 获取 FC HBA 信息，请安装光纤信道信息工具 (fcinfo)。

安装光纤信道信息工具 (fcinfo)

在使用主机总线适配器 (HBA) 将光纤信道 SAN 磁盘设备连接至您要监控的服务器时，需要使用 fcinfo 工具。它支持 Windows 中的光纤信道 HBA API，并且提供了符合 WMI 标准的功能。请参见 Microsoft 下载中心网站：
http://www.microsoft.com/downloads/details.aspx?FamilyID=73d7b879-55b2-4629-8734-b0698096d3b1&displaylang=en

将 WMI 异常添加到 Windows 防火墙

您可以通过 Windows 命令提示或使用组策略编辑器来更改权限。以下指示适用于 Windows Server 2003。如需 Windows Server 2008 或 Windows Server 2012 的详情，请参阅第2-4页上的应用Windows Server 2008或Windows Server 2012配置设置。

使用 Windows 命令提示符：

1. 登录到服务器之后，单击**开始**，然后单击**运行**。

注：在 Windows Server 2012 上，导航至**开始**和**运行**命令的步骤不同。

2. 在提示下键入 **cmd**，然后单击**“确定”**。
3. 在命令提示符下键入以下命令，然后按 **Enter** 键：

```
netsh firewall set service RemoteAdmin enable
```

使用组策略编辑器：

1. 登录到服务器之后，单击**开始**，然后单击**运行**。

注：在 Windows Server 2012 上，导航至**开始**和**运行**命令的步骤不同。

2. 要启动**组策略**编辑器，请键入 **gpedit.msc**，然后单击**确定**。
3. 在**本地计算机策略**中，展开**管理模板**文件夹。
4. 展开以下文件夹：**“网络”**、**“网络连接”**和**“Windows 防火墙”**，然后选择**“域配置文件”**。
5. 在设置列表中，右键单击 **Windows 防火墙：允许远程管理异常**，然后单击**属性**。
6. 单击**启用**，然后单击**确定**。

注：有关详情，请参见 Microsoft 开发中心网站：
http://msdn2.microsoft.com/en-us/library/aa389286(VS.85).aspx

允许远程执行 DCOM

通过在Windows命令提示下执行dcomcnfg.exe，您可以启动“组件服务”面板并确认 DCOM 状态。

1. 登录到服务器之后，单击**开始**，然后单击**运行**。

注：在 Windows Server 2012 上，导航至**开始**和**运行**命令的步骤不同。

2. 要启动**组件服务**，请键入 **dcomcnfg.exe**，然后单击**确定**。
3. 从**组件服务**中选择**计算机**，然后选择**我的电脑**。
4. 右键单击**我的电脑**，然后选择**属性**。
5. 单击**默认属性**选项卡。
6. 选中**在本机上启用分布式 COM** 框，然后单击 **COM 安全性**选项卡。
7. 要显示**启动权限**对话框，请单击**编辑限制**以用于**启动和激活权限**。如果**组或用户名**框中未显示用户名或组，则执行以下操作：
   a. 单击**添加**。
   b. 在**选择用户、计算机或组**对话框中，将用户名和组添加到**输入对象名称以便选择**框中。单击**确定**。
   c. 在**启动权限**对话框中，单击**组或用户名**区域中的用户和组。在**用户的权限**区域中，对于**远程启动**，请选中**允许**列中的框。单击**确定**。

应用 Windows Server 2008 或 Windows Server 2012 配置设置

如果您正在使用 Windows Server 2008 或 Windows Server 2012，则除了前面部分中所述的 Windows 服务器设置之外，还需要满足以下任意一项条件：

- 使用内置管理员帐户
- 使用域用户帐户
- 使用本地管理员帐户启用 WMI 远程连接

启用本地管理员帐户以进行 WMI 远程连接

您可以从监控目标计算机的控制面板中，或通过从注册表中应用设置方法来更改用户帐户控制 (UAC) 设置。

要从控制面板中更改 UAC：

1. 在**开始**菜单中，单击**控制面板**。

注：在 Windows Server 2012 上，导航至**开始**菜单的步骤不同。

2. 选择**用户帐户**，然后选择**更改用户帐户控制设置**。
3. 将 UAC 级别设为**从不通知**。
4. 重新启动计算机。

另一种监控目标计算机的方法是：在监控目标计算机的注册表中注册 **LocalAccountTokenFilterPolicy** 项，并将其最大值设为 **1**。之后禁用**按 UAC 过滤**，这样可以防止在 WMI 远程连接期间使用本地管理员权限。

通过使用本地管理员帐户，您可以管理 Windows Server 2003 和 Windows Server 2008 或 Windows Server 2012。如果编辑注册表，则可能会出现严重错误，并对整个系统造成严重影响。我们建议您在编辑之前备份注册表。

有关详情请参阅以下URL，它提供了关于Windows Vista中UAC和远程限制的描述：
http://support.microsoft.com/kb/951016/en-us

在配置注册表时，请使用：

- 注册表编辑器，或者
- “reg”命令

使用注册表编辑器：

1. 单击**开始**，然后单击**运行**。

注：在 Windows Server 2012 上，导航至**开始**和**运行**命令的步骤不同。

2. 在提示符下键入 **regedit**，然后单击**确定**。

   注册表编辑器将会显示。
3. 找到以下注册表子键：

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\ 系统
4. 如果 **LocalAccountTokenFilterPolicy** 键不存在，则添加此键：
   a. 从**编辑**菜单中选择**新建**，然后选择 **DWORD**。
   b. 键入 **LocalAccountTokenFilterPolicy**，然后按 **Enter** 键。
5. 如果 **LocalAccountTokenFilterPolicy** 的值不是 **1**，则将其更改为 **1**：
   a. 右键单击 **LocalAccountTokenFilterPolicy**，然后选择**修改**。
   b. 在输入对话框中键入 **1**，然后单击**确定**。
6. 关闭**注册表编辑器**。

使用 reg 命令：

1. 单击**开始**，然后单击**运行**。

注：在 Windows Server 2012 上，导航至**开始**和**运行**命令的步骤不同。

2. 在提示下键入以下命令：

   reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v LocalAccountTokenFilterPolicy /t REG_DWORD /d 0x1 /f
3. 单击**确定**。

检查设备管理器节点树中是否存在重复的网络适配器名称

如果管理器节点树中存在重复的网络适配器名称，IT Operations Analyzer 将无法正确显示以下性能信息：

- 网络平均数据包接收量 [数据包 / 秒]
- 网络平均数据包发送量 [数据包 / 秒]。

要检查管理器中是否存在重复的网络适配器名称：

1. 单击**“开始”** > **“我的电脑”** > **“查看系统信息”** 。将会显示**系统属性**弹出菜单。

注：在 Windows Server 2012 上，导航至**开始**菜单的步骤不同。

2. 单击**硬件**选项卡。
3. 单击**设备管理器**。
4. 检查**“设备管理器”**树的**“网络适配器”**部分中是否出现重复的名称。

注：如果列出了重复的网络适配器名称，您将无法查看精确的网络平均数据包发送量 [数据包 / 秒] 性能信息。实际值和显示的性能信息之间有差异。建议您与 IT 服务组确认如何重命名网络适配器设备，以避免任何重复。

3

准备将 SSH 用于 Linux/Solaris 服务器

IT Operations Analyzer 使用 SSH 来发现 Linux 和 Solaris 服务器。它还使用密码验证（不是证书验证）来监控这些服务器。本章介绍了如何配置您的 Linux 和 Solaris 服务器。

- 安装所需的程序包
- 获取基于登录方法的连接设置
- 应用 SSH 服务器安全设置

安装所需的程序包

对于 CentOS，必须安装必要的软件包。

表 3-1：为 CentOS 添加的示例软件包

软件包	命令包含在 IT Operations Analyzer 执行的软件包中
smartmontools	/usr/sbin/smartctl
nfs-utils	/usr/sbin/exportfs
pciutils	/sbin/lspci
iscsi-initiator-utils	/sbin/iscsid

对于 SUSE Linux 11 SP1 和 SP2，必须安装必要的软件包。

表 3-2：为 SUSE Linux 11 SP1 和 SP2 添加的示例软件包

软件包	命令包含在 IT Operations Analyzer 执行的软件包中
nfs-kernel-server	/usr/sbin/exportfs

获取基于登录方法的连接设置

使用 SSH 有不同的登录方法，可以获取来自 Linux 或 Solaris 服务器的信息：

- 如果是**根用户**，您可以直接使用 SSH 登录
- 如果是**正常用户**，则在使用 SSH 登录之后运行：
  - 用于根用户权限的 `su` 命令。
  - 用于根用户权限的 `sudo/pfexec` 命令。

对于每种登录方法，都需要某些连接设置。以下小节中介绍了这些设置。

注：对于 Linux/Solaris 节点，可以通过读 / 写权限来获取有关装载点的性能信息。不能通过读权限来获取有关 Windows 分区和 CD-ROM 驱动器的性能信息。如果无法获取性能信息，则在**监控**模块的**性能**选项卡中，性能指标的图标会指示 “未知”。

用于根用户连接方法的设置

需要以下配置：

- 启用 SSH2 连接
- 允许 SSH 密码验证
- 允许使用 SSH 进行根用户登录

表 3-3：Linux/Solaris 服务器连接设置（根用户）

设置	详情
IP 地址	指定要监控的 Linux/Solaris 服务器的 IP 地址。
端口号	指定要监控的 Linux/Solaris 服务器的 SSH 端口号。
用户名	指定根用户。
密码	指定根用户密码。
根用户密码	指定空白。

用于正常用户连接方法的设置（su 命令）

需要以下配置：

- 启用 SSH2 连接
- 允许 SSH 密码验证

表 3-4：Linux/Solaris 服务器连接设置（su 命令）

设置	详情
IP 地址	指定要监控的 Linux/Solaris 服务器的 IP 地址。
端口号	指定要监控的 Linux/Solaris 服务器的 SSH 端口号。
用户名	指定用于登录的用户 ID。
密码	指定与用户 ID 相关联的密码。
根用户密码	指定根用户密码。

用于正常用户连接方法的设置（sudo 命令）

需要以下配置：

- 启用 SSH2 连接
- 允许 SSH 密码验证
- 添加 sudo/pfexec 设置的定义。有关详情，请参阅第 3-6 页上的添加 sudo 设置定义 (Linux)。
- 为配置文件 (Solaris) 添加定义。有关详情，请参阅第 3-8 页上的添加用于 pfexec 的配置文件 (Solaris)。

表 3-5：Linux/Solaris 服务器连接设置（sudo 命令）

设置	详情
IP 地址	指定要监控的 Linux/Solaris 服务器的 IP 地址。
端口号	指定要监控的 Linux/Solaris 服务器的 SSH 端口号。
用户名	指定用于登录的用户 ID。
密码	指定与用户 ID 相关联的密码。
根用户密码	指定空白。

注：以下是在使用 SSH 时需要考虑的一些安全事项：

- 允许根用户登录是最简单的配置方法；但是一旦泄露了根用户密码，就会导致服务器设置被篡改。只有在环境可以防止擅自访问时，才应允许使用此方法。
- 允许正常用户执行 `su` 根用户登录并禁止根用户登录比允许根用户登录更为安全，除非泄露正常用户的 ID 和密码。
- SSH1 协议的泄密风险要高于 SSH2 协议，因此建议使用 SSH2 协议。
- 允许密码验证时，比仅允许公钥验证更易受攻击。由于 IT Operations Analyzer 无法处理公钥验证，因此使用端口 22 之外的其它端口比使用密码验证更为安全。

