HP Operations 系统基础结构 SPI

适用于 HP Operations Manager for Windows®、 HP-UX、 Linux 和 Solaris

软件版本：2.00

用户指南

文档发行日期：2011 年 5 月
软件发行日期：2011 年 5 月

法律声明

担保

HP 产品和服务担保声明随产品和服务明确呈示，且是唯一的呈示。此处任何内容都不得解释为其他担保。 HP 不对在此处包含的技术或编辑错误或者遗漏负责。

此处包含的信息将随时更改，恕不另行通知。

有限权利说明

机密计算机软件。必须具有 HP 提供的有效许可证才能拥有、使用或复制。基于 FAR 12.211 和 12.212，商业计算机软件、计算机软件文档和商业产品的技术数据均已获得美国政府的供应商标准商业许可证。

版权声明

商标声明

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

UNIX® 是 The Open Group 的注册商标。

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

文档更新

本文档的标题页包含以下标识信息：

- 软件版本号，表示软件版本。
- 文档发行日期，会随每次文档的更新而更改。
- 软件发行日期，表示此版本软件的发行日期。

要检查最近是否有更新或要验证使用的文档是否为最新版本，请转到：

http://h20230.www2.hp.com/selfsolve/manuals

此网站要求您注册获取 HP Passport，然后才能登录。要注册以获取 HP passport ID，请转到：

http://h20229.www2.hp.com/passport-registration.html

或在 HP Passport 登录页上单击 **New users - please register （新用户 - 请注册）**链接。

如果您订阅了相应的产品支持服务，还将接收到全新或更新的版本。有关详细信息，请联系 HP 销售代表。

支持

访问 HP Software Support Online 网站，网址是：

www.hp.com/go/hpsoftwaresupport

此网站提供联系信息以及有关 HP Software 提供的产品、服务和支持的详细信息。

HP Software Online Support 提供客户自解决功能。它为您提供一种快速高效的方法来访问交互式技术支持工具以管理您的业务。作为尊贵的支持客户，您可以通过使用支持网站受益：

- 搜索感兴趣的知识文档
- 提交和跟踪支持案例和增强功能请求
- 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
- 参加与其他软件客户的讨论
- 研究和注册软件培训

大多数支持区域要求您注册为 HP Passport 用户并登录。很多区域还要求提供支持合同。要注册以获取 HP Passport 用户 ID，请转到：

http://h20229.www2.hp.com/passport-registration.html

要查找有关访问级别的详细信息，请转到：

http://h20230.www2.hp.com/new_access_levels.jsp

目录

1 本文档中使用的约定

本文档使用以下约定。

约定	描述
HPOM for UNIX	本文档中使用 HPOM for UNIX 表示 HPOM on HP-UX、 HPOM on Linux 和 HPOM on Solaris。 需要时，会将特定操作系统区分为： • HPOM on HP-UX • HPOM on Linux • HPOM on Solaris
基础结构 SPI	HP Operations 基础结构 SPI。软件套件中包含了三个 SPI： • HP Operations 系统基础结构 SPI • HP Operations 虚拟基础结构 SPI • HP Operations 群集基础结构 SPI
SI SPI	HP Operations 系统基础结构 SPI
VI SPI	HP Operations 虚拟基础结构 SPI
CI SPI	HP Operations 群集基础结构 SPI
`%OvDataDir%`	Windows 管理服务器和被管节点上的数据目录变量。此变量由安装程序设置。用户可以根据需要重置路径。默认路径为：`C:\Documents and Settings\All Users\Application Data\HP\HP BTO Software`。

约定	描述
`$OvDataDir`	HPOM for UNIX 管理服务器和 UNIX 被管节点上的数据目录变量。此变量必须手动创建。所有 UNIX 节点和服务器上的数据目录如下所示： • HP-UX （节点和服务器）：`/var/opt/OV` • Linux （节点和服务器）：`/var/opt/OV` • Solaris （节点和服务器）：`/var/opt/OV` • AIX （节点）：`/var/opt/OV` 用户无法修改这些值。
`%OvInstallDir%`	Windows 管理服务器和被管节点上的安装目录变量。此变量由安装程序设置。用户可以根据需要重置路径。默认值为：`C:\Program Files\HP\HP BTO Software`。
`$OvInstalDir`	HPOM for UNIX 管理服务器和 UNIX 被管节点的安装目录变量。此变量必须手动创建。所有 UNIX 节点和服务器的安装目录如下所示： • HP-UX （节点和服务器）：`/opt/OV` • Linux （节点和服务器）：`/opt/OV` • Solaris （节点和服务器）：`/opt/OV` • AIX （节点）：`/usr/lpp/OV` 用户无法修改这些值。

2 简介

系统基础结构是构成企业的基础或基本基础结构，包括 CPU、操作系统、磁盘、内存和网络资源，并且需要不断地监视这些资源以确保底层物理系统的可用性、性能、安全性和平稳运行。监视系统基础结构能使您提高效率和生产力。而且有助于关联、识别和更正基础结构错误和性能下降的根本原因。

系统基础结构 SPI (SI SPI) 可监视 Microsoft Windows、 Linux、 Oracle Solaris、 IBM AIX 和 HP-UX 系统的系统基础结构。此 SI SPI 可以基于各种监视方面 （例如容量、可用性和利用率）来帮助分析系统性能。

SI SPI 属于 HP Operations 基础结构 SPI （基础结构 SPI）套件的一部分。套件中的其他组件包括：虚拟基础结构 SPI (VI SPI)、群集基础结构 SPI (CI SPI)、报告包和图形包。从基础结构 SPI 介质安装其他组件时会强制安装 SI SPI。

报告包不适用于 HPOM for Windows 9.00，因为 HP Reporter 不支持 64 位的安装程序。

SI SPI 可与其他 HP 软件产品集成，包括 HP Operations Manager (HPOM)、 HP Performance Manager、 HP Performance Agent 和 HP Operations Agent 的嵌入式性能组件 (EPC)。集成可提供策略、工具和服务视图的其他透视图。

有关系统基础结构 SPI 所支持的操作系统版本的信息，请参阅 《HP Operations 系统基础结构 SPI 发行说明》。

3 系统基础结构 SPI 组件

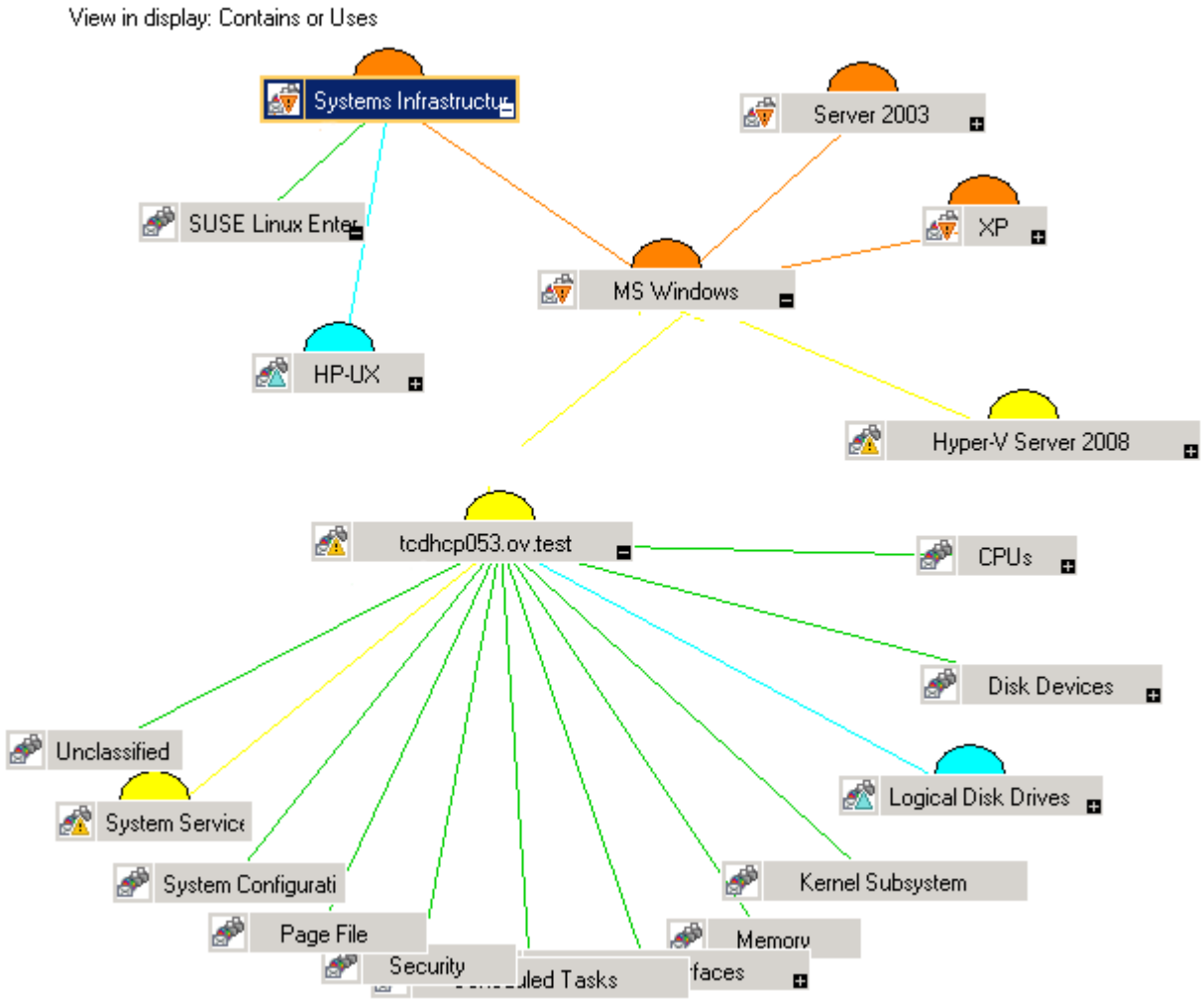
系统基础结构 SPI 提供预配置的策略和工具，可用于监视被管节点的操作、可用性和性能。将这些策略和工具与发现一起使用，可以快速控制 IT 基础结构的重要元素。

HPOM for Windows 上的图视图

将节点添加到 HPOM 控制台之后，系统基础结构 SPI 服务发现策略会自动部署到节点上，并将发现的信息添加到 HPOM 服务区域。此信息用于填充节点和服务的系统基础结构 SPI 图视图。

图视图显示了基础结构环境的实时状态。要查看图视图，请从 HPOM 控制台选择**服务**，并单击**系统基础结构**。图视图会图形化表示基础结构环境中整个服务或节点层次结构的结构视图，包括所有子系统和子服务。

图 1　　HPOM for Windows 上的图视图



图中的图标和线条是用颜色标注的，用来表示图中各个项目的严重性级别，并显示状态传播。可以使用图视图向下钻取到节点或服务层次结构中出现问题的级别。

服务视图中的已发现元素采用图形化表示，有助于迅速诊断问题。

- 要查看消息浏览器中任何已指示问题的根本原因，请单击**查看 → 根本原因**。
- 要显示受问题影响的服务和系统组件，请单击**查看 → 受影响的**。

HPOM for UNIX 上的图视图

图视图显示了基础结构环境的实时状态。要确保操作员能够查看 HPOM for HP-UX、 HPOM for Solaris 和 HPOM for Linux 操作 UI 中的服务图，请在管理服务器上运行以下命令：

```
opcservice -assign <操作员名称> SystemServices
```