应用 SSH 服务器安全设置

本节提供了以下指示：

- 启用 SSH2 连接
- 允许 SSH 密码验证
- 允许使用 SSH 进行根用户登录
- 添加 sudo 设置定义 (Linux)
- 添加用于 pfexec 的配置文件 (Solaris)

开始之前

- 验证 SSH 服务（sshd 后台程序）是否已安装并正在运行。
- 如果您使用其它SSH软件，请参阅软件手册并配置相当的设置。Linux包含OpenSSH。
- 准备好环境，以便能够登录到监控目标服务器并操作系统 shell。
- 从服务器控制台登录，或者使用 SSH 或 telnet 远程登录。我们建议通过本地控制台登录，从而在配置设置存在错误时防止重新连接失败。
- 准备根用户密码（需要根用户权限）。
- 在作为根用户或正常用户登录之后，通过使用 `su` 根用户命令来获取根用户权限。

启用 SSH2 连接

1. 使用编辑器打开 **/etc/ssh/sshd_config**。
2. 在 **sshd_config** 中，使用关键字 **Protocol** 搜索文件。
   - 如果没有描述或 **Protocol** 没有注解，则会启用 SSH1 和 SSH2。不需要进行更改。
   - 如果找到**Protocol 1**，则只会启用SSH1。将**Protocol 1**更改为**Protocol 1, 2**。
   - 如果找到 **Protocol 2**，则只会启用 SSH2。不需要进行更改。
   - 如果找到**Protocol 1, 2**或**Protocol 2, 1**，则会同时启用SSH1和SSH2。不需要进行更改。

3. 保存文件，然后关闭编辑器。要检查设置中是否有任何错误，请运行相应的命令：

   Linux：`/usr/sbin/sshd -t`

   Solaris：`/usr/lib/ssh/sshd -t`

   - 如果语法或范围中没有错误，则不会显示任何内容。
   - 如果语法或范围中存在错误，则会显示一则错误消息。

   错误的 Protocol (Protocol 2, 3) 设置实例：

   ```
   [root@linuxhost ssh]# /usr/sbin/sshd -t
   ignoring bad proto spec: '3'.
   ```

4. 执行相应的命令以重新启动 SSH 服务：
   - Linux：`service sshd restart`
   - Solaris 9：`/etc/init.d/sshd restart`
   - Solaris 10：`svcadm restart ssh`
5. 对于用于**停止 / 启动**，如果显示**确定**，则表示服务运行正常；
   例如：`Stopping sshd: [ OK ]`

允许 SSH 密码验证

注：有关编辑 **/etc/ssh/sshd_config** 并重新启动 SSH 服务的信息，请参阅上一节启用 SSH2 连接。

在**/etc/ssh/sshd_config**中，使用关键字**PasswordAuthentication**搜索文件。

- 如果没有描述或 **PasswordAuthentication** 没有注解，则会启用密码验证。不需要进行更改。
- 如果找到 **PasswordAuthentication no**，则会禁止密码验证（只会启用公钥验证）。将其更改为 **PasswordAuthentication yes**。
- 如果找到**PasswordAuthentication yes**，则表示允许密码验证。不需要进行更改。

允许使用 SSH 进行根用户登录

注：有关编辑 **/etc/ssh/sshd_config** 并重新启动 SSH 服务的信息，请参阅上一节启用 SSH2 连接。

在 **/etc/ssh/sshd_config** 中，使用关键字 **PermitRootLogin** 搜索文件。

- 如果没有描述或 **PermitRootLogin** 没有注解，则会默认启用根用户登录。不需要进行更改。
- 如果找到 **PermitRootLogin no**，则表示禁止根用户登录（只允许正常用户登录）。将其更改为 **PermitRootLogin yes**。
- 如果找到 **PermitRootLogin yes**，则允许根用户登录。不需要进行更改。

添加 sudo 设置定义 (Linux)

sudo 设置在 **/etc/sudoers** 文件中描述。只能使用 **visudo** 命令来编辑文件，因为它提供了排他控制和语法检查。

1. 运行 **visudo** 命令。如果它正常启动，则会打开一个编辑器。

注：如果在不同的地方同时执行 **visudo**，则会显示一则错误消息，并且编辑器不会启动：

```
[root@linuxhost ssh]# visudo
visudo: sudoers file busy, try again later
```

如果显示错误消息但命令未同时运行，则表示在之前执行命令时连接可能已终止，但是进程仍在运行中。在此情况下，请结束 **visudo** 进程。

2. 添加几行内容，以允许用户在不使用密码的情况下运行命令。

RedHat Linux 5.x:

```
/usr/sbin/dmidecode
/usr/sbin/smartctl
/sbin/ethtool
```

RedHat Linux 6.x:

```
/usr/sbin/dmidecode
/usr/sbin/smartctl
/sbin/ethtool
/usr/sbin/exportfs
```

SUSE Linux 10:

```
/usr/sbin/dmidecode
/usr/sbin/smartctl
/bin/cat
/usr/sbin/ethtool
```

SUSE Linux 11:

```
/usr/sbin/dmidecode
/usr/sbin/smartctl
/bin/cat
/sbin/ethtool
```

SUSE Linux 11 SP1 和 SP2：

```
/usr/sbin/dmidecode
/usr/sbin/smartctl
/bin/cat
/sbin/ethtool
/usr/sbin/exportfs
```

CentOS 和 Oracle Linux 6.x：

```
/usr/sbin/dmidecode

/usr/sbin/smartctl

/sbin/ethtool

/usr/sbin/exportfs
```

例如，如果用于连接的用户名是**sshconn**，并且适用的服务器名称是**linuxhost**，则将以下脚本指定为 SUSE Linux 11 的 /etc/sudoers：

```
sshconn linuxhost=NOPASSWD: /usr/sbin/dmidecode

sshconn linuxhost=NOPASSWD: /usr/sbin/smartctl

sshconn linuxhost=NOPASSWD: /bin/cat

sshconn linuxhost=NOPASSWD: /sbin/ethtool
```

3. 保存文件，然后关闭编辑器。

   如果存在语法错误，则会显示一则错误消息，并且保存将会延迟。

   - 在输入 **e** 时，编辑器将再次启动。对其进行修改，然后保存更改。
   - 在输入 **x** 时，更改将被放弃，并且您可以转回到运行 visudo 之前的状态。
   - 在输入 **Q** 时，将会强制保存更改（即使不正确）。例如，如果您在键入 NOPASSWD 时出错，则会显示以下错误消息：

     ```
     Warning: undeclared Cmnd_Alias `NOOPASSWD' referenced
     near line 92
     >>> sudoers file: syntax error? line 91 <<<
     What now?
     ```

注：在强制保存您可能并不熟悉其结果的更改时，应该特别小心。如果不能确定结果，请勿强制应用更改。

添加用于 pfexec 的配置文件 (Solaris)

要通过使用pfexec来添加根用户授权，请将配置文件添加至**/etc/security/prof_attr**和 **/etc/security/exec_attr**，然后将配置文件分配给用户。

1. 运行 `vi /etc/security/prof_attr`。
   - 如果它正确启动，则编辑器将会打开。
   - 如果显示错误消息，但是同时未执行命令，则可能是在之前运行命令时提早结束了连接，从而导致进程保留下来。在此情况下，请结束 **vi** 进程。
2. 注册配置文件。例如，如果配置文件名称设置为 HITOA，则会表示为：**HITOA::::**
3. 保存文件，然后退出编辑器。
4. 运行 `vi /etc/security/exec_attr`。如果它正确启动，则编辑器将会打开。
5. 添加以下四行，以便在不输入命令的情况下运行命令：

   ```
   /sbin/ifconfig
   /usr/sbin/prtvtoc
   /usr/sbin/luxadm
   /usr/sbin/iscsiadm
   ```

   例如，如果配置文件名称设置为 **HITOA**，则描述将如下所示：

   ```
   HITOA:suser:cmd:::/sbin/ifconfig:euid=0
   HITOA:suser:cmd:::/usr/sbin/prtvtoc:euid=0
   HITOA:suser:cmd:::/usr/sbin/luxadm:euid=0
   HITOA:suser:cmd:::/usr/sbin/iscsiadm:euid=0
   ```

6. 保存文件，然后退出编辑器。
7. 将配置文件分配给用户。例如，如果用户名已设置为 **sshconn**，则应该使用以下命令：

   ```
   usermod –P HITOA sshconn
   ```

4

准备 VMWare ESX 服务器

如果不安装 VMware 工具，IT Operations Analyzer 将无法在虚拟机上正确地监控 Windows 或 Linux 服务器。本章介绍了如何准备您的 ESX 服务器。

- 获取 ESX 服务器连接信息
- 在虚拟机上安装 VMware 工具

获取 ESX 服务器连接信息

下表介绍了在连接至 ESX 服务器时需要的信息。请注意，在发现进程中不需要附加凭证（只需要用户名和密码信息，如表 4-1 中所述）。

表 4-1：关于连接至 VMware ESX 服务器的信息

项目	详情
IP 地址	使用 ESX 服务器的 IP 地址。
端口号	指定 ESX 服务器所使用的端口号。
协议	根据 ESX 服务器的配置，使用 http 或 https。
用户名	使用 ESX 服务器的管理员用户名。
密码	使用 ESX 服务器的密码。

在虚拟机上安装 VMware 工具

如果您计划监控 Windows 服务器或 Linux 服务器虚拟机，则必须在虚拟机的每个 Guest OS 上安装 VMWare 工具，以便获取来自 ESX 服务器的信息。

如果未安装 VMWare 工具，虚拟机的状态和主机与 guest OS 之间的关系均无法正确显示。

请注意，Guest OS 作为单个节点进行管理。

有关这些工具的安装信息，请参阅 ESX 服务器产品手册《*基本系统管理*》，此手册可从以下网站中获得：
http://www.vmware.com/pdf/vi3_35/esx_3/r35u2/vi3_35_25_u2_admin_guide.pdf

当免费版本的 ESX 确定用于管理时，IT Operations Analyzer 可能无法精确获取磁盘的状态。

注：对于充当已启用分布式虚拟交换机的 VMware ESX 服务器，IT Operations Analyzer 不支持对其进行监控。但是，当 IT Operations Analyzer 按计划重新收集或更新已启用分布式虚拟交换机的配置信息时，系统将报告属于分布式虚拟交换机和服务控制台 NIC 的 VM 内核 NIC 的所有更改事件信息。

5

准备将 SNMP 用于 IP 交换机

IT Operations Analyzer 可以接收来自 IP 交换机的 SNMP 陷阱。本章介绍了如何配置您的 IP 交换机。

概述

IT Operations Analyzer 可以监控环境中的 IP 交换机，只要其设置如下：

- SNMP 版本 1 已安装并正在运行。
- MIB-II 可以使用您的社区名称来读取。
- Bridge MIB 可以使用您的社区名称来读取。

要监控 IP 交换机，需要表 5-1 和表 5-2 中概述的信息。

表 5-1：关于连接至 IP 交换机的信息：SNMP 版本 1 或 2c

项目	详情
IP 地址	SNMP IP 交换机节点的地址。
端口号	SNMP IP 交换机等待通信所在的端口（端口 161）。
社区名称	用于 SNMP IP 交换机的社区名称。

表 5-2：关于连接至 IP 交换机的信息：SNMP 版本 3

项目	详情
IP 地址	SNMP IP 交换机节点的地址。
端口号	SNMP IP 交换机等待通信所在的端口（端口 161）。
用户名	用于 SNMP IP 交换机的用户名。
安全级别	用于 SNMPv3 中通信的安全级别。选项：noAuthNoPriv、authNoPriv、authPriv
验证方法	用于 SNMPv3 中通信的验证方法。选项，可以在已查看的主题之间导航：MD5、SHA
验证密码	用于 SNMPv3 中通信的验证密码。
加密方法	用于SNMPv3中通信的加密方法。选项，可以在已查看的主题之间导航：DES、AES128
加密密码	用于 SNMPv3 中通信的加密密码。

这些可选设置有助于确保所收集数据的准确性：

- Virtual Bridge MIB 可以使用您的社区名称来读取。
- Cisco VTP MIB 可以使用您的社区名称来读取。
- Extreme FDB MIB 可以使用社区名称来读取。
- SNMP 版本 1、2c 或版本 3 已安装且正在运行。
- Interfaces Group MIB 可以使用社区名称来读取。

注：要监控的 IP 交换机必须符合以下两个条件：
-RFC1213：支持 SNMP v1 MIB-II。
-RFC1493：支持 SNMP v1 Bridge MIB。
为确保 RCA 和拓扑视图工作正常，请验证是否支持 RFC2674 (Virtual Bridge MIB)（或RFC4363 (Virtual Bridge MIB)）或Cisco VTP MIB。当监控Extreme Networks® 的 IP 交换机时，请使用 ExtremeXOS®（12.1.2 或更高版本）。

Cisco IP 交换机 (IOS) 的配置过程实例

对于 SNMPv1 或 v2c：

1. 使用 telnet 连接至 IP 交换机。
   a. 键入 `enable`。如果提示您输入密码，请输入。
   b. 键入 `configure terminal`。
   c. 键入 `snmp-server community public RO`。
      （其中 `public` 是社区名称，可以更改。）
   d. 键入 `end`。
   e. 键入 `show running-config`，然后确认设置。
2. 断开 telnet 连接。

对于 SNMPv3：

1. 使用 telnet 连接至 IP 交换机。
   a. 键入 `enable`。如果提示您输入密码，请输入。
   b. 键入 `configure terminal`。
   c. 键入 `snmp-server view allView`。
      （其中 `allView` 是视图名称，可以更改。）
   d. 创建视图。
   e. 键入 `snmp-server group privGroup v3 priv read allView notify allView`。（其中：`privGroup` 是组名，可以更改，`allView` 是您在步骤 c 中指定的视图名称。）
   f. 创建组。
   g. 键入 `snmp-server user Md5DesUser privGroup v3 auth md5 password1 priv des password2`
      （其中：`Md5DesUser` 是用户名，可以更改。
      `privGroup` 是您在步骤 c 中指定的组名。
      `md5` 是验证方法，可以更改。
      `password1` 是验证密码，可以更改。
      `des` 是加密方法，可以更改。
      `password2` 是加密密码，可以更改。）
      根据安全级别设置密码和验证方法 / 加密 / 密码。
   h. 创建用户。
   i. 键入 `end`。
2. 断开 telnet 连接。

Cisco (Catalyst) IP 交换机 (IOS) 的配置过程实例

对于 SNMP v3：

1. 使用 telnet 连接至 IP 交换机。
   a. 键入 `enable`。如果提示您输入密码，请输入。
   b. 键入 `configure terminal`。
   c. 键入 `snmp-server view allView iso included`。
      （其中 `allView` 是视图名称，可以更改。）
   d. 创建视图。
   e. 键入 `snmp-server group authGroup v3 auth read allView notify allView?`（其中：`authGroup`是组名，可以更改，`allView`是您在步骤c中指定的视图名称。）
   f. 创建组。
   g. 键入 `snmp-server user Md5NoneUser authGroup v3 auth md5 password1`
      （其中：`Md5NoneUser` 是用户名，可以更改。
      `authGroup` 是您在步骤 e 中指定的组名。
      `md5` 是验证方法，可以更改。
      `password1` 是验证密码，可以更改。
      `des` 是加密方法，可以更改。）
      根据安全级别设置密码和验证方法 / 加密 / 密码。
   h. 创建用户。
   i. 键入 `show vlan` 并确认 vlan 列表。在该例中，键入 `refrains from the one of enet(ethernet)`。
   j. 键入 `snmp-server group authGroup v3 auth context vlan-1 read allView notify allView` 并将其设为允许上下文。请注意，如果该设置未应用到所有 VLAN，可能会出现授权错误。
      `authGroup` 是组名，可以更改。
      `vlan-1` 是 VLAN 名称。将其设为所有受限 VLAN。
      `allView` 是您在步骤 e 中指定的视图名称。
   k. 键入 `end`。
2. 断开 telnet 连接。

HP IP 交换机的配置过程实例

对于 SNMPv1 或 v2c：

1. 使用 telnet 连接至 IP 交换机。
   a. 键入 `configure terminal`。
   b. 键入 `snmp-server community public manager restricted?`
      （其中：`public` 是社区名称，可以更改。）
   c. 键入 `show snmp-server`，然后确认设置。
2. 断开 telnet 连接。

对于 SNMPv3：

1. 使用 telnet 连接至 IP 交换机。
   a. 键入 `configure terminal`。
   b. 键入 `snmpv3 user Md5DesUser auth md5 password1 priv password2`。
      （其中：`Md5DesUser` 是用户名，可以更改。
      `md5` 是验证方法，可以更改。
      `password1` 是验证密码，可以更改。
      `password2` 是加密密码，可以更改。）
      根据安全级别设置密码和验证方法 / 加密 / 密码。
   c. 创建用户。
   d. 键入 `snmpv3 group managerpriv user Md5DesUser sec-model ver3`
      （其中：`managerpriv` 是组名，可以更改，`Md5DesUser` 是您在步骤 b 中指定的用户名。）
   e. 将组与用户连接。
2. 断开 telnet 连接。

Juniper IP 交换机的配置过程实例

对于 SNMPv1 或 v2c：

1. 使用 Web 浏览器访问 Juniper Web 设备管理器。
   a. 登录。
   b. 在导航窗格中，选择**系统**、**管理**、**SNMP**，然后选择**社区配置**。
   c. 在**社区配置**面板中，添加或更新将由 IT Operations Analyzer 管理服务器访问的 SNMP 社区。
2. 关闭 Web 浏览器。

对于 SNMPv3：

1. 使用 telnet 连接至 IP 交换机。
   a. 键入 `cli`，然后更改为 cli 模式。
   b. 键入 `configure`。
   c. 键入 `set snmp view allView oid .1 include`
   （其中：`allView` 是视图名称，可以更改。）
   d. 创建视图。
   e. 键入 `set snmp v3 vacm access group privGroup default-context-prefix security-model usm security-level privacy read-view allView notify-view allView`
   （其中：`privGroup` 是组名，可以更改，`allView` 是您在步骤 c 中指定的视图名称。）
   f. 创建组。
   g. 键入 `set snmp v3 usm local-engine user Md5DesUser authentication-md5 authentication-password password1`
   （其中：`Md5DesUser` 是用户名，可以更改。
   `authentication-md5` 是验证方法，可以更改。
   `password1` 是验证密码，可以更改。）
   根据安全级别设置验证系统 / 密码。
   h. 创建用户。
   i. 键入 `set snmp v3 usm local-engine user Md5DesUser privacy-des privacy-password password2`
   （其中：`Md5DesUser` 是您在步骤 g 中指定的用户名。
   `privacy-des` 是加密方法，可以更改。
   `password2` 是加密密码，可以更改。）
   根据安全级别设置加密方法 / 加密密码。
   j. 键入 `set snmp v3 vacm security-to-group security-model usm security-name Md5DesUser group privGroup`
   （其中，“`Md5DesUser`” 是您在步骤 g 中指定的用户名。
   “`privGroup`” 是您在步骤 e 中指定的组名。）
   用户和组已关联。
   k. 键入 commit。
2. 断开 telnet 连接。

Enterasys IP 交换机的配置过程实例

对于 SNMPv1 或 v2c：

1. 使用 telnet 连接至 IP 交换机。使用管理员模式登录并运行以下命令：
   a. `set snmp community public`。
   b. `set snmp group groupRW user public security-model v1`（其中，`groupRW` 和 `public` 是可以更改的名称）？
   c. `show snmp access groupRW`，然后确认设置。
2. 断开 telnet 连接。

Extreme IP 交换机的配置过程实例

对于 SNMPv1 或 v2c：

1. 使用 Web 浏览器访问 ExtremeXOS ScreenPlay：
   a. 登录。
   b. 在导航窗格中，选择**系统**、**管理**、**SNMP**，然后选择**社区配置**。
   c. 在**社区配置**面板中，添加或更新将由 IT Operations Analyzer 管理服务器访问的 SNMP 社区。
2. 关闭 Web 浏览器。

对于 SNMPv3：

1. 使用 telnet 连接至 IP 交换机。
   a. 键入 `configure snmpv3 add mib-view allView subtree 1 type included`（其中：`allView` 是视图名称，可以根据需要更改。）
   b. 创建视图。
   c. 键入 `configure snmpv3 add access authGroup sec-model usm sec-level authnopriv read-view allView notify-view allView`（其中：`authGroup` 是组名，可以更改，`allView` 是您在步骤 a 中指定的视图名称。）
   d. 创建组。
   e. 键入 `configure snmpv3 add user Md5NoneUser authentication md5 password1`
   （其中：`Md5NoneUser` 是用户名，可以更改。
   `md5` 是验证方法，可以更改。
   `password1` 是验证密码，可以更改。）
   根据安全级别设置验证方法 / 密码。
   f. 创建用户。
   g. 键入 `configure snmpv3 add group authGroup user Md5NoneUser sec-model usm`（其中：`authGroup` 是您在步骤 c 中指定的组名，`Md5NoneUser` 是您在步骤 e 中指定的用户名。）
   h. 在用户和组之间建立连接。
2. 断开 telnet 连接。

NETGEAR 交换机的配置过程实例

对于 SNMPv1 或 v2c：

1. 使用 Web 浏览器访问 NETGEAR 交换机：
   a. 登录。
   b. 在导航窗格中，选择**系统**、**管理**、**SNMP**，然后选择**社区配置**。
   c. 在**“社区配置”**面板中，添加或更新一个将由 IT Operations Analyzer 管理服务器访问的 SNMP 社区。
2. 关闭 Web 浏览器。

DELL IP 交换机的配置过程实例

对于 SNMPv1 或 v2c：

1. 使用 Web 浏览器访问 DELL OpenManage Switch Administrator：
   a. 登录。
   b. 在导航窗格中，选择**“系统”**、**“SNMP”**，然后选择**“全局参数”**。
   c. 在**全局参数**面板中，将 **SNMP 通知**设为**启用**。
   d. 在导航窗格中，选择**社区**。
   e. 在**社区**面板中，添加或更新一个将由 IT Operations Analyzer 管理服务器访问的 SNMP 社区。
2. 关闭 Web 浏览器。