其中，操作员名称是要将服务分配至的操作员的名称 （例如 opc_adm 或 opc_op）。

系统基础结构 SPI 服务发现策略不会自动将策略部署到节点。您可以进行手动部署。

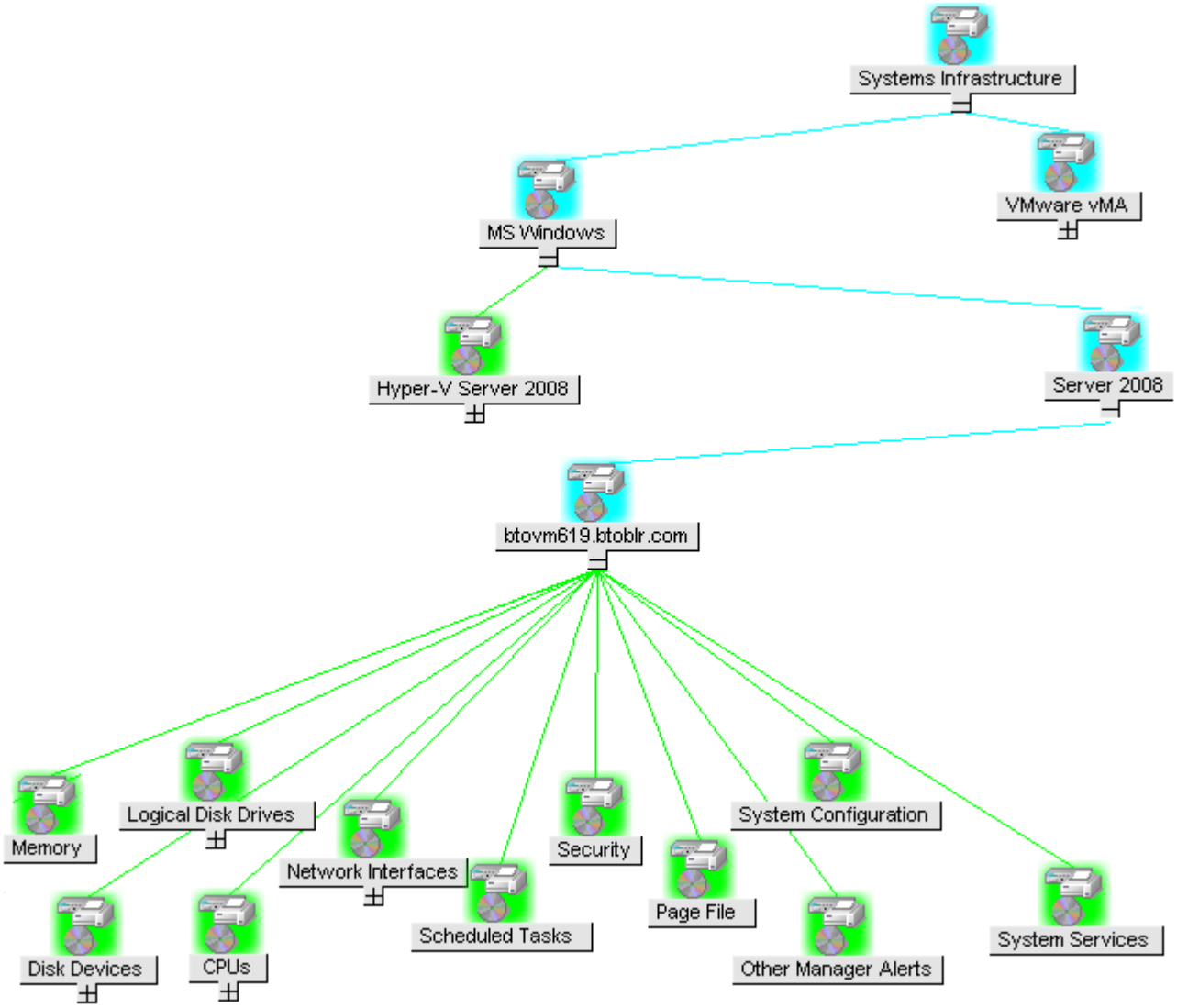
要查看图视图：

1 启动 HPOM 操作 UI。

2 使用您的用户名和密码登录。

3 选择**服务** → **系统基础结构** → **显示图形**可以查看图视图。

图 2 HPOM for UNIX/HPOM for Linux/HPOM for Solaris 上的图视图



图视图会图形化表示基础结构环境中整个服务或节点层次结构的结构视图，包括所有子系统和子服务。

工具

系统基础结构 SPI 工具将显示为特定被管节点收集的数据。有关系统基础结构 SPI 所提供工具的信息，请参阅系统基础结构 SPI 工具。

策略

对于 HPOM for Windows，安装过程中会将几个默认策略自动部署到支持的被管节点。这些策略可以按原样使用，用于开始从环境中接收与系统基础结构相关的数据和消息。在发现服务时，您可以选择关闭策略的自动部署。此外，您还可以修改预配置的策略并使用新名称进行保存，从而针对自己的特殊目的创建自定义策略。

有关从管理服务器部署策略的信息，请参阅从 HPOM for Windows 管理服务器部署 SI SPI。

对于 HPOM for UNIX/Linux/Solaris，系统基础结构 SPI 服务发现策略不会自动将策略部署到节点。您可以进行手动部署。

有关从管理服务器部署策略的信息，请参阅从 HPOM for UNIX 管理服务器部署 SI SPI 策略（第 103 页）。

系统基础结构 SPI 策略均以 SI 开头，易于识别和修改。策略类型如下：

- **服务 / 进程监视策略**，可监视系统服务和进程。
- **日志文件条目策略**，可捕获系统节点生成的状态 / 错误消息。
- **度量阈值策略**，可定义每个度量的条件，以便解释收集的度量值或在消息浏览器中显示警报 / 消息。每个度量阈值策略会比较实际度量值和指定的 / 自动阈值。如果阈值和实际度量值不匹配，则会生成消息和说明文本以帮助解决问题。
- **计划任务策略**，可确定要收集的度量值，以及开始收集度量的时间。此策略定义了收集间隔。收集间隔表示特定组的数据收集频率。计划任务策略有两个功能：一是达到每个收集间隔时在节点上运行收集器 / 分析器，二是为策略的**命令**文本框中列出的所有度量收集数据。
- **服务发现策略**，发现各个系统节点实例，并为所有系统基础结构 SPI 发现的实例建立图视图。

有关系统基础结构 SPI 所提供策略的详细信息，请参阅系统基础结构 SPI 策略。

图

使用系统基础结构 SPI 可使您能查看并跟踪受监视元素常规行为中出现不一致的根本原因。HPOM 可与 HP Performance Manager 集成，后者是一个基于 Web 的分析工具，可用于评估系统性能、观察使用趋势以及比较系统之间的性能。您可以使用 HP Performance Manager 查看：

- 图，例如折线图、柱状图或区域图
- 数据表，例如进程详细信息
- 基线图
- Java 格式的动态图形，允许您关闭单个度量的显示，或者悬停在图形某点以查看显示的值

通过查看图形化表示的数据，可以快捷地对报告的严重或紧急错误消息进行分析。有关系统基础结构 SPI 所提供图形的详细信息，请参阅系统基础结构 SPI 图形。

报告

您可以安装 HP Reporter 并与系统基础结构 SPI 集成，以生成基于 Web 的度量数据报告。

如果 HP Reporter 安装在用于 Windows 的 HPOM 管理服务器上，则可以从控制台查看报告。要查看报告，请在控制台树中展开**报告**，然后双击某个报告。

如果 HP Reporter 安装在连接到 HPOM 管理服务器（用于 Windows、UNIX、Linux 或 Solaris 操作系统）的单独系统上，则可以在 HP Reporter 系统上查看报告。有关 HP Reporter 与 HPOM 集成的详细信息，请参阅 《HP Reporter 安装和特殊配置指南》。

有关系统基础结构 SPI 所提供报告的信息，请参阅系统基础结构 SPI 报告。

4 系统基础结构 SPI 策略和工具

系统基础结构 SPI 提供了一系列管理基础结构的策略和工具。这些策略可用于监视系统，而工具可用于显示为系统收集的数据。

系统基础结构 SPI 策略

策略是用于自动监视的一个或一组规则。 SI SPI 策略可用于监视 Windows、 Linux、 Solaris、 AIX 和 HP-UX 环境中的系统。大多数策略适用于所有环境，但某些策略仅与特定的环境相关，应仅部署在相关平台上。将策略部署到不支持的平台可能会引发意外行为或导致策略失败。

“基础结构管理”组文件夹包含按照语言排列的子组。例如，英文策略的子组是 **en**、日文是 **ja**，而简体中文是 **zh**。

要访问 HPOM for UNIX/HPOM for Linux/HPOM for Solaris 的控制台或管理 UI 上的策略，请选择：

策略库 → 基础结构管理 → < *语言* > → 系统基础结构

有关从管理服务器部署策略的信息，请参阅从 HPOM for UNIX 管理服务器部署 SI SPI 策略（第 103 页）。

跟踪

用于监视容量和性能的策略包含跟踪的脚本参数：*Debug* 或 *DebugLevel*。使用此参数可以启用跟踪。可以指定以下任一值：

- Debug=0，将不会发送跟踪消息。
- Debug=1，将跟踪消息发送到控制台。
- Debug=2，将跟踪消息记录在被管节点的跟踪文件中。被管节点上的跟踪文件位置是 `$OvDataDir/Log`。

要查看脚本参数，请执行以下操作：

1 以根用户登录。

2 双击所需策略。此时将打开策略窗口。

3 选择 “脚本参数”选项卡。将列出该策略的脚本参数。

您还可以根据需要修改参数值。有关编辑脚本参数值的信息，请参阅 《HP Operations 基础结构 SPI 概念指南》。

发现策略

SI-SystemDiscovery 策略从被管节点 （例如硬件资源、操作系统属性和应用程序）收集服务信息。

节点添加到 HPOM 控制台的相应节点组后，随 SI-SystemDiscovery 策略一起部署的发现模块将在节点上运行服务发现。这些服务发现模块将以 XML 段的形式收集信息并发送回 HPOM。这些段将生成服务树，提供系统基础结构 SPI 发现进程运行时被管节点上所部署服务的快照。首次部署之后，自动发现策略便设置为定期运行。发现代理每次运行时都会将检索的服务信息与之前运行的结果进行比较。当发现代理程序发现被管节点上所运行服务自上次运行以来进行了更改或添加时，它会向 HPOM 管理服务器发送一条消息，后者便使用这些更改来更新服务视图。此策略的默认策略组为：

基础结构管理 → < *语言* > → 系统基础结构 → 自动发现

限制发现

SI-ConfigureDiscovery 策略是一种允许您包含或排除虚拟机上指定资源的发现的 ConfigFile 策略。

默认情况下， SI-SystemDiscovery 策略将发现节点上运行的所有服务和资源。但有时可能并不需要在服务图上显示所有资源。

为了限制发现的数量，必须在运行发现策略之前部署 SI-ConfigureDiscovery 策略。

SI-ConfigureDiscovery 策略具有配置切换功能，可以包含或排除跨基础结构 SPI 支持的所有虚拟技术的所有虚拟机资源。

将此策略部署到节点之后， `SIDiscovery.cfg` 配置文件将保存在以下文件夹中：

UNIX：`/var/opt/OV/conf/sispi/configuration`

Windows：`%Ovdatadir%\Data\conf\sispi\configuration`

如果 `/var/opt/OV/conf/sispi/configuration/` 文件夹中不存在 `SIDiscovery.cfg` 文件，则默认情况下 SI 发现将发现所有资源。