对于 SNMPv3

1. 使用 telnet 连接至 IP 交换机。
   a. 键入 `configure`。
   b. 键入 `snmp engineid local default` 并配置引擎 ID。
   c. 键入 `snmp view allView 1 included`
      （其中：`allView` 是视图名称，可以更改。）
   d. 创建视图。
   e. 键入 `snmp group authGroup v3 auth read allView notify allView`（其中：`authGroup` 是组名，可以更改，`allView` 是您在步骤 c 中指定的视图名称。）
   f. 创建组。
   g. 键入 `snmp user Md5NoneUser authGroup auth-md5 password1`
      （其中：`Md5NoneUser` 是用户名，可以更改。
      `authGroup` 是您在步骤 e 中指定的组名。
      `auth-md5` 是验证方法，可以更改。
      `password1` 是验证密码，可以更改。）
      根据安全级别设置验证方法 / 密码。
   h. 创建用户。
2. 断开 telnet 连接。

Allied-Telesis (AT-9424T) 交换机的配置过程实例

对于 SNMPv3

1. 使用 telnet 连接至 IP 交换机。
   a. 键入 `enable snmp` 并启动 SNMP。
   b. 键入 `create snmpv3 view allView Subtree=1 Type=Included`（其中：`allView` 是视图名称，可以更改。）
   c. 创建视图。
   d. 键入 `create snmpv3 access authGroup SecurityModel=V3 SecurityLevel=Authentication ReadView=allView NotifyView=allView`（其中：`authGroup` 是组名，可以更改，`allView` 是您在步骤 b 中指定的视图名称。）
   e. 创建组。
   f. 键入 `add snmpv3 user Md5NoneUser Authentication=Md5 AuthPassword=password1`
   （其中：`Md5NoneUser` 是用户名，可以更改。
   `Md5` 是验证方法，可以更改。
   `password1` 是验证密码，可以更改。）
   根据安全级别设置验证方法 / 密码。
   g. 创建用户。
   h. 键入 `create snmpv3 group UserName=Md5NoneUser SecurityModel=V3 GroupName=authGroup`（其中：`Md5NoneUser` 是您在步骤 f 中指定的用户名，`authGroup` 是您在步骤 d 中指定的组名。）
2. 断开 telnet 连接。

ALAXALA (AX3600) 交换机的配置过程实例

对于 SNMPv3

1. 使用 telnet 连接至 IP 交换机。
   a. 键入 `configure terminal`。
   b. 键入 `snmp-server view allView 1 included`
   （其中：`allView` 是视图名称，可以更改。）
   c. 创建视图。
   d. 键入 `snmp-server group authGroup v3 auth read allView notify allView`（其中：`authGroup` 是组名，可以更改，`allView` 是您在步骤 b 中指定的视图名称。）
   e. 创建组。
   f. 键入 `snmp-server user Md5NoneUser authGroup v3 auth md5 password1`
   （其中：`Md5NoneUser` 是用户名，可以更改。
   `authGroup` 是组名。在步骤 d 中指定。
   `md5` 是验证方法，可以更改。
   `password1` 是验证密码，可以更改。）
   根据安全级别设置验证方法 / 密码。

g. 创建用户。

h. 键入 `write`。

2. 断开 telnet 连接。

启用 SNMP 陷阱

无论何时IP交换机通信连线或掉线，IT Operations Analyzer都能接收SNMP陷阱。要选择设置这些陷阱接收，请应用以下设置：

- 启用**发送陷阱**（版本必须为 SNMP v1）。
- 将**发送陷阱目的地地址**设置为IT Operations Analyzer管理服务器IP地址，并将**发送陷阱目的地端口**设置为 IT Operations Analyzer 管理服务器**陷阱端口**（端口号为 162）。

注：有关 IT Operations Analyzer 使用的默认端口号的信息，请参阅《*Hitachi IT Operations Analyzer 入门指南*》的第 2 章。

Cisco IP 交换机 (IOS) 的配置过程实例

1. 使用 telnet 连接至 IP 交换机。键入以下命令：
   a. `enable`。如果提示您输入密码，请输入。
   b. `configure terminal`。
   c. `snmp-server enable traps`。
   d. `snmp-server host 192.168.1.1 version 1 public`
   （其中的 `192.168.1.1` 是发送陷阱的目的地，`public` 是社区名称。两者都可以在必要时更改）。
   e. `end`。
   f. `show running-config`，然后确认设置。
2. 断开 telnet 连接。

HP IP 交换机的配置过程实例

1. 使用 telnet 连接至 IP 交换机。
   a. 键入 `configure`。
   b. 键入 `snmp-server host 192.168.1.1 public all`。
   （其中：`192.168.1.1` 是发送陷阱的目标，`public` 是社区名称。两者均可在需要时更改。）
   c. 键入 `show snmp-server`，然后确认设置。
2. 断开 telnet 连接。

Juniper IP 交换机 (EX 系列) 的配置过程实例

1. 使用 Web 浏览器访问 Juniper Web 设备管理器：
   a. 登录。
   b. 单击**配置**。
   c. 单击**服务**，然后选择 **SNMP**。
   d. 在**陷阱组**中单击**添加**。
   e. 指定一个**陷阱组名称**。
   f. 从**类别**区域中选择**链接**或**无**。
   g. 在**目标**中添加管理服务器的 IP 地址。
   h. 单击**确定**。
2. 关闭 Web 浏览器。

Enterasys IP 交换机的配置过程实例

1. 使用 telnet 连接至 IP 交换机。使用管理员模式登录并运行以下命令：
   a. `set snmp targetparams testParams user public security-model v1 message-processing v1`。

      请注意，**testParams** 是可以按需更改的名称。
   b. `set snmp notify testNotify tag testTag trap`。

      请注意，**testNotify** 和 **testTag** 是可以按需更改的名称。
   c. `set snmp targetaddr testTargetAddr 192.168.55.11 param testParams udpport 162 mask 255.255.255.0 taglist testTag`。

      请注意，**testTargetAddr** 是自发名称，**192.168.55.11** 是陷阱目的地的 IP 地址，**162** 是陷阱目的地的端口号，而 **255.255.255.0** 是陷阱目的地的子网掩码。如果需要，您可以更改此信息。
   d. `show running-config`，然后确认设置。
2. 断开 telnet 连接。

Extreme IP 交换机的配置过程实例

1. 使用 telnet 连接至 IP 交换机。使用管理员模式登录并运行以下命令：
   a. `configure snmpv3 add target-params testTargetParam user v1v2c_ro mp-model snmpv1 sec-model snmpv1 sec-level noauth`。

      请注意，**testTargetParam** 是任意名称，而 **v1v2c_ro** 是安全名称。任何名称都可以在必要时更改。您可使用 `show snmpv3 community` 来确认安全名称。
   b. `configure snmpv3 add target-addr 192.168.55.11 param testTargetParam ipaddress 192.168.55.11/FFFFFF00 transport-port 162 from 192.168.55.7`。

      请注意，**191.168.55.11** 是陷阱目的地的 IP 地址，**FFFFFF00** 是陷阱目的地的子网掩码，**162** 是陷阱目的地的端口号，而 **192.168.55.7** 是陷阱来源的 IP 地址。如果需要，您可以更改此信息。
   c. `show running-config`，然后确认设置。
2. 断开 telnet 连接。

NETGEAR IP 交换机的配置过程实例

1. 使用 Web 浏览器访问 NETGEAR 交换机：
   a. 登录。
   b. 在导航窗格中，选择**系统**、**管理**、**SNMP**，然后选择**陷阱配置**。
   c. 在“**陷阱配置**”面板中，添加或更新用于将 SNMP 陷阱发送到 IT Operations Analyzer 管理服务器的陷阱配置。对于 **SNMP 版本**，请指定 **SNMP V1**。
   d. 在导航窗格中，选择**“陷阱标志”**。
   e. 在**“陷阱标志”**窗格中，将**“连接 / 掉线”**设为**“启用”**。
2. 关闭 Web 浏览器。

DELL IP 交换机的配置过程实例

1. 使用 Web 浏览器访问 DELL **OpenManage Switch Administrator**：
   a. 登录。
   b. 在导航窗格中，选择**“系统”**、**“SNMP”**，然后选择**“全局参数”**。
   c. 在**全局参数**面板中，将 **SNMP 通知**设为**启用**。
   d. 在导航窗格中，选择**“通知收件人”**。
   e. 在**“通知收件人”**面板中，添加或更新用于将SNMP陷阱发送到IT Operations Analyzer 管理服务器的陷阱配置。对于该配置，请选择**“SNMPv1.2”**。
2. 关闭 Web 浏览器。

6

准备 Hitachi 存储设备

IT Operations Analyzer 可以监控 Hitachi AMS/WMS/SMS 系列和 Hitachi Unified Storage 系列。它还可以通过 Device Manager 的 SMI-S Agent监控Hitachi 9500V和Hitachi USP VM。但是，其不会监控Hitachi 9500V 的性能。

本章描述连接到 Hitachi AMS/WMS/SMS 存储节点、Hitachi Unified Storage、Hitachi 9500V和Hitachi USP VM时必须收集的信息。此外，本章还介绍获取 Hitachi AMS/WMS/SMS 系列、Hitachi Unified Storage 系列和 Hitachi USP VM 的性能信息所需执行的准备任务。

- 连接至 Hitachi AMS/WMS/SMS 系列和 Hitachi Unified Storage 系列的准备
- 获取 Hitachi AMS/WMS/SMS 系列和 Hitachi Unified Storage 系列的性能信息的准备
- 连接到 Hitachi 9500V 和 USP VM 之前的准备
- 获取 Hitachi USP VM 性能信息之前的准备

连接至 Hitachi AMS/WMS/SMS 系列和 Hitachi Unified Storage 系列的准备

IT Operations Analyzer 可以监控 Hitachi AMS/WMS/SMS 系列和 Hitachi Unified Storage 系列。当您连接至 Hitachi AMS/WMS/SMS 系列和 Hitachi Unified Storage 系列时，必须使用表 6-1 中列出的信息。

表 6-1：连接至 Hitachi AMS/WMS/SMS 系列和 Hitachi Unified Storage 系列的信息

项目	详情
IP 地址	用于连接至存储设备的 IP 地址。
用户 ID	如果已启用**帐户验证**或**密码保护**，请指定可以登录到存储设备的用户的 ID。
密码	与用户 ID 相关联的密码。如果已启用**帐户验证**或**密码保护**，则需要此信息。

注：在使用**密码保护**时，可能会出现错误。例如，当多个管理服务器同时尝试访问已配置**密码保护**的 Hitachi 存储设备时。为防止出现错误，我们建议禁用**密码保护**。

关于修改端口号

Hitachi 存储设备的管理端口号修改后，请在服务文件中注册更改的端口号。该服务文件位于以下 Windows 目录中：

<*Windows 目录*>\system32\drivers\etc\services

- **正常端口**号的服务名称：df-damp-snm
- **安全端口**号的服务名称：df-damp-snm-ssl

下列实例中，**正常端口**设置为 2300，安**全端口**设置为 25000：

df-damp-snm 2300/tcp #normal port

df-damp-snm-ssl 25000/tcp #secure port - SSL

注：IT Operations Analyzer 监控的 Hitachi 存储设备的端口号应匹配。服务文件更改后，更改会影响使用 HSNM2-API 的产品，如 Hitachi Storage Navigator Modular 2，HiCommand 系列等。

获取 Hitachi AMS/WMS/SMS 系列和 Hitachi Unified Storage 系列的性能信息的准备

完成以下步骤以获取性能信息。

1. 从 Hitachi Storage Navigator Modular 2 中打开要监控其性能的存储设备的**性能统计**面板。
2. 基于新窗口中是否显示管理对话框完成任务：
   - **当管理对话框出现在新窗口中时**
   a. 登录到 Hitachi Storage Navigator Modular 2。
   b. 单击目标阵列名称并打开管理对话框。
   c. 在该菜单中，单击**工具**、**性能**，然后选择**设置**。

- **当管理对话框出现在同一窗口中时**

a. 登录到 Hitachi Storage Navigator Modular 2。

b. 单击目标阵列名称并打开管理屏幕。

c. 在树视图中，打开**性能**，然后单击**监控**。

d. 单击**获取项目更改**。

3. 确认已选择以下项：**RAID 组 / 逻辑单元信息**、**缓存信息**、**处理器信息**和**驱动器激活信息**，然后单击**确定**。

连接到 Hitachi 9500V 和 USP VM 之前的准备

IT Operations Analyzer 可以监控：

- Hitachi9500V（通过 Hitachi Device Manager 的 SMI-S Agent）。安装 Device Manager 5.9 或更高版本并允许使用 SMI-S Provider。
- Hitachi USP VM（通过 Device Manager 的 SMI-S Agent）。安装 Device Manager 6.2 或更高版本并允许使用 SMI-S Provider。

下面是用于获取 Hitachi 9500V 和 Hitachi USP VM 连接信息的常规过程概要。有关特定细节，请参阅适用的手册：

- Hitachi Device Manager, Provisioning Manager and Tiered Storage Manager Software Installation Guide
- Hitachi Device Manager and Provisioning Manager Software System Configuration Guide
- Hitachi Device Manager Software Web Client User Guide

1. 在任意服务器上安装 **Device Manager**。您可以在安装期间选择存在 SMI-S Agent，因此请将其启用。
2. 登录到 **Device Manager**，单击**子系统**，然后单击**添加子系统**并注册存储设备。

   在注册设备时，请使用存储控制器的 IP 地址、用户 ID 和密码。表 6-2 列出了在连接至 Hitachi 存储设备时需要的信息。
3. 当按照本手册中的说明使用 SMI-S Provider 时，您需要增加 Device Manager 服务器的内存 heap 大小。以下是在使用 Microsoft Windows 时的过程实例：

   a. 计算机内存 heap 大小。

   b. 使用文本编辑器打开 **Server.ini** 文件：

   <*Device Manager 服务器安装位置* >\HiCommandServer\Server.ini

   c. 根据在步骤 a 中的计算结果，更改 **JVM_XOPT_HEAP_MAX** 的值。例如：

   JVM_XOPT_HEAP_MAX=Xmx< *设置值* >m

   d. 重新启动 Device Manager 服务器。

表 6-2：连接到 Hitachi 9500V 和 Hitachi USP VM 的信息

项目	详情
IP 地址	使用装有 Device Manager 的服务器的 IP 地址。
名称空间	对于 Device Manager5.9 或更高版本，请指定：root/smis/smis12 对于 Device Manager 6.2 或更高版本，请指定：root/smis/smis13 对于 Device Manager 7.0 或更高版本，请指定：root/smis/smis14
SSL 的存在	使用在 Device Manager 安装期间应用的设置。
端口号	使用在 Device Manager 安装期间应用的设置。默认情况下： • 非 SSL 通信：5988 • SSL 通信：5989
用户 ID	使用 Device Manager 的用户 ID。
密码	使用与用户 ID 相关联的密码。

注：当您的工作场所使用 Hitachi Device Manager 来监控 Hitachi 存储设备时，以下组件在**监控**模块中始终被报告为“工作正常”：
- 存储控制器
- 存储 FC 端口
- 存储磁盘驱动器
- 存储卷
- LUN

因此，将不会检测到任何错误条件。

获取 Hitachi USP VM 性能信息之前的准备

下面概述了如何获取 Hitachi USP VM 性能信息。有关详情，请参阅 Hitachi Device Manager 手册。

1. 准备存储子系统。

   在您希望获取其性能数据的每个存储子系统中准备命令设备。（命令设备是一种控制设备，它可以向大型磁盘阵列单元发出控制命令。）然后，为用于收集性能数据的主机分配路径，并配置主机以识别命令设备。

2. 准备用于收集性能数据的主机。

   安装 Device Manager Agent，并配置命令设备。

3. 准备 Device Manager 服务器。

   在 Device Manager 服务器的属性文件中，设置用于收集性能数据的主机名。

7

准备将 SMI-S 用于 FC 交换机和存储设备

IT Operations Analyzer 使用 SMI-S 来发现和监控其它存储设备和 FC 交换机。本章介绍了 SMI-S 和需要设置您的 FC 交换机及存储设备的任务。

- 复查 SMI-S 准备
- 准备将 SMI-S 用于光纤信道 (FC) 交换机
- 准备将 SMI-S 用于存储设备

复查 SMI-S 准备

SMI-S 是全球网络存储工业协会 (SNIA) 标准，提供了一种开放式管理应用编程接口 (API)。它支持对存储网络和存储设备进行交互式管理，包括虚拟存储、交换机和主机。

如果您的环境使用第三方存储设备（即Hitachi存储设备之外的存储设备或FC交换机），则 IT Operations Analyzer 可以通过使用 SMI-S Agent 来发现并监控。

在带有 SMI-S Agent 并使用第三方存储设备的环境中，可以使用两种模型之一：嵌入式模型或代理模型。

- 在**嵌入式模型**中，SMI-S Agent 在一个设备上运行。我们将其称为 SMI-S Agent（嵌入式）。
- 在**代理模型**中，SMI-S Agent 安装在一台服务器上。我们将其称为 SMI-S Agent（代理式）。

图 7-1 提供了 SMI-S 环境的实例，由一台服务器（称为 SMI-S 服务器）和一台客户端组成。IT Operations Analyzer 作为客户端操作，在此实例中用于收集关于光纤信道 (FC) 交换机的信息。请注意包含嵌入式和代理模型的蓝色阴影区域，在启动初次发现之前必须对其进行准备。

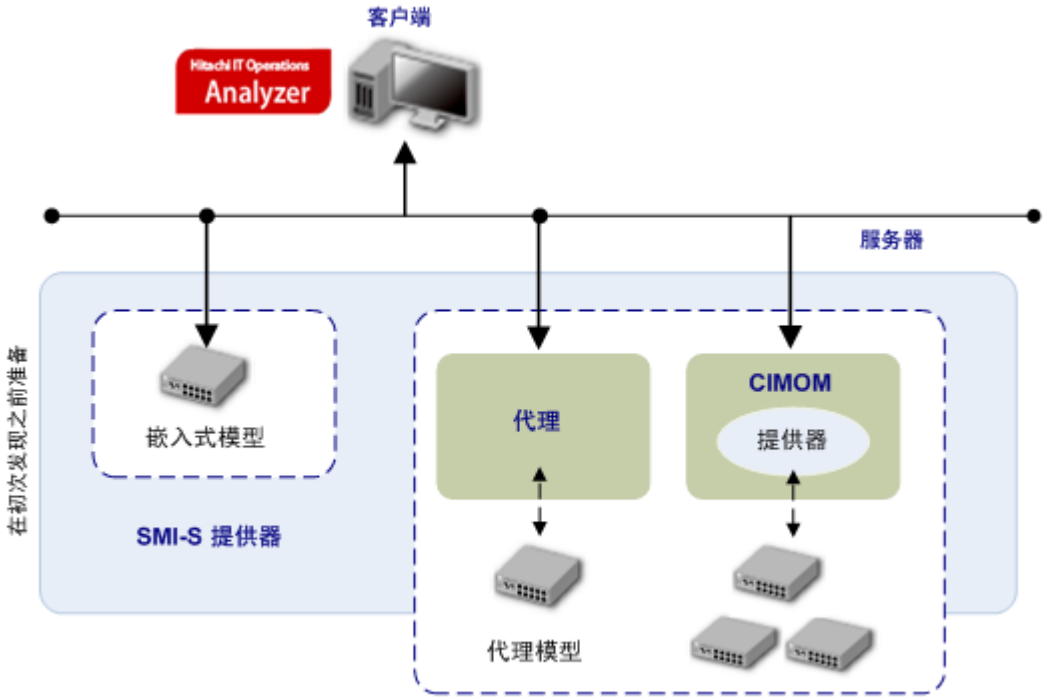

图 7-1：SMI-S 环境的实例

以下小节介绍了必须对环境中的 FC 交换机和存储设备进行的准备工作。

准备将 SMI-S 用于光纤信道 (FC) 交换机

要将设备指定为监控目标，它们必须支持 SMI-S 版本 1.0-1.3，并且必须运行用于管理这些设备的服务。本节介绍了用于以下设备的 SMI-S Agent 设置：

- Brocade® FC 交换机
- Brocade Sphereon 系列 FC 交换机
- QLogic® FC 交换机
- Cisco® FC 交换机

配置 Brocade FC 交换机（Sphereon 系列除外）

按照以下指导配置SMI-S Agent设置：有关详情，请参阅以下网站上提供的Brocade SMI Agent 文档：
http://www.brocade.com/services-support/drivers-downloads/smi-agent/index.page

您可以确认发行说明中包含的安装要求、安装过程、安装后设置和更新，如下所示：

- 安装要求

  Brocade SMI Agent v120.6.0a 安装指南第 1 章“安装要求”
- 安装过程

  Brocade SMI Agent v120.6.0a 安装指南第 2 章“安装 SMI Agent”
- 安装后设置

  Brocade SMI Agent v120.6.0a 用户指南
- 发行说明

  Brocade SMI Agent v120.6.0a 发行说明 v1.1

安装前要求

- Brocade SMI-S Agent 版本：Brocade SMI Agent v120.6.0a
- 操作系统：Microsoft Windows Server 2003（32 位）

如果已安装 Brocade SMI-S Agent 的之前版本，请完成以下安装任务。

安装 Brocade SMI Agent：

1. 从以下网站下载 Brocade SMI-S Agent v120.6.0a，然后运行 **install.exe**：
   http://www.brocade.com/services-support/drivers-downloads/smi-agent/index.page
2. 完成每个安装向导指示。对于特定提示，请检查以下指导：
   a. **HTTP 端口配置**。默认端口号为 5988。请注意，您指定的端口号用于连接到 IT Operations Analyzer。
   b. **HTTPS端口配置**。默认端口号为5988。请注意，您指定的端口号用于连接到 IT Operations Analyzer。

c. **代理连接配置**。指定以下内容：

代理 IP：FC 交换机的 IP 地址

用户名：FC 交换机的用户名称

密码：FC 交换机的密码

根据您的环境指定其他设置。

3. 要在 Brocade Agent 安装结束时保存更改，请单击**完成**。

至此，您已准备好注册 FC 交换机。

注册 FC 交换机：

1. 启动 **Brocade SMI Agent 配置工具**：

a. 在**开始**菜单中，选择**所有程序**。

注：在 Windows Server 2012 上，导航至**开始**菜单的步骤不同。

b. 依次选择 **SMIAgent120.6.0a** 和 **Brocade SMI Agent 配置工具**。

2. 单击**添加**以启动**代理配置**对话框。
3. 输入所需的信息，然后单击**确定**以保存设置并关闭**代理配置**对话框。
4. 在 **Brocade SMI Agent** 配置工具中，通过单击**应用**，将代理状态从**未连接**更改为**已连接**。

表 7-1 列出了在连接至 Brocade FC 交换机时需要的信息。

表 7-1：关于连接至 Brocade FC 交换机的信息

项目	详情
IP 地址	指定安装 Brocade SMI Agent 的服务器的 IP 地址。
名称空间	指定 `root/brocade1`。
SSL 的存在	应用在安装期间配置的 Brocade SMI Agent 设置。
端口号	应用在安装期间配置的 Brocade SMI Agent 设置。默认情况下： • 非 SSL 通信：5988 • SSL 通信：5989
用户 ID	使用 Brocade SMI Agent 的用户 ID。
密码	输入用户 ID 的密码。