`SIDiscovery.cfg` 文件包含以下信息：

```
#To include or exclude a particular resource in SI discovery, add the
particular value under the respective Resource.
#The resources which can be restricted or expanded for being discovered are
mentioned below:
#
#File System
#Disk
#Network
#CPU
#
#The values which can be part of the INCLUDE and EXCLUDE parameters with
respect to each of the resources can be as follows:
#
```

```
#FS include or exclude parameters should contain File system path(In
general FS_DIRNAME value)
#Example:
#FS_INCLUDE:     /etc*Or
#FS_EXCLUDE:     /zones*
#
#DSK include or exclude parameters should contain name of the Disk
device(In general BYDSK_DEVNAME value)
#Example:
#DSK_INCLUDE:vdc0Or
#DSK_EXCLUDE:vdc1
#
#NET include or exclude parameters should contain Network Interface
name(In general BYNETIF_NAME value)
#Example:
#NET_INCLUDE:lo0Or
#NET_EXCLUDE:vnet0
#
#CPU include or exclude parameters should contain ID number of the CPU (In
general BYCPU_ID value)
#Example:
#CPU_INCLUDE:0,1Or
#CPU_EXCLUDE:2,3
#
#Multiple entries should be separate with comma -
#For example if one wants to exclude 2 of the File Systems, then the
following entry should configured:
#FS_INCLUDE:/zones*,/etc*
#
#Resource Name and value should be separated with ":" -
#For example if one wants to add FS_EXCLUDE, then the following entry
should be configured separated with ":"
#FS_EXCLUDE:     /zones*
#
#Different resources(_INCLUDE and _EXCLUDE) should be separated with
"===". As in the below case, FS, DSK, NET and CPU are
#separated with "==="
##########################################################################
##########################################################
===
FS_INCLUDE:
FS_EXCLUDE:     /zones*
===
DSK_INCLUDE:
DSK_EXCLUDE:
===
NET_INCLUDE:
NET_EXCLUDE:
===
CPU_INCLUDE:
CPU_EXCLUDE:
```

要发现或不发现资源，请按照文件中提供的说明编辑 SIDiscovery.cfg 文件。

如果在 INCLUDE 参数下面提供特定资源名称，则 SI 发现将仅发现这些资源并显示在服务图中。如果在 EXCLUDE 参数下面提供特定资源名称，则 SI 发现不会发现这些资源，也不会显示在服务图中。

指定资源名称时，可以使用完整资源名称，也可以使用通配符 (*****)。

您只能设置一个参数：EXCLUDE 或 INCLUDE。如果为两个参数都设置了值或都未设置值，则默认情况下 SI 发现策略将发现所有资源。

如果为 INCLUDE 参数设置了错误的实例值，则 SI 发现不会发现指定的资源实例，而且会向 HPOM 控制台发送如下严重性为 “警告” 的警报消息：

```
Improper usage as _INLUCDE parameter is not having the correct value.
```

但是，如果为 EXCLUDE 参数设置了错误的实例值，则 SI 发现将发现该资源实例。

如果 **SI-SystemDiscovery** 策略无法打开或读取 `SIDiscovery.cfg` 文件，则它会向 HPOM 控制台发送严重性为 “警告” 的如下警报消息：

```
Improper usage as both _INCLUDE and _EXCLUDE are configured.
```

示例

假定某 Oracle Solaris 容器具有三个非全局区域，称为 emailserver、webserver1 和 webserver2，则可能存在如下的几个文件系统：

```
/etc/svc/volatile
/tmp
/var/run
/zones/emailserver/root/etc/svc/volatile
/zones/emailserver/root/tmp
/zones/emailserver/root/var/run
/zones/webserver1/root/etc/svc/volatile
/zones/webserver1/root/tmp
/zones/webserver1/root/var/run
/zones/webserver2/root/etc/svc/volatile
/zones/webserver2/root/tmp
/zones/webserver2/root/var/run
```

- 如果只需要发现特定的文件系统，则可通过为 INCLUDE 参数输入以下*任一*值来修改 `SIDiscovery.cfg` 文件而实现：
  - `FS_INCLUDE`: **`/zones/webserver2*`**
  - `FS_INCLUDE`: **`/zones/webserver2/root/etc/svc/volatile`**
- 如果不需要发现特定的文件系统，则可通过为 EXCLUDE 参数输入以下*任一*值来修改 `SIDiscovery.cfg` 文件而实现：
  - `FS_EXCLUDE`: **`/zones/emailserver*`**
  - `FS_EXCLUDE`: **`/zones/emailserverroot/tmp`**

可用性策略

可用性监视帮助确保足够的资源可用性。识别出不可接受的资源可用性级别非常重要。将计算 IT 基础结构上的当前负载，并与阈值级别相比较，然后确定资源可用性是否存在不足。

随着 IT 资源利用率的变化和功能的改进，磁盘空间量、处理能力、内存及其他参数也会随之变化。了解当前需求以及需求如何随时间变化是非常重要的。监视一段时间内这些方面的变化情况有助于了解它们对 IT 资源利用率的影响。

服务器角色描述了诸如传真服务器、电子邮件服务器等服务器的主要功能。一个系统可以安装一个或多个服务器角色，每个服务器角色可以包括记为角色子元素的一个或多个角色服务。可用性策略将监视被管节点上角色服务的可用性。

如果系统基础结构 SPI 在选定节点上发现由预配置的可用性策略管理的角色服务，则这些策略将自动安装。这些策略的默认策略组为：

基础结构管理 → < *语言* > → 系统基础结构 → 可用性

可用性策略将监视 Linux、Windows、Solaris、AIX 和 HP-UX 被管节点上进程和服务的可用性。当进程不可用或服务状态发生变化 （例如从 “正在运行” 变成 “已停止” 或 “已禁用”）时，此策略会向 HPOM 发送消息。如果状态更改，则可定义要监视的状态和要采取的操作。

可用性策略根据服务器角色分组，并根据操作系统划分子组。可以根据被管节点上的操作系统选择所需的策略。

策略监视进程和服务

这些策略的默认策略组包括：

- **基础结构管理 → < *语言* > → 系统基础结构 → 可用性 → < *进程 / 服务* > → < *操作系统* >**
- **基础结构管理 → < *语言* > → 系统基础结构 → 按供应商分组的策略 → < *操作系统* > - 高级**

此处的 **< 操作系统 >** 指的是 AIX、HP-UX、RHEL、SLES、Windows 或 Solaris 操作系统。下表列出了受支持平台上提供的进程和服务以及相应的监视策略。

基础结构 SPI 为 Solaris 区域上的进程监视提供了可用性策略。 Solaris 计算机有全局和局部区域（或容器）。这些策略将监视 Solaris 进程的可用性，并在进程不可用时向 HPOM 发送警报消息。

表 1　　用于 AIX 的监视策略

进程 / 服务名称	监视策略
DHCP 服务器	SI-AIXDHCPProcessMonitor
DNS 服务器	SI-AIXNamedProcessMonitor
电子邮件服务	SI-AIXSendmailProcessMonitor
传真服务	-
文件服务	SI-AIXNfsServerProcessMonitor
防火墙服务	-
Internet 服务	SI-AIXInetdProcessMonitor
网络服务	-
打印服务	• SI-AIXQdaemonProcessMonitor • SI-AIXLpdProcessMonitor

表 1　　用于 AIX 的监视策略

进程 / 服务名称	监视策略
RPC 服务	SI-AIXPortmapProcessMonitor
计划作业服务	SI-AIXCronProcessMonitor
安全登录服务	SI-OpenSshdProcessMonitor[1]
SNMP 服务	SI-UnixSnmpdProcessMonitor
系统记录器	SI-AIXSyslogProcessMonitor
终端服务	-
Web 服务器	SI-AIXWebserverProcessMonitor

表 2　　用于 HP-UX 的监视策略

进程 / 服务名称	监视策略
DHCP 服务器	SI-HPUXBootpdProcessMonitor
DNS 服务器	SI-HPUXNamedProcessMonitor
电子邮件服务	SI-HPUXSendmailProcessMonitor
传真服务	-
文件服务	SI-HPUXNfsServerProcessMonitor
防火墙服务	-
Internet 服务	SI-HPUXInetdProcessMonitor
网络服务	-
打印服务	SI-HPUXLpschedProcessMonitor
RPC 服务	-
计划作业服务	SI-HPUXCronProcessMonitor
安全登录服务	• SI-HPUXSshdProcessMonitor • SI-OpenSshdProcessMonitor[1]
SNMP 服务	SI-UnixSnmpdProcessMonitor
系统记录器	SI-HPUXSyslogProcessMonitor
终端服务	-
Web 服务器	SI-HPUXWebserverProcessMonitor

表 3　　用于 RHEL 的监视策略

进程 / 服务名称	监视策略
DHCP 服务器	SI-LinuxDHCPProcessMonitor
DNS 服务器	SI-LinuxNamedProcessMonitor
电子邮件服务	SI-LinuxSendmailProcessMonitor
传真服务	-
文件服务	• SI-LinuxNfsServerProcessMonitor • SI-LinuxSmbServerProcessMonitor
防火墙服务	-
Internet 服务	SI-LinuxXinetdProcessMonitor
网络服务	-
打印服务	SI-LinuxCupsProcessMonitor
RPC 服务	-
计划作业服务	SI-RHELCronProcessMonitor
安全登录服务	• SI-LinuxSshdProcessMonitor • SI-OpenSshdProcessMonitor[1]
SNMP 服务	SI-UnixSnmpdProcessMonitor
系统记录器	SI-RHELSyslogProcessMonitor
终端服务	-
Web 服务器	SI-LinuxWebserverProcessMonitor

表 4　　用于 SLES 的监视策略

进程 / 服务名称	SLES
DHCP 服务器	SI-LinuxDHCPProcessMonitor
DNS 服务器	SI-LinuxNamedProcessMonitor
电子邮件服务	SI-LinuxSendmailProcessMonitor
传真服务	-
文件服务	• SI-LinuxNfsServerProcessMonitor • SI-LinuxSmbServerProcessMonitor
防火墙服务	-
Internet 服务	SI-LinuxXinetdProcessMonitor
网络服务	-

表 4　　用于 SLES 的监视策略

进程 / 服务名称	SLES
打印服务	SI-LinuxCupsProcessMonitor
RPC 服务	-
计划作业服务	SI-SLESCronProcessMonitor
安全登录服务	• SI-LinuxSshdProcessMonitor • SI-OpenSshdProcessMonitor[1]
SNMP 服务	SI-UnixSnmpdProcessMonitor
系统记录器	SI-SLESSyslogProcessMonitor
终端服务	-
Web 服务器	SI-LinuxWebserverProcessMonitor

表 5　　用于 Solaris 的监视策略

进程 / 服务名称	监视策略
DHCP 服务器	SI-SunSolarisDHCPProcessMonitor
DNS 服务器	SI-SunSolarisNamedProcessMonitor
电子邮件服务	SI-SunSolarisSendmailProcessMonitor
传真服务	-
文件服务	SI-SunSolarisNfsServerProcessMonitor
防火墙服务	-
Internet 服务	SI-SunSolarisInetdProcessMonitor
网络服务	-
打印服务	SI-SunSolarisLpdProcessMonitor
RPC 服务	-
计划作业服务	SI-SunSolarisCronProcessMonitor
安全登录服务	• SI-SunSolarisSshdProcessMonitor • SI-OpenSshdProcessMonitor[1]
SNMP 服务	SI-UnixSnmpdProcessMonitor
系统记录器	SI-SunSolarisSyslogProcessMonitor
终端服务	-
Web 服务器	SI-SunSolarisWebserverProcessMonitor

表 6　　用于 Windows 的监视策略

进程 / 服务名称	监视策略
DHCP 服务器	SI-MSWindowsDHCPServerRoleMonitor
DNS 服务器	SI-MSWindowsDNSServerRoleMonitor
电子邮件服务	-
传真服务	SI-MSWindowsFaxServerRoleMonitor
文件服务	• SI-MSWindowsWin2k3FileServicesRoleMonitor • SI-MSWindowsDFSRoleMonitor • SI-MSWindowsFileServerRoleMonitor • SI-MSWindowsNFSRoleMonitor
防火墙服务	SI-MSWindowsFirewallRoleMonitor
Internet 服务	-
网络服务	• SI-MSWindowsRRAServicesRoleMonitor • SI-MSWindowsNetworkPolicyServerRoleMonitor
打印服务	SI-MSWindowsPrintServiceRoleMonitor
RPC 服务	SI-MSWindowsRpcRoleMonitor
计划作业服务	SI-MSWindowsTaskSchedulerRoleMonitor
安全登录服务	SI-OpenSshdProcessMonitor[1]
SNMP 服务	SI-MSWindowsSnmpProcessMonitor
系统记录器	SI-MSWindowsEventLogRoleMonitor
终端服务	• SI-MSWindowsTSWebAccessRoleMonitor • SI-MSWindowsTSGatewayRoleMonitor • SI-MSWindowsTerminalServerRoleMonitor • SI-MSWindowsTSLicensingRoleMonitor
Web 服务器	SI-MSWindowsWebServerRoleMonitor

[1]AIX、HP-UX、Linux、MS windows 和 Solaris 操作系统均支持此策略。请确保在将此策略部署到任何支持的平台之前，先安装 *openssh* 包。

将用于 Solaris 的当前进程监视策略部署到全局区域后，SI SPI 将监视全局区域和非全局区域中运行的所有进程，不对进程所属的区域进行区分。因此，要监视全局区域中运行的进程，阈值级别必须设置为包括非全局进程。

例如：如果有 x 个非全局区域 （从属于全局区域）进程，则阈值级别必须设置为包括全局和非全局区域的所有进程，即为 x+1 个。

如果将同一策略部署到全局和非全局区域 （其中非全局区域从属于全局区域），则您会收到重复警报。

非全局区域不支持的策略

- SI-CPUSpikeCheck
- SI-PerNetifInbyteBaseline-AT
- SI-PerNetifOutbyteBaseline-AT
- SI-PerDiskAvgServiceTime-AT
- SI-PerDiskUtilization-AT

硬件监视策略

系统基础结构 SPI 2.00 提供的策略可用于监视 HP ProLiant 服务器的运行状况和状态。这些策略将监视 SIM 代理程序生成的 SNMP 陷阱，并向 HPOM 控制台发送警报消息。所有这些策略均为 SNMP 拦截器类型。

这些策略的默认策略组为：

基础结构管理 → < *语言* > → **系统基础结构** → **硬件** → **HP ProLiant**

所需配置：

- 确保 SNMP 服务已启动并正在运行。
- 要启用硬件监视，请打开节点上的 `xpl config` 文件，并在 `eaagt` 命名空间下添加如下行：
  - 如果使用的是 HP Operations Agent 8.60，请添加：

    ```
    [eaagt]
    SNMP_SESSION_MODE=NO_TRAPD
    ```

  - 如果使用的是 HP Operations Agent 11.00，请添加：

    ```
    [eaagt]
    SNMP_SESSION_MODE=NETSNMP
    ```

- 在安装 SIM 代理程序的 Linux 节点上，打开位于 `/etc/snmp/snmpd.conf` 的 SNMP 配置文件，并在结尾处追加以下行：

  `trapsink` < *节点的主机名* >
- 在 Windows 节点上，检查是否安装了以下 SIM 代理程序：
  - Foundation Agent
  - NIC Agent
  - Server Agent

- Storage Agent

如果未安装，请安装适用于 Windows Servers 2003/2008 x64 版本的 HP Insight Management。

服务器运行状况陷阱监视策略

SI-HPProLiant_CPQHLTHTraps

SI-HPProLiant_CPQHLTHTraps 策略将拦截与服务器运行状况相关的 SNMP 陷阱，每次生成陷阱后便向 HPOM 控制台发送警报。此策略将监视以下 SNMP 陷阱：

MIB ID	SNMP 陷阱描述
1.3.6.1.2.1.11.6.0	coldStart。
1.3.6.1.2.1.11.6.1	warmStart。
1.3.6.1.2.1.11.6.2	linkDown。
1.3.6.1.2.1.11.6.3	linkUp。
1.3.6.1.4.1.232.0.6003	系统将由于此热状态而关闭。
1.3.6.1.4.1.232.0.6017	系统将由于此热状态而关闭。
1.3.6.1.4.1.232.0.6004	温度超出范围，可能发生关闭。
1.3.6.1.4.1.232.0.6018	温度超出范围，可能发生关闭。
1.3.6.1.4.1.232.0.6019	温度已恢复到正常范围。
1.3.6.1.4.1.232.0.6005	温度已恢复到正常范围。
1.3.6.1.4.1.232.0.6040	SNMP Varbind 3 所含基板和 SNMP Varbind 4 所含位置上的温度状态为失败。
1.3.6.1.4.1.232.0.6041	SNMP Varbind 4 所含基板和 SNMP Varbind 5 所含位置上的温度状态已降级。
1.3.6.1.4.1.232.0.6041	SNMP Varbind 4 所含基板和 SNMP Varbind 5 所含位置上的温度超出范围。可能不久会发生关闭。
1.3.6.1.4.1.232.0.6042	SNMP Varbind 3 所含基板和 SNMP Varbind 4 所含位置上的温度正常。
1.3.6.1.4.1.232.0.6007	可选风扇未正常运转。
1.3.6.1.4.1.232.0.6021	可选风扇未正常运转。
1.3.6.1.4.1.232.0.6006	需要的风扇未正常运转。可能发生关闭。
1.3.6.1.4.1.232.0.6020	需要的风扇未正常运转。
1.3.6.1.4.1.232.0.6020	系统风扇发生故障。
1.3.6.1.4.1.232.0.6022	系统风扇已恢复到正常运转状态。
1.3.6.1.4.1.232.0.6008	系统风扇已恢复到正常运转状态。
1.3.6.1.4.1.232.0.6009	CPU 风扇发生故障，服务器将关闭。

MIB ID	SNMP 陷阱描述
1.3.6.1.4.1.232.0.6010	CPU 风扇现在正常。
1.3.6.1.4.1.232.0.6023	CPU 风扇发生故障，服务器将关闭。
1.3.6.1.4.1.232.0.6024	CPU 风扇现在正常。
1.3.6.1.4.1.232.0.6035	SNMP Varbind 3 所含基板上的风扇和 SNMP Varbind 4 所含风扇已降级。
1.3.6.1.4.1.232.0.6036	SNMP Varbind 3 所含基板上的风扇和 SNMP Varbind 4 所含风扇发生故障。
1.3.6.1.4.1.232.0.6037	SNMP Varbind 3 所含基板上的风扇不再冗余。
1.3.6.1.4.1.232.0.6055	对于指定基板，容错风扇已返回到冗余状态。
1.3.6.1.4.1.232.0.6048	SNMP Varbind 3 中的基板上的电源正常。
1.3.6.1.4.1.232.0.6049	SNMP Varbind 3 中的基板上的电源已降级。
1.3.6.1.4.1.232.0.6050	SNMP Varbind 3 中的基板上的电源发生故障。
1.3.6.1.4.1.232.0.6014	服务器电源状态已变为降级。
1.3.6.1.4.1.232.0.6028	服务器电源状态已变为降级。
1.3.6.1.4.1.232.0.6030	SNMP Varbind 3 所含基板和 SNMP Varbind 4 所含隔舱上的电源已降级。
1.3.6.1.4.1.232.0.6054	容错电源的电源冗余已恢复。
1.3.6.1.4.1.232.0.6031	SNMP Varbind 3 所含基板和 SNMP Varbind 4 所含隔舱上的电源发生故障。
1.3.6.1.4.1.232.0.6032	SNMP Varbind 3 所含基板上的电源不再冗余。
1.3.6.1.4.1.232.0.6043	SNMP Varbind 3 中的基板上、 SNMP Varbind 4 中的插槽上和 SNMP Varbind 5 中的插座上的电源转换器已降级。
1.3.6.1.4.1.232.0.6044	SNMP Varbind 3 中的基板上、 SNMP Varbind 4 中的插槽上和 SNMP Varbind 5 中的插座上的电源转换器发生故障。
1.3.6.1.4.1.232.0.6045	SNMP Varbind 3 所含基板上的电源转换器不再冗余。
1.3.6.1.4.1.232.0.6012	在热关闭后，服务器再次可操作。
1.3.6.1.4.1.232.0.6027	在服务器重新启动期间发生错误。
1.3.6.1.4.1.232.0.6059	检测到内存板或匣总线错误。
1.3.6.1.4.1.232.0.6063	管理处理器未能重置。
1.3.6.1.4.1.232.0.6025	在 ASR 关闭之后，服务器再次可操作。
1.3.6.1.4.1.232.0.6016	内存错误太多，跟踪现在已禁用。
1.3.6.1.4.1.232.0.6016	错误跟踪现在已启用。

MIB ID	SNMP 陷阱描述
1.3.6.1.4.1.232.0.6002	内存错误太多，跟踪现在已禁用。
1.3.6.1.4.1.232.0.6026	在热关闭后，服务器再次可操作。
1.3.6.1.4.1.232.0.6061	管理处理器当前正在重置。
1.3.6.1.4.1.232.0.6062	管理处理器已就绪。
1.3.6.1.4.1.232.0.6013	在服务器重新启动期间发生错误。

对于以上每个 SNMP 陷阱，此策略均包含一条规则。问题解决之后，将自动确认之前的警报消息。

RAID 控制器陷阱监视策略

SI-HPProLiant_CPQRCTraps

SI-HPProLiant_CPQRCTraps 策略将拦截与 RAID 控制器的性能和可用性相关的 SNMP 陷阱，每次生成陷阱后便向 HPOM 控制台发送警报。此策略将监视以下陷阱：

MIB ID	SNMP 陷阱描述
1.3.6.1.4.1.232.141.3.8.0.27	扩展柜中的温度已触发临界状态，控制器已检测到此情况。
1.3.6.1.4.1.232.141.3.8.6.26	cpqCrExpCabTemperatureWarningTrap。
1.3.6.1.4.1.232.141.3.8.0.22	扩展柜中的某个电源发生故障。
1.3.6.1.4.1.232.141.3.8.0.20	扩展柜中的风扇发生故障。
1.3.6.1.4.1.232.141.3.7.0.25	主柜中的温度已恢复到正常范围。
1.3.6.1.4.1.232.141.3.2.0.2	子系统中的主控制器已恢复。
1.3.6.1.4.1.232.141.3.8.0.29	扩展柜中的某个电源已恢复。
1.3.6.1.4.1.232.141.3.3.0.6	RAIDset 发生故障，并脱机。
1.3.6.1.4.1.232.141.3.8.0.28	扩展柜中的温度已恢复到正常范围。
1.3.6.1.4.1.232.141.3.2.0.1	子系统中的主控制器发生故障。
1.3.6.1.4.1.232.141.3.7.0.16	主柜中的某个散热风扇发生故障。
1.3.6.1.4.1.232.141.3.2.0.4	子系统中的辅助控制器已恢复。
1.3.6.1.4.1.232.141.3.7.0.19	主柜中的某个电源已恢复。
.1.3.6.1.4.1.232.141.3.5.6.31	cpqCrPhyDiskFailureTrap。
1.3.6.1.4.1.232.141.3.7.0.24	主柜中的温度已触发临界状态，控制器已检测到此情况。

MIB ID	SNMP 陷阱描述
1.3.6.1.4.1.232.141.3.5.0.10	磁盘设备已恢复。
1.3.6.1.4.1.232.141.3.7.0.17	主柜中的某个散热风扇已恢复。
1.3.6.1.4.1.232.141.3.5.6.30	cpqCrPhyDiskInformationTrap。
1.3.6.1.4.1.232.141.3.2.0.3	子系统中的辅助控制器发生故障。
1.3.6.1.4.1.232.141.3.8.0.21	扩展柜中的某个散热风扇已恢复。
1.3.6.1.4.1.232.141.3.5.0.11	磁盘设备发生故障。
1.3.6.1.4.1.232.141.3.7.0.23	主柜温度警告。
1.3.6.1.4.1.232.141.3.7.0.18	主柜中的某个电源发生故障。

对于以上每个 SNMP 陷阱，此策略均包含一条规则。问题解决之后，将自动确认之前的警报消息。

NIC 陷阱监视策略

SI-HPProLiant_CPQNICTraps

SI-HPProLiant_CPQNICTraps 策略将拦截与网络接口卡 (NIC) 的性能和可用性相关的 SNMP 陷阱，每次生成陷阱后便向 HPOM 控制台发送警报。此策略将监视以下陷阱：