注：当FC-FC路由端口状态为“链接关闭”时，虚拟交换机的状态变为“无法访问”。即使此端口状态再次变为正常状态，此交换机无法访问的状态仍不会改变。

要将此交换机的状态从无法访问改变为正常，IT Operations Analyzer需要重新发现此交换机。如果此端口状态为链接关闭，则在虚拟交换机的 SMI-S Provider 未答复或响应时需要执行此操作。即使端口状态再次变为正常状态，SMI-S Provider也会将交换机状态报告为无法访问。

有关发现交换机、节点和其它设备的信息，请参阅联机帮助。

配置 Brocade Sphereon FC 交换机

按照以下指导配置SMI-S Agent设置：有关详情，请参阅以下网站上提供的Brocade SMI Agent for EOS 文档：
http://www.brocade.com/services-support/drivers-downloads/smi-agent/index.page

您可以确认发行说明中包含的安装要求、安装过程、安装后设置和更新，如下所示：

- 安装要求

  Brocade SMI Agent for EOS 产品用户指南 2.0 第 1 章“系统要求”
- 安装过程

  Brocade SMI Agent for EOS 产品用户指南 2.0 第 2 章“安装 Brocade SMI Agent for EOS 产品”
- 安装后设置

  Brocade SMI Agent for EOS 产品用户指南 2.0 第 3 章“使用 SMI Agent for EOS 产品服务器配置程序”和第 4 章“客户端操作的服务器设置”
- 发行说明

  Brocade SMI Agent for EOS 产品 2.0 发行说明

安装前要求

- Brocade SMI-S Agent 版本：用于 Windows 的 Brocade SMI Agent for EOS 产品 2.0
- 操作系统：Microsoft Windows Server 2003（32 位）

安装 Brocade SMI Agent：

1. 从以下网站下载用于 Windows 的 Brocade SMI Agent for EOS，然后运行 **install.exe**：
   http://www.brocade.com/services-support/drivers-downloads/smi-agent/index.page
2. 完成每个安装向导指示。
3. 要在 Brocade Agent 安装结束时保存更改，请单击**完成**。

   至此，您已准备好注册 FC 交换机。

注册 FC 交换机：

1. 打开以下路径中的 **Switch.properties** 文件：< *安装目录* >\agent\server\jserver\bin
2. 指定以下参数：
   - **cimserver**

     服务器的 URL，例如：https://localhost/root/mcdata
   - **cimserverusername**

     用于登录到 CIM 服务器的用户名，例如：Administrator
   - **cimserverpassword**

     用于登录到 CIM 服务器的密码，例如：Password

- **switchip**

  交换机的 IP 地址，例如：172.26.24.180
- **switchtype**

  交换机产品类型代码。请参阅下面的注释。
- **switchusername**

  用于登录到交换机的用户名。
- **switchpassword**

  用于登录到交换机的密码。

注：下面是 FC 交换机产品类型代码：

Sphereon 3016：代码 2

Sphereon 3032：代码 3

Sphereon 3216：代码 4

Sphereon 3232：代码 5

Sphereon 4300：代码 6

Sphereon 4400：代码 12

Sphereon 4500：代码 7

Sphereon 4700：代码 13

3. 从命令提示符下将信息移到以下路径下：<*安装目录*>\agent\server\jserver\bin
4. 运行以下命令：ManageSwitch Add

表 7-2 列出了在连接至 Brocade Sphereon 系列 FC 交换机时需要的信息。

表 7-2：关于连接至 Brocade FC 交换机的信息

项目	详情
IP 地址	指定安装 Brocade SMI Agent for EOS 的服务器的 IP 地址。
名称空间	指定 `root/mcdata`。
SSL 的存在	应用在安装期间配置的 Brocade SMI Agent 设置。
端口号	应用在安装期间配置的 Brocade SMI Agent for EOS 设置。
用户 ID	使用 Brocade SMI Agent for EOS 的用户 ID。
密码	输入用户 ID 的密码。

配置 QLogic FC 交换机

SMI-S Provider 嵌入在 QLogic FC 交换机中。本节的过程描述了如何使用 Web 浏览器连接到 QLogic FC 交换机的管理端口。

有关使用命令行界面 (CLI) 配置 SMI-S Provider 设置的详情，请参阅 QLogic FC 交换机的文档。以下网站提供该文档：

http://driverdownloads.qlogic.com/QLogicDriverDownloads_UI/NewDefault.aspx

配置 QLogic FC 交换机：

1. 通过Web浏览器连接至QLogic FC交换机管理端口（例如，http://10.208.113.46）。**交换机管理器**窗口将会显示。
2. 在**交换机管理器**菜单栏中选择**交换机**，然后选择**服务**。**系统服务**对话框将会显示。
3. 验证 SMI-S Provider 服务是否已启用：
   - 如果已选定 **CIM 服务**，则已启用 SMI-S Provider 服务。单击**关闭**。
   - 如果未选定 **CIM 服务**，请选择并单击**确定**。
4. 如果用于指定**SSL服务**的选项在**系统服务对话框中存在**，则可以使用SSL端口**5989**。

表 7-3 列出了在连接至 QLogic FC 交换机时需要的信息。

表 7-3：关于连接至 QLogic FC 交换机的信息

项目	详情
IP 地址	QLogic FC 交换机的 IP 地址。
名称空间	指定 `root/switch`。
SSL 的存在	应用 QLogic FC 交换机设置。
端口号	应用在安装期间配置的 QLogic FC 交换机设置。默认情况下： • 非 SSL 通信：5988 • SSL 通信：5989
用户 ID	使用 QLogic FC 交换机的用户 ID。
密码	输入用户 ID 的密码。

配置 Cisco MDS 9000 系列 FC 交换机

SMI-S Provider 嵌入在 Cisco FC 交换机中。本节的过程描述了如何启用服务器，以及如何使用 HTTP 协议（端口 5988）连接到服务器。如果您的工作场所选择使用 HTTPS 协议（端口 5989），请应用安全套接层 (SSL) 验证以加密登录信息，然后启用 HTTPS 和 SMI-S Agent（代理）。表 7-4 中引用的链接提供了此过程的详情。

有关其他详情，请参阅Cisco MDS 9000 系列SMI-S 编程参考。以下网站提供该文档：

http://www.cisco.com/en/US/docs/switches/datacenter/mds9000/sw/4_1/smi_s/programming/guide/proced.html

配置 Cisco MDS 9000 系列 FC 交换机：

步骤 8 后面列出了以下过程中描述的命令执行示例。

1. 通过 telnet 访问 FC 交换机，然后登录。
2. 输入 `show cimserver`，然后验证是否已启用 cim 服务器 Http。
3. 输入 `config terminal`，然后启动配置模式。
4. 默认情况下已启用 HTTP。如果不是这样，请输入 `cimserver enableHttp` 以启用 HTTP。
5. 输入 `cimserver enable` 以启用 CIM 服务器。
6. 输入 `end` 以结束配置模式。
7. 输入 `show cimserver` 并验证设置：
   - cimserver is enabled
   - cimserver Http is enabled
8. 输入 `exit` 以断开 telnet 连接。

命令示例

```
FCGS03 login: ********
```

密码：

```
FCGS03# show cimserver
 cimserver is not enabled
 cimserver Http is enabled
 cimserver Https is not enabled
 cimserver certificate file is not installed
FCGS03# config terminal
Enter configuration commands, one per line. End with CNTL/Z。
FCGS03(config)# cimserver enable
FCGS03(config)# end
FCGS03# show cimserver
 cimserver is enabled
 cimserver Http is enabled
 cimserver Https is not enabled
 cimserver certificate file is not installed
 Current value for the property logLevel in CIMServer is
'WARNING'.
FCGS03# exit
```

表 7-4：关于连接至 Cisco FC 交换机的信息

项目	详情
IP 地址	Cisco FC 交换机的 IP 地址。
名称空间	指定 `root/cimv2`。
SSL 的存在	应用 Cisco FC 交换机设置。有关详情，请参阅《Cisco MDS 9000 系列 SMI-S 编程指南》：http://www.cisco.com/en/US/docs/switches/datacenter/mds9000/sw/4_1/smi_s/programming/guide/proced.html
端口号	应用在安装期间配置的 Cisco FC 交换机设置。默认情况下： • 非 SSL 通信：5988 • SSL 通信：5989
用户 ID	使用 Cisco FC 交换机的用户 ID。
密码	输入用户 ID 的密码。

准备将 SMI-S 用于存储设备

要将存储设备指定为监控目标，它必须支持 SMI-S 版本 1.0-1.3，并且必须运行用于管理存储设备的服务。本节介绍了用于以下设备的 SMI-S 设置：

- EMC 存储设备
- HP EVA 系列存储设备
- HP MSA 系列存储设备
- Engenio OEM Sun 存储设备和 IBM 存储设备
- NetApp 存储设备

注：有关配置 Hitachi 存储设备和获取 Hitachi 存储设备 (USP VM) 性能的信息，请参阅第 6 章，准备 Hitachi 存储设备。

关于可为一个存储设备监控的最大卷数的注释

可为一个存储设备监控的卷（逻辑设备）的最大数量是 2000。当存储卷的数量超过 2000 时，“存储卷（组件类型）”（显示在**监控**模块的**组件**选项卡中）将反映以下信息以及无法监控的卷：

- 组件名称：卷（卷数）
- 组件状态：无法监控卷，原因是卷数量超过 2000。

此外，无法获取下列与卷有关的信息。**监控**模块中显示的信息如下所示：

- **组件**选项卡。对于以下组件类型，不会显示任何内容：“LUN”，“存储已导出文件共享”，“存储文件共享端口”，“存储卷”
- **性能**选项卡。对于“写入缓存命中比例”，状态为“未知”，并且不能获取性能。

配置 EMC 存储设备

按照以下指导配置 SMI-S Agent 设置：有关详情，请参阅 EMC SMI-S Agent 文档：

- EMC SMI-S Provider 发行说明

  概述：安装方法和安装后的设置方法

  http://Powerlink.EMC.com

  Support（支持）> Technical Documentation and Advisories（技术文档和顾问）> Software ~ S ~ Documentation（软件 ~ S ~ 文档）> SMI-S Provider（SMI-S 提供商）>Release Notes（发行说明）

- EMC 支持矩阵

  概述 :EMC SMI-S Provider 的支持目标

  http://developer.emc.com/developer/devcenters/storage/snia/smi-s/downloads/EMC_Providers_SMI-S_Only.pdf

安装前要求

- EMC SMI-S Provider 版本：V3.2.3、V3.3.1
- 操作系统：Microsoft Windows 2003 [x86] R2, SP1
- 存储阵列：CLARiiON

有关 EMC 支持矩阵的存储设备工作环境要求，请参阅以下链接：

http://developer.emc.com/developer/devcenters/storage/snia/smi-s/downloads/EMC_Providers_SMI-S_Only.pdf