MIB ID	SNMP 陷阱描述
1.3.6.1.4.1.232.0.11005	NIC 状态良好。
1.3.6.1.4.1.232.0.11006	NIC 状态失败。
1.3.6.1.4.1.232.0.11007	发生了 NIC 切换。
1.3.6.1.4.1.232.0.11008	NIC 状态良好。
1.3.6.1.4.1.232.0.11009	NIC 状态失败。
1.3.6.1.4.1.232.0.11010	NIC 切换。
1.3.6.1.2.1.11.6.2	linkDown。
1.3.6.1.2.1.11.6.3	linkUp。
1.3.6.1.4.1.232.0.18006	对于 SNMP Varbind 3 所含插槽中的逻辑适配器和 SNMP Varbind 4 所含端口，连接已丢失。
1.3.6.1.4.1.232.6.18012	cpqNic3ConnectivityLost。
1.3.6.1.4.1.232.6.18011	cpqNic3ConnectivityRestored。
1.3.6.1.4.1.232.0.18009	检测到 NIC 类似病毒活动时发送的陷阱。
1.3.6.1.4.1.232.0.18010	不再检测到 NIC 类似病毒活动时发送的陷阱。

对于以上每个 SNMP 陷阱，此策略均包含一条规则。问题解决之后，将自动确认之前的警报消息。

CMC 陷阱监视策略

SI-HPProLiant_CPQCMCTraps

SI-HPProLiant_CPQCMCTraps 策略将拦截与控制台管理控制器 (CMC) 在耗电量、烟量、湿度、温度和风扇等方面的运行状况相关的 SNMP 陷阱，每次生成陷阱后该策略便向 HPOM 控制台发送警报。

它将监视以下陷阱：

MIB ID	SNMP 陷阱描述
1.3.6.1.4.1.232.153.0.153013	CMC 检测到机架中烟的存在状态为 “存在”，此状态包含在 SNMP Varbind 5 中。
1.3.6.1.4.1.232.153.0.153013	CMC 检测到机架中烟的存在状态为 “正常”，此状态包含在 SNMP Varbind 5 中。
1.3.6.1.4.1.232.153.0.153005	CMC 的电压状态为 “超过最大值”，此状态包含在 SNMP Varbind 5 中。
1.3.6.1.4.1.232.153.0.153005	CMC 的电压状态为 “低于最小值”，此状态包含在 SNMP Varbind 5 中。
1.3.6.1.4.1.232.153.0.153005	CMC 的电压状态为 “正常”，此状态包含在 SNMP Varbind 5 中。
1.3.6.1.4.1.232.153.0.153001	CMC 温度传感器 1 探测到机架中的温度已超过最大阈值，此状态包含在 SNMP Varbind 5 中。
1.3.6.1.4.1.232.153.0.153001	CMC 温度传感器 1 探测到机架中的温度已低于最小阈值，此状态包含在 SNMP Varbind 5 中。
1.3.6.1.4.1.232.153.0.153002	CMC 温度传感器 1 探测到机架中的温度为 “正常”，此状态包含在 SNMP Varbind 5 中。
1.3.6.1.4.1.232.153.0.153002)	CMC 温度传感器 2 探测到机架中的温度已超过最大阈值，此状态包含在 SNMP Varbind 5 中。
1.3.6.1.4.1.232.153.0.153002	CMC 温度传感器 2 探测到机架中的温度已低于最小阈值，此状态包含在 SNMP Varbind 5 中。
1.3.6.1.4.1.232.153.0.153002	CMC 温度传感器 2 探测到机架中的温度为 “正常”，此状态包含在 SNMP Varbind 5 中。
1.3.6.1.4.1.232.153.0.153006	湿度的状态为 “超过最大值”，此状态包含在 SNMP Varbind 5 中。
1.3.6.1.4.1.232.153.0.153006	湿度的状态为 “低于最小值”，此状态包含在 SNMP Varbind 5 中。
1.3.6.1.4.1.232.153.0.153006	湿度的状态为 “正常”，此状态包含在 SNMP Varbind 5 中。

MIB ID	SNMP 陷阱描述
1.3.6.1.4.1.232.153.0.153003	机架中风扇 1 的状态为 “正常”，此状态包含在 SNMP Varbind 5 中。
1.3.6.1.4.1.232.153.0.153003	机架中风扇 1 的状态为 “自动关闭”，此状态包含在 SNMP Varbind 5 中。
1.3.6.1.4.1.232.153.0.153003	机架中风扇 1 的状态为 “因烟关闭”，此状态包含在 SNMP Varbind 5 中。
1.3.6.1.4.1.232.153.0.153003	机架中风扇 1 的状态为 “因门关闭”，此状态包含在 SNMP Varbind 5 中。
1.3.6.1.4.1.232.153.0.153004	机架中风扇 2 的状态为 “自动打开”，此状态包含在 SNMP Varbind 5 中。
1.3.6.1.4.1.232.153.0.153004	机架中风扇 2 的状态为 “自动关闭”，此状态包含在 SNMP Varbind 5 中。
1.3.6.1.4.1.232.153.0.153004	机架中风扇 2 的状态为 “因烟关闭”，此状态包含在 SNMP Varbind 5 中。
1.3.6.1.4.1.232.153.0.153004	机架中风扇 2 的状态为 “因门关闭”，此状态包含在 SNMP Varbind 5 中。

对于以上每个 SNMP 陷阱，此策略均包含一条规则。问题解决之后，将自动确认之前的警报消息。

系统信息陷阱监视策略

SI-HPProLiant_CPQSysInfoTraps

SI-HPProLiant_CPQSysInfoTraps 策略会拦截与系统信息相关的、关于电池、监视器、热插槽板、内存和外罩的状态的 SNMP 陷阱。每次生成陷阱后该策略便向 HPOM 控制台发送警报。

它将监视以下陷阱：

MIB ID	SNMP 陷阱描述
1.3.6.1.4.1.232.0.2012	SNMP Varbind 3 中所含电池的充电容量已降级。
1.3.6.1.4.1.232.0.2011	SNMP Varbind 3 中所含的电池已发生故障。
1.3.6.1.4.1.232.0.2013	SNMP Varbind 3 中所含的电池存在校准错误。
1.3.6.1.4.1.232.0.2003	监视器状态已经设置为降级。
1.3.6.1.4.1.232.0.2004	监视器状态已经设置为故障。
1.3.6.1.4.1.232.0.2002	监视器状态已经设置为正常。
1.3.6.1.4.1.232.0.2006	内存模块 ECC 状态已经设置为正常。
1.3.6.1.4.1.232.0.2005	内存模块 ECC 状态已设置为降级。
1.3.6.1.4.1.232.0.2009	热插槽板插入到 SNMP Varbind 3 中所含的基板、 SNMP Varbind 4 中所含的插槽。

MIB ID	SNMP 陷阱描述
1.3.6.1.4.1.232.0.2010	SNMP Varbind 3 中所含基板、 SNMP Varbind 4 中所含插槽上的热插槽板发生故障，错误包含在 SNMP ind 5 中。
1.3.6.1.4.1.232.0.2008)	热插槽板已从基板取出。
1.3.6.1.4.1.232.0.2007	系统的内存配置已更改。
1.3.6.1.4.1.232.0.2001	从部件除去了外罩。

对于以上每个 SNMP 陷阱，此策略均包含一条规则。问题解决之后，将自动确认之前的警报消息。

虚拟连接域陷阱监视策略

SI-HPProLiant_VCDomainTraps

The SI-HPProLiant_VCDomainTraps 策略拦截与虚拟连接域有关的 SNMP 陷阱。每次生成陷阱后该策略便向 HPOM 控制台发送警报。

它将监视以下陷阱：

MIB ID	SNMP 陷阱描述
1.3.6.1.4.1.11.5.7.5.2.1.2.0.5	vcFcFabricManagedStatusChange
1.3.6.1.4.1.11.5.7.5.2.1.2.0.3	vcCheckpointCompleted
1.3.6.1.4.1.11.5.7.5.2.1.2.0.9	vcProfileManagedStatusChange
1.3.6.1.4.1.11.5.7.5.2.1.2.0.6	vcModuleManagedStatusChange
1.3.6.1.4.1.11.5.7.5.2.1.2.0.8	vcPhysicalServerManagedStatusChange
1.3.6.1.4.1.11.5.7.5.2.1.2.0.1	vcDomainManagedStatusChange
1.3.6.1.4.1.11.5.7.5.2.1.2.0.2	vcCheckpointTimeout

对于以上每个 SNMP 陷阱，此策略均包含一条规则。问题解决之后，将自动确认之前的警报消息。

群集陷阱监视策略

SI-HPProLiant_CPQCLUSTraps

SI-HPProLiant_CPQCLUSTraps 策略会拦截与电池、监视、热插槽板、内存和引擎罩状态方面群集相关的 SNMP 陷阱。每次生成陷阱后该策略便向 HPOM 控制台发送警报。

它将监视以下陷阱：

MIB ID	SNMP 陷阱描述
1.3.6.1.4.1.232.0.15001	SNMP Varbind 3 中所含群集性能下降。
1.3.6.1.4.1.232.0.15002	SNMP Varbind 3 中所含群集故障。
1.3.6.1.4.1.232.0.15003	SNMP Varbind 3 中所含群集服务性能下降。
1.3.6.1.4.1.232.0.15004	SNMP Varbind 3 中所含节点上的群集服务故障。
1.3.6.1.4.1.232.0.15007	SNMP Varbind 3 中所含群集资源性能下降。
1.3.6.1.4.1.232.0.15005	SNMP Varbind 3 中所含群集资源故障。
1.3.6.1.4.1.232.0.15008	SNMP Varbind 3 中所含群集网络性能下降。
1.3.6.1.4.1.232.0.15006	SNMP Varbind 3 中所含群集网络故障。

对于以上每个 SNMP 陷阱，此策略均包含一条规则。问题解决之后，将自动确认之前的警报消息。

机架电源管理器陷阱监视策略

SI-HPProLiant_CPQRPMTraps

The SI-HPProLiant_CPQRPMTraps 策略拦截与机架电源管理器有关的 SNMP 陷阱。每次生成陷阱后该策略便向 HPOM 控制台发送警报。

它将监视以下陷阱：

MIB ID	SNMP 陷阱描述
1.3.6.1.4.1.232.154.2.1	UPS 设备正在报告连接丢失
1.3.6.1.4.1.232.154.2.2	UPS 设备正在报告连接丢失
1.3.6.1.4.1.232.154.2.3	CRPM 未能找到设备主机名的 IP 地址
1.3.6.1.4.1.232.154.2.4	CRPM 未能连接到设备
1.3.6.1.4.1.232.154.2.5	cpqRPMTrapDeviceSettingsChanged
1.3.6.1.4.1.232.154.2.10001	CMC 设备正在报告温度 1 低于最小阈值
1.3.6.1.4.1.232.154.2.10002	CMC 设备正在报告温度 1 高于警告阈值
1.3.6.1.4.1.232.154.2.10003	CMC 设备正在报告温度 1 高于最大阈值
1.3.6.1.4.1.232.154.2.10004	CMC 设备正在报告温度 1 已恢复到正常温度