---

注：EMC CLARiiON 中未获取参数指标 **WriteHitIOs** 的值。

安装 EMC SMI-S Provider：

请注意，若已安装 EMC SMI-S Provider 的之前版本或 Solutions Enabler，将卸载它们。

1. 从以下网站下载 EMC SMI-S Provider：

   http://Powerlink.EMC.com

2. 导航至以下站点位置：**支持 > 软件下载和许可 > 下载 S > SMI-S Provider**
3. 在开始安装前关闭所有应用程序
4. 下载**se6430-WINDOWS-x86-SMI.msi** 或 **se65132-WINDOWS-x86-SMI.msi**。
5. 运行安装可执行文件以启动 **EMC Solutions Enabler with SMI** 向导。
6. 完成向导中的所有提示。完成后单击**完成**。

   至此，您已准备好注册存储设备信息。

注册存储设备信息：

以下过程将确保您可以使用 EMC SMI-S Provider 管理存储设备。

1. 如果 EMC 存储卷未应用到装有 EMC SMI-S Provider 的服务器，则请完成以下带外步骤。步骤 j 后面列出了以下过程中描述的命令执行示例：
   a. 运行以下路径中的**TestSmiProvider.exe**文件：<*安装文件夹*>\SYMCLI\storbin\TestSmiProvider.exe
   b. 对于所有主机、连接类型、日志文件路径、端口、用户名和密码，请单击 Enter 保留默认信息。
   c. 键入 **addsys**，然后按 **Enter**。
   d. 键入 **y**，然后按 **Enter**。
   e. 选择存储阵列类型。对于 CLARiiON，键入 **1**，然后按 **Enter**。
   f. 指定**处理器 A** 的 IP 地址，然后按 **Enter**。同时还指定**处理器 B** 的 IP 地址，然后按 **Enter**，两次。
   g. 选择在步骤 f 中指定的地址的类型。键入 **2**，然后单击 **Enter**。
   h. 对于您正注册的存储设备，指定与管理员权限关联的用户 ID 和密码。
   i. 注册成功后将显示**输出：0**。记下相应命令区域中提及的序列号，例如 CK200080001000。
   j. 键入 **dv**，然后按 **Enter**。检查**固件版本信息**中是否显示您在步骤 i 中记录的序列号。

命令示例

```
Host [localhost]:
Connection Type (ssl,no_ssl) [no_ssl]:
Logfile path [Testsmiprovider.log]:
Port [5988]:
Username []:
Password []:
Connecting to localhost:5988
(localhost: 5988) ? addsys
Add System {y|n} [n]: y
ArrayType (1=Clar, 2=Symm) [1]: 1
One or more IP address or Hostname or Array ID
Elements for Addresses
IP address or hostname or array id 0 (blank to quit):
192.168.10.31
IP address or hostname or array id 1 (blank to quit):
192.168.10.32
IP address or hostname or array id 2 (blank to quit):
Address types corresponding to addresses specified above.
```

```
(1=URL, 2=IP/Nodename, 3=Array ID)
Address Type (0) [default=2]: 2
Address Type (1) [default=2]: 2
User [null]: analyzer
Password [null]: analyzerpass
++++ EMCAddSystem ++++
OUTPUT : 0
Legend:0=Success, 1=Not Supported, 2=Unknown, 3=Timeout,
4=Failed
       5=Invalid Parameter
       4096=Job Queued, 4097=Size Not Supported
System: //kaede/root/
emc:Clar_StorageSystem.CreationClassName="Clar_StorageSys
tem",Name="CLARiiON+CK200080001000"
(localhost:5988) ? dv
++++ Display version information ++++
CIM ObjectManager Name: PG:5B48A8C4-682F-4FCB-AE98-
F0687C31225F
CIMOM Version: Pegasus CIM Server Version 2.6.1
SMI-S spec version: 1.3.0
SMI-S Provider version: V3.3.1.0
Solutions Enabler version: V6.5-883 1.32
Firmware version information:
CLARiiON Array CK200080001000 (Rack Mounted CX3_10_C) :
3.26.10.5.019
```

2. 如果 EMC 存储卷已应用到装有 EMC SMI-S Provider 的服务器，则请完成以下带内步骤。步骤 f 后面列出了以下过程中描述的命令执行示例：
   a. 确认至少已注册一个 CLARiiON LUN。在装有 EMC SMI-S Provider 的服务器上运行以下命令：

      < *安装文件夹* >\SYMCLI\bin> syminq -cids

   b. 确认以下设置的值已设为 **true**：
      OslProv/com.emc.se.osls.osl.StorApi.database.discover
      此设置位于配置文件**emcprovider.conf**中：<安装文件夹>\SYMCLI\storbin
      如果值为 **false**，请将其更改为 **true**。

   c. 运行以下命令以暂停 EMC SMI-S Provider 服务：

      < *安装文件夹* >\SYMCLI\strobin> cimserver -stop EMC_SMI_Provider

d. 运行以下命令以注册验证信息：

< *安装文件夹* >\SYMCLI\bin>symcfg authorization add -host < *存储设备IP 地址* > -Username < 存储设备用户ID> -Password < *存储设备密码* >

示例：当 IT Operations Analyzer 密码为 **analyzerpass**、CLARiiON **处理器A** 的IP地址为 **192.168.10.31**、**处理器B** 的IP地址为 **192.168.10.32** 时，将运行以下命令。首先注册处理器 A：

< *安装文件夹* >\SYMCLI\bin>symcfg authorization add -host 192.168.10.31 -username analyzer -password analyzerpass

< *安装文件夹* >\SYMCLI\bin>symcfg authorization add -host 192.168.10.32 -username analyzer -password analyzerpass

e. 运行以下命令以启动 EMC SMI-S Provider 服务。然后，需要过一段时间才能从 IT Operations Analyzer 进行搜索：

< *安装文件夹* >\SYMCLI\strobin> cimserver -start EMC_SMI_Provider

f. 运行以下命令以确认注册信息：

< *安装文件夹* >\SYMCLI\bin> symcfg list auth

命令示例

```
C:\Program Files\EMC\SYMCLI\bin>syminq -cids
Device                  Clariion                Device
------------------------ --------------------- ---------
Name                Type   ID Rev  Ser Num      Cap (KB)
------------------------ --------------------- ---------
\\.\PHYSICALDRIVE2      CK200080001000  0326 070000B5
1048576

C:\Program Files\EMC\SYMCLI\storbin>cimserver -stop
EMC_SMI_Provider

Pegasus stopped as a Windows service

C:\Program Files\EMC\SYMCLI\bin>symcfg authorization add -
host 192.168.10.31 -username analyzer -password
analyzerpass

C:\Program Files\EMC\SYMCLI\bin>symcfg authorization add -
host 192.168.10.32 -username analyzer -password
analyzerpass

C:\Program Files\EMC\SYMCLI\storbin>cimserver -start
EMC_SMI_Provider

Pegasus started as a Windows service

C:\Program Files\EMC\SYMCLI\bin>symcfg list auth

Hostname            Username          Namespace     Port

192.168.10.31         analyzer

192.168.10.32         analyzer
```

获取 EMC 存储设备性能数据

使用以下过程，获取 EMC 存储设备性能数据。

1. 使用 EMC 存储设备管理软件来获取性能数据。为举例说明，以下介绍了 **EMC Navisphere Management Suite**：
   a. 从 **EMC Navisphere Management Suite** 菜单栏中打开**数据记录**窗口：在**工具**菜单中选择 **Analyzer**，然后选择**数据记录** ...
   b. 在**目标**区域中选择您要从中获取性能数据的存储设备，然后确认**记录**的**状态**字段：

      如果**状态**为**已停止**，请单击**启动**。

      如果**状态**为**正在运行。已在日期时间启动**，请单击**取消**。不需要重新启动 SMI-S Agent。
2. 重新启动 SMI-S Provider。如果您使用 CLI，请运行 `cimserver` 命令，然后停止并启动 SMI-S Provider：

```
< 安装文件夹 >\SYMCLI\strobin> cimserver -stop EMC_SMI_Provider
Pegasus stopped as a Windows service
< 安装文件夹 >\SYMCLI\strobin> cimserver -start EMC_SMI_Provider
Pegasus started as a Windows service
```

表 7-5：关于连接至 EMC 存储设备的信息

项目	详情
IP 地址	使用安装 EMC SMI-S Provider 的服务器的 IP 地址。
名称空间	指定 `root/emc`。
SSL 的存在	使用 EMC Provider 设置。
端口号	使用 EMC SMI-S Provider 设置。默认情况下： • 非 SSL 通信：5988 • SSL 通信：5989
用户 ID	使用 EMC Provider 的用户 ID。默认为空。
密码	使用与用户 ID 相关联的密码。默认为空。

配置 HP EVA 系列存储设备

按照以下指导配置 SMI-S Provider 设置。有关详情，请参阅 Command View EVA 手册。

注：HP EVA 系列 SMI-S 代理不支持收集性能信息的功能。

安装前要求

- 支持的版本：HP StorageWorks Command View EVA 8.0
- 操作系统：Microsoft Windows Server 2003
- 存储设备：HP StorageWorks 4400 Enterprise Virtual Array

安装 HP StorageWorks Command View EVA 8.0

1. 运行可执行文件 HP StorageWorks Command View EVA Software Suite.exe。
2. 单击**确定**启动安装向导。
3. 在安装面板**选择安装集**中，验证是否已选择 **SMI-S CIMOM**。

   HP SMI-S EVA 使用默认端口号 5988 或 5989。

   如果无法使用默认端口，则会显示一则指明哪些端口不可用的消息。如果收到此类消息，请指定一个可用的端口号（从 60000 到 65536）。然后，继续安装。
4. 安装向导的最后一个面板显示**安装完成**。要完成安装，请单击**完成**。

   至此，您已准备好应用 HP Command View EVA 设置。

应用 HP Command View EVA 设置：

1. 配置 CIMOM 服务器：
   a. 修改以下文件以更改用于 CIMOM 服务器的端口号和 HTTP/HTTPS：

      < *安装目录* >\SMI-S\CXWSCimom\config\cxws.properties
   b. 下面是默认值：

      enableHttp: true

      enableHttps: true

      cxws.http.port：5988

      cxws.https.port：5989

      使 enableHttp (Https) 无效并指定要使用的端口号时，请指定 **False**。
   c. 更改设置后，请重新启动 HP StorageWorks CIM Object Manager Service（对象管理器服务）：

      在**开始**菜单中，选择：**设置**、**控制面板**、**管理工具**，然后选择**服务**。

注：在 Windows Server 2012 上，导航至**开始**菜单的步骤不同。

2. 注册存储设备：
   a. 启动浏览器并指定以下 URL：

      https://host_name:2372

      为 **host_name** 指定**服务器名称**或 **IP 地址**。
   b. 在 **HP Command View EVA 提示符**窗口中登录。

      登录时，使用装有 HP Command View EVA 的服务器的用户帐户信息。确保该用户帐户属于 **HP 存储设备管理组**。
   c. 登录后，确认您的存储设备已显示在**存储系统**面板中。如果未显示，请单击**发现**注册您的存储设备。

注：为注册存储设备，装有 HP Command View EVA 的服务器必须直接连接到 FS 交换机。

表 7-6：关于连接至 HP EVA 存储设备的信息

项目	详情
IP 地址	使用装有 Command View EVA 的服务器的 IP 地址。
名称空间	指定 `root/eva`。
SSL 的存在	使用 Command View EVA 设置。
端口号	使用 Command View EVA 设置。默认情况下： • 非 SSL 通信：5988 • SSL 通信：5989
用户 ID	使用用于 Command View EVA 的用户 ID。
密码	使用与用户 ID 相关联的密码。