MIB ID	SNMP 陷阱描述
1.3.6.1.4.1.232.154.2.10005	CMC 设备正在报告温度 2 低于最小阈值
1.3.6.1.4.1.232.154.2.10006	CMC 设备正在报告温度 2 高于警告阈值
1.3.6.1.4.1.232.154.2.10007	CMC 设备正在报告温度 2 高于最大阈值
1.3.6.1.4.1.232.154.2.10008	CMC 设备正在报告温度 2 已恢复到正常温度
1.3.6.1.4.1.232.154.2.10011	CMC 设备正在报告电压低于最小阈值
1.3.6.1.4.1.232.154.2.10012	CMC 设备正在报告电压高于最大阈值
1.3.6.1.4.1.232.154.2.10013	CMC 设备正在报告电压已恢复到正常值
1.3.6.1.4.1.232.154.2.10021	CMC 设备正在报告湿度低于最小阈值
1.3.6.1.4.1.232.154.2.10022	CMC 设备正在报告湿度高于最大阈值
1.3.6.1.4.1.232.154.2.10023	CMC 设备正在报告湿度已恢复到正常值
1.3.6.1.4.1.232.154.2.10031	CMC 设备正在报告检测到烟
1.3.6.1.4.1.232.154.2.10032	CMC 设备正在报告烟已被清除
1.3.6.1.4.1.232.154.2.10041	CMC 设备正在报告检测到震动
1.3.6.1.4.1.232.154.2.10042	CMC 设备正在报告震动已被清除
1.3.6.1.4.1.232.154.2.10051	CMC 设备已进入辅助输入 1 的警报状态
1.3.6.1.4.1.232.154.2.10052	CMC 设备正在报告辅助输入 1 警报已清除
1.3.6.1.4.1.232.154.2.10053	CMC 设备已进入辅助输入 2 的警报状态
1.3.6.1.4.1.232.154.2.10054	CMC 设备正在报告辅助输入 2 警报已清除
1.3.6.1.4.1.232.154.2.10101	CMC 设备正在报告输入 1 已打开
1.3.6.1.4.1.232.154.2.10102	CMC 设备正在报告输入 1 已关闭
1.3.6.1.4.1.232.154.2.10103	CMC 设备正在报告输入 2 已打开
1.3.6.1.4.1.232.154.2.10104	CMC 设备正在报告输入 2 已关闭
1.3.6.1.4.1.232.154.2.10105	CMC 设备正在报告输入 3 已打开
1.3.6.1.4.1.232.154.2.10106	CMC 设备正在报告输入 3 已关闭
1.3.6.1.4.1.232.154.2.10107	CMC 设备正在报告输入 4 已打开
1.3.6.1.4.1.232.154.2.10108	CMC 设备正在报告输入 4 已关闭

MIB ID	SNMP 陷阱描述
1.3.6.1.4.1.232.154.2.10111	CMC 设备正在报告锁集 1 已解锁
1.3.6.1.4.1.232.154.2.10112	CMC 设备正在报告锁集 1 未能锁定
1.3.6.1.4.1.232.154.2.10113	CMC 设备正在报告锁集 1 出错
1.3.6.1.4.1.232.154.2.10114	CMC 设备正在报告锁集 1 已锁定
1.3.6.1.4.1.232.154.2.10116	CMC 设备正在报告锁集 2 已解锁
1.3.6.1.4.1.232.154.2.10117	CMC 设备正在报告锁集 2 未能锁定
1.3.6.1.4.1.232.154.2.10118	CMC 设备正在报告锁集 2 出错
1.3.6.1.4.1.232.154.2.10119	CMC 设备正在报告锁集 2 已锁定
1.3.6.1.4.1.232.154.2.10134	CMC 设备正在报告锁集 1 正常
1.3.6.1.4.1.232.154.2.10135	CMC 设备正在报告锁集 2 正常
1.3.6.1.4.1.232.154.2.20001	cpqRPMTrapUPSInputVoltageBelowMin
1.3.6.1.4.1.232.154.2.20002	cpqRPMTrapUPSInputVoltageAboveMax
1.3.6.1.4.1.232.154.2.20003	cpqRPMTrapUPSInputVoltageNormal
1.3.6.1.4.1.232.154.2.20011	cpqRPMTrapUPSOutputVoltageBelowMin
1.3.6.1.4.1.232.154.2.20012	cpqRPMTrapUPSOutputVoltageAboveMax
1.3.6.1.4.1.232.154.2.20014	UPS 设备正在报告超负荷状态
1.3.6.1.4.1.232.154.2.20015	UPS 设备正在报告超负荷状态已清除
1.3.6.1.4.1.232.154.2.20022	cpqRPMTrapUPSBatteryDepleted
1.3.6.1.4.1.232.154.2.20023	cpqRPMTrapUPSBatteryLevelNormal
1.3.6.1.4.1.232.154.2.20032	cpqRPMTrapUPSOnBypass
1.3.6.1.4.1.232.154.2.20101	cpqRPMTrapUPSTemperatureLow
1.3.6.1.4.1.232.154.2.20102	cpqRPMTrapUPSTemperatureHigh
1.3.6.1.4.1.232.154.2.20103	UPS 设备正在报告温度正常
1.3.6.1.4.1.232.154.2.20111	UPS 设备正在报告常规 UPS 故障
1.3.6.1.4.1.232.154.2.20112	UPS 设备正在报告常规 UPS 故障已清除
1.3.6.1.4.1.232.154.2.20121	UPS 设备正在报告电池故障
1.3.6.1.4.1.232.154.2.20122	UPS 设备正在报告电池故障已清除
1.3.6.1.4.1.232.154.2.20131	UPS 设备正在报告诊断测试失败
1.3.6.1.4.1.232.154.2.20132	UPS 设备正在报告诊断测试成功
1.3.6.1.4.1.232.154.2.20141	UPS 输入 （供电线路）：测量的输入频率超出正常运行的频率规格上限或下限

MIB ID	SNMP 陷阱描述
1.3.6.1.4.1.232.154.2.20142	UPS 测得的输入频率正常
1.3.6.1.4.1.232.154.2.20151	使用电池电源时已启动 UPS 设备
1.3.6.1.4.1.232.154.2.20152	使用供电线路电源时已启动 UPS 设备
1.3.6.1.4.1.232.154.2.20161	UPS 设备正在报告旁路不可用
1.3.6.1.4.1.232.154.2.20162	UPS 设备正在报告旁路不可用错误已清除
1.3.6.1.4.1.232.154.2.20171	cpqRPMTrapUPSUtilityFail
1.3.6.1.4.1.232.154.2.20172	cpqRPMTrapUPSUtilityFailCleared
1.3.6.1.4.1.232.154.2.20181	cpqRPMTrapUPSUtilityNotPresent
1.3.6.1.4.1.232.154.2.20182	cpqRPMTrapUPSUtilityNotPresentCleared
1.3.6.1.4.1.232.154.2.20191	cpqRPMTrapUPSBypassManualTurnedOn
1.3.6.1.4.1.232.154.2.20192	cpqRPMTrapUPSBypassManualTurnedOff
1.3.6.1.4.1.232.154.2.20201	UPS 设备正在报告输入线缆发生故障
1.3.6.1.4.1.232.154.2.20202	UPS 设备正在报告输入线缆正常
1.3.6.1.4.1.232.154.2.21007	UPS 设备正在报告温度超出范围
1.3.6.1.4.1.232.154.2.21008	UPS 设备正在报告温度正常
1.3.6.1.4.1.232.154.2.21011	UPS 设备正在报告关闭挂起状态
1.3.6.1.4.1.232.154.2.21012	UPS 不再处于关闭挂起状态
1.3.6.1.4.1.232.154.2.21013	UPS 设备正在报告即将关闭状态
1.3.6.1.4.1.232.154.2.21014	UPS 设备正在报告即将关闭状态已清除
1.3.6.1.4.1.232.154.2.21019	UPS 设备正在报告输出电压超出范围
1.3.6.1.4.1.232.154.2.21020	UPS 设备正在报告输出电压正常
1.3.6.1.4.1.232.154.2.21021	UPS 设备正在报告输入电压超出范围
1.3.6.1.4.1.232.154.2.21021	UPS 设备正在报告输入电压超出范围
1.3.6.1.4.1.232.154.2.21023	UPS 设备正在报告冗余丢失
1.3.6.1.4.1.232.154.2.21024	UPS 设备正在报告冗余丢失错误已清除
1.3.6.1.4.232.154.2.21029	UPS 设备正在报告开启降压状态
1.3.6.1.4.232.154.2.21031	UPS 设备正在报告开启升压状态
1.3.6.1.4.1.232.154.2.21033	UPS 已通过用户交互关闭电源
1.3.6.1.4.1.232.154.2.21034	UPS 输出已恢复
1.3.6.1.4.1.232.154.2.21035	UPS 设备正在报告风扇发生故障

MIB ID	SNMP 陷阱描述
1.3.6.1.4.1.232.154.2.21036	UPS 设备正在报告风扇故障已清除
1.3.6.1.4.1.232.154.2.21037	UPS 设备正在报告紧急断电 (EPO) 命令
1.3.6.1.4.1.232.154.2.21041	UPS 设备正在报告输出断路器或继电器发生故障
1.3.6.1.4.1.232.154.2.21042	UPS 设备正在报告输出断路器正常运行
1.3.6.1.4.1.232.154.2.21045	UPS 设备正在报告覆盖面板已移除
1.3.6.1.4.1.232.154.2.21046	UPS 设备正在报告覆盖面板已更换
1.3.6.1.4.1.232.154.2.21047	UPS 设备正在以自动旁路模式运行
1.3.6.1.4.1.232.154.2.21048	UPS 设备现在不以自动旁路模式运行
1.3.6.1.4.1.232.154.2.21053	UPS 设备正在报告 UPS 未连接电池
1.3.6.1.4.1.232.154.2.21054	UPS 设备正在报告 UPS 已重新连接电池
1.3.6.1.4.1.232.154.2.21055	UPS 设备正在报告电池电量低
1.3.6.1.4.1.232.154.2.21056	UPS 设备正在报告电池电量低的错误已清除
1.3.6.1.4.1.232.154.2.21057	UPS 设备正在报告电池已完全放电
1.3.6.1.4.1.232.154.2.21058	UPS 设备正在报告电池已完全放电
1.3.6.1.4.1.232.154.2.21059	UPS 设备正在以手动旁路模式运行
1.3.6.1.4.1.232.154.2.21060	UPS 设备正在以正常模式运行
1.3.6.1.4.1.232.154.2.21063	UPS 设备正在报告在使用电池
1.3.6.1.4.1.232.154.2.21064	UPS 设备正在报告在使用供电线路电源
1.3.6.1.4.1.232.154.3.1	已出现严重警报
1.3.6.1.4.1.232.154.3.2	UPS 已出现警告警报
1.3.6.1.4.1.232.154.2.3	CRPM 未能找到设备主机名的 IP 地址
1.3.6.1.4.1.232.154.3.4	UPS 警报已清除
1.3.6.1.4.1.232.154.2.50001	cpqRPMTestTrap
1.3.6.1.4.1.232.154.2.29999	cpqRPMTrapUPSDCStartOccurredCleared
1.3.6.1.4.1.232.154.2.29998	cpqRPMTrapUPSDCStartOccurred

对于以上每个 SNMP 陷阱，此策略均包含一条规则。问题解决之后，将自动确认之前的警报消息。

智能驱动器阵列陷阱监视策略

SI-HPProLiant_FwdDriveArrayTraps

The SI-HPProLiant_FwdDriveArrayTraps 策略拦截与 Compaq 智能驱动器阵列有关的 SNMP 陷阱。每次生成陷阱后该策略便向 HPOM 控制台发送警报。

此策略将监视以下陷阱：

MIB ID	SNMP 陷阱描述
1.3.6.1.4.1.232.0.3001	智能驱动器阵列逻辑驱动器状态为 “正常”，此状态包含在 SNMP Varbind 1 中。
	智能驱动器阵列逻辑驱动器状态为 “故障”，此状态包含在 SNMP Varbind 1 中。
	智能驱动器阵列逻辑驱动器状态为 “正在恢复”，此状态包含在 SNMP Varbind 1 中。
	智能驱动器阵列逻辑驱动器状态为 “准备重建”，此状态包含在 SNMP Varbind 1 中。
	智能驱动器阵列逻辑驱动器状态为 “正在重建”，此状态包含在 SNMP Varbind 1 中。
	智能驱动器阵列逻辑驱动器状态为 “错误的驱动器”，此状态包含在 SNMP Varbind 1 中。
	智能驱动器阵列逻辑驱动器状态为 “无效连接”，此状态包含在 SNMP Varbind 1 中。
	智能驱动器阵列逻辑驱动器状态为 “过热”，此状态包含在 SNMP Varbind 1 中。
	智能驱动器阵列逻辑驱动器状态为 “关闭”，此状态包含在 SNMP Varbind 1 中。
	智能驱动器阵列逻辑驱动器状态为 “不可用”，此状态包含在 SNMP Varbind 1 中。
	智能驱动器阵列逻辑驱动器状态为 “未配置”，此状态包含在 SNMP Varbind 1 中。
	智能驱动器阵列逻辑驱动器状态为 “正在扩展”，此状态包含在 SNMP Varbind 1 中。
	智能驱动器阵列逻辑驱动器状态为 “排队等待扩展”，此状态包含在 SNMP Varbind 1 中。

MIB ID	SNMP 陷阱描述
1.3.6.1.4.1.232.0.3002	智能驱动器阵列备用驱动器状态为 “活动”，此状态包含在 SNMP Varbind 1 中。
	智能驱动器阵列备用驱动器状态为 “无效”，此状态包含在 SNMP Varbind 1 中。
	智能驱动器阵列备用驱动器状态为 “不活动”，此状态包含在 SNMP Varbind 1 中。
	智能驱动器阵列备用驱动器状态为 “故障”，此状态包含在 SNMP Varbind 1 中。
	智能驱动器阵列备用驱动器状态为 “正在构建”，此状态包含在 SNMP Varbind 1 中。
1.3.6.1.4.1.232.0.3003	智能驱动器阵列物理驱动器状态为 “正常”，此状态包含在 SNMP Varbind 1 中。
	智能驱动器阵列物理驱动器状态为 “故障”，此状态包含在 SNMP Varbind 1 中。
	智能驱动器阵列物理驱动器状态为 “预测故障”，此状态包含在 SNMP Varbind 1 中。
1.3.6.1.4.1.232.0.3004	智能驱动器阵列物理驱动器阈值已超出，此状态包含在 SNMP Varbind 1 中。
1.3.6.1.4.1.232.0.3005	智能驱动器阵列加速器板状态为 “无效”，此状态包含在 SNMP Varbind 1 中。
	智能驱动器阵列加速器板状态为 “已启用”，此状态包含在 SNMP Varbind 1 中。
	智能驱动器阵列加速器板状态为 “暂时禁用”，此状态包含在 SNMP Varbind 1 中。
	智能驱动器阵列加速器板状态为 “永久禁用”，此状态包含在 SNMP Varbind 1 中。
	智能驱动器阵列加速器板状态为 “永久禁用”，此状态包含在 SNMP Varbind 1 中。
1.3.6.1.4.1.232.0.3006	智能驱动器阵列加速器失去了电池供电。可能发生数据丢失。
1.3.6.1.4.1.232.0.3007	智能驱动器阵列加速器板电池状态为 “正在充电”。包含在 SNMP Varbind 1 中。
	智能驱动器阵列加速器板电池状态为 “不存在”。包含在 SNMP Varbind 1 中。
	智能驱动器阵列加速器板电池状态为 “正常”。包含在 SNMP Varbind 1 中。
	智能驱动器阵列加速器板电池状态为 “故障”。包含在 SNMP Varbind 1 中。
	智能驱动器阵列加速器板电池状态为 “降级”。包含在 SNMP Varbind 1 中。

MIB ID	SNMP 陷阱描述
1.3.6.1.4.1.232.0.3008	智能驱动器阵列逻辑驱动器状态为 “未配置”，此状态包含在 SNMP Varbind 3 中。
	智能驱动器阵列逻辑驱动器状态为 “正在扩展”，此状态包含在 SNMP Varbind 3 中。
	智能驱动器阵列逻辑驱动器状态为 “排队等待扩展”，此状态包含在 SNMP Varbind 3 中。
	智能驱动器阵列逻辑驱动器状态为 “正常”，此状态包含在 SNMP Varbind 3 中。
	智能驱动器阵列逻辑驱动器状态为 “故障”，此状态包含在 SNMP Varbind 3 中。
	智能驱动器阵列逻辑驱动器状态为 “正在恢复”，此状态包含在 SNMP Varbind 3 中。
	智能驱动器阵列逻辑驱动器状态为 “准备重建”，此状态包含在 SNMP Varbind 3 中。
	智能驱动器阵列逻辑驱动器状态为 “正在重建”，此状态包含在 SNMP Varbind 3 中。
	智能驱动器阵列逻辑驱动器状态为 “错误的驱动器”，此状态包含在 SNMP Varbind 3 中。
	智能驱动器阵列逻辑驱动器状态为 “无效连接”，此状态包含在 SNMP Varbind 3 中。
	智能驱动器阵列逻辑驱动器状态为 “过热”，此状态包含在 SNMP Varbind 3 中。
	智能驱动器阵列逻辑驱动器状态为 “关闭”，此状态包含在 SNMP Varbind 3 中。
	智能驱动器阵列逻辑驱动器状态为 “不可用”，此状态包含在 SNMP Varbind 3 中。
1.3.6.1.4.1.232.0.3009	智能驱动器阵列备用驱动器状态为 “无效”，此状态包含在 SNMP Varbind 3 中。
	智能驱动器阵列备用驱动器状态为 “不活动”，此状态包含在 SNMP Varbind 3 中。
	智能驱动器阵列备用驱动器状态为 “活动”，此状态包含在 SNMP Varbind 3 中。
	智能驱动器阵列备用驱动器状态为 “故障”，此状态包含在 SNMP Varbind 3 中。
	智能驱动器阵列备用驱动器状态为 “正在构建”，此状态包含在 SNMP Varbind 3 中。

MIB ID	SNMP 陷阱描述
1.3.6.1.4.1.232.0.3010	智能驱动器阵列物理驱动器状态为 “正常”，此状态包含在 SNMP Varbind 3 中。
	智能驱动器阵列物理驱动器状态为 “故障”，此状态包含在 SNMP Varbind 3 中（在 Varbind 4 所含的 SCSI 总线上）。
	SCSI 总线上的智能驱动器阵列物理驱动器状态为 “预测故障”，此状态包含在 SNMP Varbind 3 中 （在 Varbind 4 所含的 SCSI 总线号上）。
1.3.6.1.4.1.232.0.3011	智能驱动器阵列物理驱动器阈值已超出，此状态包含在 SNMP Varbind 3 中。
1.3.6.1.4.1.232.0.3012	智能驱动器阵列加速器板状态为 “无效”，此状态包含在 SNMP Varbind 3 中。
	智能驱动器阵列加速器板状态为 “已启用”，此状态包含在 SNMP Varbind 3 中。
	智能驱动器阵列加速器板状态为 “暂时禁用”，此状态包含在 SNMP Varbind 3 中。
	智能驱动器阵列加速器板状态为 “永久禁用”，此状态包含在 SNMP Varbind 3 中。
1.3.6.1.4.1.232.0.3013	智能驱动器阵列加速器失去了电池供电。可能发生数据丢失。
1.3.6.1.4.1.232.0.3014	智能驱动器阵列加速器板电池状态为 “正在充电”。包含在 SNMP Varbind 3 中。
	智能驱动器阵列加速器板电池状态为 “不存在”。包含在 SNMP Varbind 3 中。
	智能驱动器阵列加速器板电池状态为 “正常”。包含在 SNMP Varbind 3 中。
	智能驱动器阵列加速器板电池状态为 “故障”。包含在 SNMP Varbind 3 中。
	智能驱动器阵列加速器板电池状态为 “降级”。包含在 SNMP Varbind 3 中。
1.3.6.1.4.1.232.0.3015	智能驱动器阵列控制器状态为 “正常”，此状态包含在 SNMP Varbind 4 中。
	智能驱动器阵列控制器状态为 “故障”，此状态包含在 SNMP Varbind 4 中。
	智能驱动器阵列控制器存在电缆问题，此状态包含在 SNMP Varbind 4 中。
	智能驱动器阵列控制器已关闭电源，此状态包含在 SNMP Varbind 4 中。
1.3.6.1.4.1.232.0.3016	插槽中的控制器状态现在为活动。

MIB ID	SNMP 陷阱描述
1.3.6.1.4.1.232.0.3017	智能驱动器阵列备用驱动器状态为 “无效”，此状态包含在 SNMP Varbind 3 中。
	智能驱动器阵列备用驱动器状态为 “不活动”，此状态包含在 SNMP Varbind 3 中。
	智能驱动器阵列备用驱动器状态为 “活动”，此状态包含在 SNMP Varbind 3 中。
	智能驱动器阵列备用驱动器状态为 “故障”，此状态包含在 SNMP Varbind 3 中。
	智能驱动器阵列备用驱动器状态为 “正在构建”，此状态包含在 SNMP Varbind 1 中。
1.3.6.1.4.1.232.0.3018	智能驱动器阵列物理驱动器状态为 “正常”，此状态包含在 SNMP Varbind 3 中。
	智能驱动器阵列物理驱动器状态为 “故障”，此状态包含在 SNMP Varbind 3 中。
	智能驱动器阵列物理驱动器状态为 “预测故障”，此状态包含在 SNMP Varbind 3 中。
1.3.6.1.4.1.232.0.3019	智能驱动器阵列物理驱动器阈值已超出。
1.3.6.1.4.1.232.0.3020	智能驱动器阵列磁带库状态为 “正常”，磁带库的状态包含在 SNMP Varbind 7 中。
	智能驱动器阵列磁带库状态为 “故障”，磁带库的状态包含在 SNMP Varbind 7 中。
	智能驱动器阵列磁带库状态为 “降级”，磁带库的状态包含在 SNMP Varbind 7 中。
	智能驱动器阵列磁带库状态为 “脱机”，磁带库的状态包含在 SNMP Varbind 7 中。
1.3.6.1.4.1.232.0.3021	智能驱动器阵列磁带库门状态为 “打开”，状态包含在 SNMP Varbind 7 中。
	智能驱动器阵列磁带库门状态为 “关闭”，状态包含在 SNMP Varbind 7 中。
	智能驱动器阵列磁带库门状态为 “不受支持”，状态包含在 SNMP Varbind 7 中。

MIB ID	SNMP 陷阱描述
1.3.6.1.4.1.232.0.3022	智能驱动器阵列磁带驱动器状态为 “正常”，状态包含在 SNMP Varbind 7 中。
	智能驱动器阵列磁带驱动器状态为 “降级”，状态包含在 SNMP Varbind 7 中。
	智能驱动器阵列磁带驱动器状态为 “故障”，状态包含在 SNMP Varbind 7 中。
	智能驱动器阵列磁带驱动器状态为 “脱机”，状态包含在 SNMP Varbind 7 中。
	智能驱动器阵列磁带驱动器状态为 “缺失 / 曾为正常”，状态包含在 SNMP Varbind 7 中。
	智能驱动器阵列磁带驱动器状态为 “缺失 / 曾为脱机”，状态包含在 SNMP Varbind 7 中。
1.3.6.1.4.1.232.0.3023	智能驱动器阵列磁带驱动器需要清洁。
1.3.6.1.4.1.232.0.3024	清洁磁带需要更换。
1.3.6.1.4.1.232.0.3025	智能驱动器阵列加速器板状态为 “无效”，此状态包含在 SNMP Varbind 7 中。
	智能驱动器阵列加速器板状态为 “已启用”，此状态包含在 SNMP Varbind 7 中。
	智能驱动器阵列加速器板状态为 “暂时禁用”，此状态包含在 SNMP Varbind 7 中。
	智能驱动器阵列加速器板状态为 “暂时禁用”，此状态包含在 SNMP Varbind 7 中。
1.3.6.1.4.1.232.0.3026	智能驱动器阵列加速器失去了电池供电。可能发生数据丢失。
1.3.6.1.4.1.232.0.3027	智能驱动器阵列加速器电池发生故障。
1.3.6.1.4.1.232.0.3028	智能驱动器阵列控制器板状态为 “正常”，此状态包含在 SNMP Varbind 4 中。
	智能驱动器阵列控制器板发生故障，此状态包含在 SNMP Varbind 4 中。
	智能驱动器阵列控制器板 “存在电缆问题”，此状态包含在 SNMP Varbind 4 中。
	智能驱动器阵列控制器板 “已关闭电源”，此状态包含在 SNMP Varbind 4 中。
1.3.6.1.4.1.232.0.3029	智能驱动器阵列物理驱动器状态为 “正常”，此状态包含在 SNMP Varbind 3 中。
	智能驱动器阵列物理驱动器状态为 “故障”，此状态包含在 SNMP Varbind 3 中。
	智能驱动器阵列物理驱动器状态为 “预测故障”，此状态包含在 SNMP Varbind 3 中。