配置 HP MSA 系列存储设备

根据以下过程配置SMI-S Agent设置。有关详情，请参阅MSA SMI-S Agent文档。

注：HP MSA 系列 SMI-S Agent 不支持收集性能信息的功能。

1. 通过以下网站下载 **MSA SMI-S Provider**：
   http://h18006.www1.hp.com/storage/smis.html
2. 在任意服务器上安装 **MSA SMI-S Provider**。

表 7-7：关于连接至 HP MSA 存储设备的信息

项目	详情
IP 地址	使用 MSA SMI-S Provider 安装所在服务器的 IP 地址。
名称空间	指定 `root/hpmsa`。
SSL 的存在	使用 MSA SMI-S Provider 设置。
端口号	使用 MSA SMI-S Provider 设置。
用户 ID	使用 MSA SMI-S Provider 的用户 ID。
密码	使用与用户 ID 相关联的密码。

配置 Engenio OEM Sun 存储设备和 IBM 存储设备

根据以下过程配置SMI-S Provider设置。有关详情，请参阅Engenio SMI-S Provider文档。要下载文档，需要拥有用于登录 NetApp 网站的登录帐户：

http://support.netapp.com/NOW/apbu/oemcp/protcd/

安装前要求

- 支持的版本：Engenio SMI Provider 09.19.G0.07
- 操作系统：Microsoft Windows Server 2003（32 位）

安装 Engenio SMI-S Provider：

1. 运行可执行文件以安装 Engenio SMI Provider 09.19.G0.07。
2. 完成安装向导中的所有提示。
3. 完成安装后，单击**完成**。

注册存储设备：

以下过程将注册您想使用 Engenio SMI Provider 管理的存储设备。

1. 启动命令提示符。
2. 切换到以下目录：

   < *安装目录* >\SMI_SProvider\bin
3. 运行 `ProviderUtil` 命令并输入以下信息：
   - **输入 CIMOM 用户名**

     （可选）指定 CIMOM 用户名，例如：any
   - **输入 CIMOM 密码**

     （可选）指定 CIMOM 密码，例如：any
   - **输入端口 [5988]**

     （可选）指定端口号。默认值为 5988。
   - **输入操作**

     1) 添加设备

     2) 删除设备

     3) 添加阵列的凭证

     请输入 1、2 或 3

     指定**“1”**以注册存储设备。
   - **输入 DNS 可解析的设备主机名或 IP 地址**

     指定存储设备的 IP 地址或主机名。
   - **输入阵列密码**（默认为空）：

     指定存储设备的密码。

   显示 **The extrinsic call succeeded（外部调用成功）**消息时表示存储设备注册成功。

表 7-8 列出了在连接至您要监控的存储设备节点时需要的信息。

表 7-8：关于连接至 Sun 存储设备和 IBM 存储设备的信息

项目	详情
IP 地址	使用装有 Engenio SMI-S Provider 的服务器的 IP 地址。
名称空间	指定 `root/lsissi11`。
SSL 的存在	使用 Engenio SMI-S Provider 设置。
端口号	使用 Engenio SMI-S Provider 设置。默认情况下： • 非 SSL 通信：5988 • SSL 通信：5989
用户 ID	使用 Engenio SMI-S Provider 的用户 ID。
密码	使用与用户 ID 相关联的密码。

配置 NetApp 存储设备

根据以下过程配置NetApp存储设备的SMI-S Provider设置。有关详情，请参阅NetApp SMI-S Provider 文档。要下载文档，需要拥有用于登录 NetApp 网站的登录帐户：

http://support.netapp.com/NOW/apbu/oemcp/protcd/

安装前要求

- NetApp Data ONTAP SMI-S Agent 的支持版本：Data ONTAP SMI-S Agent 3.0
- 操作系统：Microsoft Windows Server 2003（32 位）

要使用 NetApp Data ONTAP SMI-S Agent，需要 JDK 1.5.0 或更高版本以及 JRE 1.5.0。确认装有 SMI-S Agent 的 Windows 服务器上是否已安装此信息。

安装 Data ONTAP SMI-S Agent 3.0：

1. 下载 Data ONTAP SMI-S Agent 安装文件。
2. 从 **Data ONTAP SMI-S Agent** 的**选择平台**中选择 **Windows**，然后单击**进入**。
3. 单击**查看和下载**。
4. 单击**软件下载说明**页面中的**继续**。
5. 单击**接受**以继续。下载 SMI-S Agent 及相应的手册。
6. 运行可执行文件以安装 Data ONTAP SMI-S Agent 3.0。
7. 根据您的首选项，指明要使用的安装类型：**典型**或**自定义**。
8. 完成安装向导中的所有提示。
9. 完成安装后，单击**完成**。

配置 SMI-S Provider 设置：

1. 在**编辑系统变量**对话框中，指定**JAVA_HOME**作为系统环境变量或用户环境变量。如果指定包含空格的路径，请将路径包括在双引号 (”) 中。
2. 要连接至 SMI-S Provider，请使用端口号 **5989** 和 **https** 协议。要更改端口号或允许使用 http 协议进行连接，请编辑以下目录中包含的 **WEBSconfig.ini** 文件：**C:\Program Files\ws\server\cserver\bin**。下面是 **WEBSconfig.ini** 文件中列出的默认设置。如果更改它们，则将 **enableOverride** 设为 **True**。

   enableOverride=False（如果修改后续任何设置，必须将其设为 **True**。）

   HTTPPort=5988

   HTTPSPort=5989

   enableSSL=True

   enableHTTP=False

注册存储设备：

1. 在命令提示符窗口中，切换到以下路径：

   C:\Program Files\ws\server\cserver\bin

2. 指定 **C:\Program Files\ws\bin**
3. 要注册存储设备，请运行以下命令：

   `smis.bat <`*用户 ID*`> <`*密码*`> add <`*存储设备 IP 地址*`> <`*存储设备用户 ID*`> <`*存储设备密码*`> [-p http]*`

   * 仅在使用 http 协议时才指定。

   < 用户 ID> 和 < 密码 > 使用装有 SMI-S 的服务器的 Windows 管理权限帐户。存储设备的 IP 地址 < 存储设备 _ 用户 ID> 和 < 存储设备 _ 密码 > 指定了 < 存储设备 IP> 的存储设备验证信息。

4. 要检查是否已注册该信息，请运行 **smis.bat** 文件：

   `smis.bat <`*用户 ID*`> <`*密码*`> list`

5. 运行 **ws\bin** 目录中的 natest 脚本，检查 SMI-S Provider 是否包含存储信息。以下实例介绍了存储设备磁盘信息的输出：

   `natest.bat <`*用户 ID*`> <`*密码*`> disks`

表 7-9 列出了在连接至 NetApp 存储设备时需要的信息。

表 7-9：关于连接至 NetApp 存储设备的信息

项目	详情
IP 地址	指定 Data ONTAP SMI-S Agent 安装所在服务器的 IP 地址。
名称空间	指定 `root/ontap`。
SSL 的存在	使用 Data ONTAP SMI-S Agent 设置。
端口号	使用 Data ONTAP SMI-S Agent 设置。默认情况下： • 非 SSL 通信：5988 • SSL 通信：5989
用户 ID	使用 Data ONTAP SMI-S Agent 安装所在服务器的用户 ID。
密码	使用与用户 ID 相关联的密码。

注：在**监控**模块中选择 NetApp 存储设备节点时，将有一个图标显示 IT Operations Analyzer 何时在处理状态信息或者何时在收集组件信息。此外，15 分钟内会显示以下错误消息：

KAZZ20087-E 未成功更新配置。出现故障的节点名称：< 设备名称 >

存在以下所有条件时，将显示此错误消息：

1. 正在监控 NetApp 存储设备。
2. 在 Linux 服务器上使用 Linux 版本 SMI-S Agent 管理 NetApp 存储设备。
3. IT Operations Analyzer 管理服务器和当前监控的 Linux 版本 SMI-S Agent 之间存在 HTTPS 连接。

完成以下任务之一：

- 在装有IT Operations Analyzer的服务器（管理服务器）的主机文件中注册Linux 版本 SMI-S Agent 的 IP 地址和主机名。
- 将 IT Operations Analyzer 管理服务器和 Linux 版本 SMI-S Agent 之间存在的当前 HTTPS 连接方法更改为 HTTP。
- 将 Linux 版本 SMI-S Agent 更改为 Windows 版本 SMI-S Agent。

8

准备 Dell 服务器

本章介绍了设置您的 Dell 服务器所需的任务。

概述

您必须对以下每种操作系统的服务器进行两项设置：

- 对于基于 Windows 的 Dell 服务器为 WMI/SNMP （凭证信息）。
- 对于基于 Linux 的 Dell 服务器为 SSH/SNMP （凭证信息）。

表 8-1 列出了在连接至 Dell 服务器时需要的信息。

表 8-1：关于连接至 Dell 服务器的信息

项目	详情
IP 地址	指定 Dell 服务器的 IP 地址。
端口号	Dell 服务器等待通信的 SNMP 端口（端口 161）。
社区名称	用于 SNMP Dell 服务器的社区名称。

启用 SNMP 服务和陷阱通信

您必须将每台受监控 Dell 服务器上的 SNMP 代理配置为向 Hitachi IT Operations Analyzer 管理服务器发送 SNMP 陷阱。

从服务器收到 Dell OMSA 陷阱时，IT Operations Analyzer 会根据所收到陷阱的严重性更新 Dell OMSA 陷阱组件的状态。

在 Microsoft Windows 环境下配置 SNMP 代理

要在 Microsoft Windows 环境下配置 Dell 服务器的 SNMP 代理：

1. 从桌面的**开始**菜单中，选择**控制面板**。

注：在 Windows Server 2012 上，导航至**开始**菜单的步骤不同。

2. 打开**管理工具**。
3. 打开**服务**。
4. 右键单击 **SNMP 服务**，然后选择**属性**。
5. 单击**安全性**选项卡以打开**安全性**对话框。
6. 选择**“接受来自任何主机的 SNMP 数据包”**或选择**“接受来自下列主机的 SNMP 数据包”**，然后单击 **“添加”**。

   SNMP 服务配置框将显示。
7. 键入 IT Operations Analyzer 管理服务器的主机名或 IP 地址，然后单击**添加**。
8. 单击**陷阱**选项卡以打开**陷阱**对话框。
9. 从**社区名称**下拉列表中选择适当的 SNMP 社区名称，然后单击**陷阱目的地**列表框下面的**添加**。

   SNMP 服务配置框将显示。
10. 键入 IT Operations Analyzer 管理服务器的主机名或 IP 地址，然后单击**添加**。
11. 单击**确定**以关闭对话框。

在 Linux 环境下配置 SNMP 代理

要在 Red Hat Enterprise Linux 环境下配置 Dell 服务器的 SNMP 代理：

1. 将以下行添加到 **/etc/snmp/snmpd.conf** 配置文件：

   trapsink IP_address community_name

   IP_address 变量的值是 IT Operations Analyzer 管理服务器的 IP 地址。**community_name** 变量的值是 SNMP 社区名称。

2. 使用以下命令重新启动 SNMP 代理：

   /sbin/service snmpd restart

索引

V

Y

Z

Hitachi Data Systems

公司总部
2845 Lafayette Street
Santa Clara, California 95050-2639
U.S.A.
www.hds.com

区域联系信息

美洲
+1 408 970 1000
info@hds.com

欧洲、中东和非洲
+44 (0)1753 618000
info.emea@hds.com

亚太地区
+852 3189 7900
hds.marketing.apac@hds.com

Hitachi Data Systems

MK-90IOS006SC-12