MIB ID	SNMP 陷阱描述
1.3.6.1.4.1.232.0.3030	智能驱动器阵列物理驱动器阈值已超出。
1.3.6.1.4.1.232.0.3031	智能驱动器阵列磁带库状态为 “故障”，磁带库的状态包含在 SNMP Varbind 10 中。
	智能驱动器阵列磁带库状态为 “正常”，磁带库的状态包含在 SNMP Varbind 10 中。
	智能驱动器阵列磁带库状态为 “降级”，磁带库的状态包含在 SNMP Varbind 10 中。
	智能驱动器阵列磁带库状态为 “脱机”，磁带库的状态包含在 SNMP Varbind 10 中。
1.3.6.1.4.1.232.0.3032	智能驱动器阵列磁带驱动器状态为 “正常”，此状态包含在 SNMP Varbind 7 中。
	智能驱动器阵列磁带驱动器状态为 “脱机”，此状态包含在 SNMP Varbind 7 中。
	智能驱动器阵列磁带驱动器状态为 “降级”，此状态包含在 SNMP Varbind 7 中。
	智能驱动器阵列磁带驱动器状态为 “故障”，此状态包含在 SNMP Varbind 10 中。
	智能驱动器阵列磁带驱动器状态为 “缺失 / 曾为正常”，此状态包含在 SNMP Varbind 10 中。
	智能驱动器阵列磁带驱动器状态为 “缺失 / 曾为脱机”，此状态包含在 SNMP Varbind 10 中。
1.3.6.1.4.1.232.0.3033	智能驱动器阵列控制器状态为 “一般故障”，此状态包含在 SNMP Varbind 5 中。
	智能驱动器阵列控制器 “存在电缆问题”，此状态包含在 SNMP Varbind 5 中。
	智能驱动器阵列控制器 “已关闭电源”，此状态包含在 SNMP Varbind 5 中。
	智能驱动器阵列控制器 “正常”，此状态包含在 SNMP Varbind 5 中。

MIB ID	SNMP 陷阱描述
1.3.6.1.4.1.232.0.3034	智能驱动器阵列逻辑驱动器状态为 “未配置”，此状态包含在 SNMP Varbind 6 中。
	智能驱动器阵列逻辑驱动器状态为 “排队等待扩展”，此状态包含在 SNMP Varbind 6 中。
	智能驱动器阵列逻辑驱动器状态为 “正常”，此状态包含在 SNMP Varbind 6 中。
	智能驱动器阵列逻辑驱动器状态为 “故障”，此状态包含在 SNMP Varbind 6 中。
	智能驱动器阵列逻辑驱动器状态为 “正在恢复”，此状态包含在 SNMP Varbind 6 中。
	智能驱动器阵列逻辑驱动器状态为 “准备重建”，此状态包含在 SNMP Varbind 6 中。
	智能驱动器阵列逻辑驱动器状态为 “正在重建”，此状态包含在 SNMP Varbind 6 中。
	智能驱动器阵列逻辑驱动器状态为 “错误的驱动器”，此状态包含在 SNMP Varbind 6 中。
	智能驱动器阵列逻辑驱动器状态为 “无效连接”，此状态包含在 SNMP Varbind 6 中。
	智能驱动器阵列逻辑驱动器状态为 “过热”，此状态包含在 SNMP Varbind 6 中。
	智能驱动器阵列逻辑驱动器状态为 “关闭”，此状态包含在 SNMP Varbind 6 中。
	智能驱动器阵列逻辑驱动器状态为 “正在扩展”，此状态包含在 SNMP Varbind 6 中。
	智能驱动器阵列逻辑驱动器状态为 “不可用”，此状态包含在 SNMP Varbind 6 中。
1.3.6.1.4.1.232.0.3035	智能驱动器阵列备用驱动器状态为 “无效”，此状态包含在 SNMP Varbind 6 中。
	智能驱动器阵列备用驱动器状态为 “不活动”，此状态包含在 SNMP Varbind 6 中。
	智能驱动器阵列备用驱动器状态为 “活动”，此状态包含在 SNMP Varbind 6 中。
	智能驱动器阵列备用驱动器状态为 “故障”，此状态包含在 SNMP Varbind 6 中。
	智能驱动器阵列备用驱动器状态为 “正在构建”，此状态包含在 SNMP Varbind 6 中。

MIB ID	SNMP 陷阱描述
1.3.6.1.4.1.232.0.3036	智能驱动器阵列物理驱动器状态为 “正常”，此状态包含在 SNMP Varbind 12 中。
	智能驱动器阵列物理驱动器状态为 “故障”，此状态包含在 SNMP Varbind 12 中。
	智能驱动器阵列物理驱动器状态为 “预测故障”，此状态包含在 SNMP Varbind 12 中。
1.3.6.1.4.1.232.0.3037	智能驱动器阵列物理驱动器阈值已超出，物理驱动器索引包含在 SNMP Varbind 5 中。
1.3.6.1.4.1.232.0.3038	智能驱动器阵列加速器板状态为 “无效”，此状态包含在 SNMP Varbind 8 中。
	智能驱动器阵列加速器板状态为 “已启用”，此状态包含在 SNMP Varbind 8 中。
	智能驱动器阵列加速器板状态为 “暂时禁用”，此状态包含在 SNMP Varbind 8 中。
	智能驱动器阵列加速器板状态为 “永久禁用”，此状态包含在 SNMP Varbind 8 中。
1.3.6.1.4.1.232.0.3039	智能驱动器阵列加速器失去了电池供电。可能发生数据丢失。
1.3.6.1.4.1.232.0.3040	智能驱动器阵列加速器电池发生故障。
1.3.6.1.4.1.232.0.3041	智能驱动器阵列磁带库状态为 “正常”，磁带库的状态包含在 SNMP Varbind 11 中。
	智能驱动器阵列磁带库状态为 “降级”，磁带库的状态包含在 SNMP Varbind 11 中。
	智能驱动器阵列磁带库状态为 “故障”，磁带库的状态包含在 SNMP Varbind 11 中。
	智能驱动器阵列磁带库状态为 “脱机”，磁带库的状态包含在 SNMP Varbind 11 中。
1.3.6.1.4.1.232.0.3042	智能驱动器阵列磁带库门状态为 “打开”，此状态包含在 SNMP Varbind 11 中。
	智能驱动器阵列磁带库门状态为 “关闭”，此状态包含在 SNMP Varbind 11 中。
	智能驱动器阵列磁带库门状态为 “不受支持”，此状态包含在 SNMP Varbind 11 中。

MIB ID	SNMP 陷阱描述
1.3.6.1.4.1.232.0.3043	智能驱动器阵列磁带驱动器状态为 “降级”，此状态包含在 SNMP Varbind 11 中。
	智能驱动器阵列磁带驱动器状态为 “正常”，此状态包含在 SNMP Varbind 11 中。
	智能驱动器阵列磁带驱动器状态为 “故障”，此状态包含在 SNMP Varbind 11 中。
	智能驱动器阵列磁带驱动器状态为 “脱机”，此状态包含在 SNMP Varbind 11 中。
	智能驱动器阵列磁带驱动器状态为 “缺失 / 曾为正常”，此状态包含在 SNMP Varbind 11 中。
	智能驱动器阵列磁带驱动器状态为 “缺失 / 曾为脱机”，此状态包含在 SNMP Varbind 11 中。
1.3.6.1.4.1.232.0.3044	智能驱动器阵列磁带驱动器需要清理。
1.3.6.1.4.1.232.0.3045	清洁磁带需要更换。
1.3.6.1.4.1.232.0.3046	物理驱动器状态为 “正常”，此状态包含在 SNMP Varbind 12 中。
	物理驱动器状态为 “故障”，此状态包含在 SNMP Varbind 12 中。
	物理驱动器状态为 “预测故障”，此状态包含在 SNMP Varbind 12 中。
1.3.6.1.4.1.232.0.3047	备件状态已更改。

对于以上每个 SNMP 陷阱，此策略均包含一条规则。问题解决之后，将自动确认之前的警报消息。

机架信息陷阱监视策略

SI-HPProLiant_CPQRackTraps

SI-HPProLiant_CPQRackTraps 策略拦截与温度、电源和状态方面的机架信息有关的 SNMP 陷阱。每次生成陷阱后该策略便向 HPOM 控制台发送警报。

它将监视以下陷阱：

MIB ID	SNMP 陷阱描述
1.3.6.1.4.1.232.0.22002	机架 SNMP Varbind 3 中的机柜名称已更改为 SNMP Varbind 5。
1.3.6.1.4.1.232.0.22003	已从机架 SNMP Varbind 3 移除机柜 SNMP Varbind 5。
1.3.6.1.4.1.232.0.22004	机柜 SNMP Varbind 5 已插入机架 SNMP Varbind 3 中。
1.3.6.1.4.1.232.0.22005	机架 SNMP Varbind 3 中的机柜 SNMP Varbind 5 温度传感器已设置为 “故障”。
1.3.6.1.4.1.232.0.22006	机架 SNMP Varbind 3 中的机柜 SNMP Varbind 5 温度传感器已设置为 “降级”。

MIB ID	SNMP 陷阱描述
1.3.6.1.4.1.232.0.22007	机架 SNMP Varbind 3 中的机柜 SNMP Varbind 5 温度传感器已设置为 “正常”。
1.3.6.1.4.1.232.0.22008	机架 SNMP Varbind 3 中的机柜 SNMP Varbind 5 风扇已设置为 “故障”。
1.3.6.1.4.1.232.0.22009	机架 SNMP Varbind 3 中的机柜 SNMP Varbind 5 风扇已设置为 “降级”。
1.3.6.1.4.1.232.0.22010	机架 SNMP Varbind 3 中的机柜 SNMP Varbind 5 风扇已设置为 “正常”。
1.3.6.1.4.1.232.0.22011	机架 SNMP Varbind 3 中的机柜 SNMP Varbind 5 风扇已移除。
1.3.6.1.4.1.232.0.22012	机架 SNMP Varbind 3 中的机柜 SNMP Varbind 5 风扇已插入。
1.3.6.1.4.1.232.0.22013	机架 SNMP Varbind 3 机柜 SNMP Varbind 5 的 SNMP Varbind 7 中的电源已设置为 “失败”。
1.3.6.1.4.1.232.0.22014	机架 SNMP Varbind 3 机柜 SNMP Varbind 5 的 SNMP Varbind 7 中的电源已设置为 “降级”。
1.3.6.1.4.1.232.0.22015	机架 SNMP Varbind 3 机柜 SNMP Varbind 5 的 SNMP Varbind 7 中的电源已设置为 “正常”。
1.3.6.1.4.1.232.0.22016	机架 SNMP Varbind 3 机柜 SNMP Varbind 5 的 SNMP Varbind 7 中的电源已移除。
1.3.6.1.4.1.232.0.22017	机架 SNMP Varbind 3 机柜 SNMP Varbind 5 的 SNMP Varbind 7 中的电源已插入。
1.3.6.1.4.1.232.0.22018	机架 SNMP Varbind 3 机柜 SNMP Varbind 5 中的电源子系统不再冗余。
1.3.6.1.4.1.232.0.22019	机架电源检测到机架 SNMP Varbind 3 机柜 SNMP Varbind 5 的 SNMP Varbind 6 中的电源输入线路电压存在问题。
1.3.6.1.4.1.232.0.22020	机架 SNMP Varbind 3 机柜 SNMP Varbind 5 中的电源子系统处于超负荷状态。
1.3.6.1.4.1.232.0.22021	由于机架 SNMP Varbind 3 上机柜 SNMP Varbind 5 中的刀片 SNMP Varbind 6 缺少电源，服务器关闭。
1.3.6.1.4.1.232.0.22022	为了保留机架 SNMP Varbind 3 机柜上 SNMP Varbind 5 中的刀片 SNMP Varbind 6 内的冗余，阻止了服务器的开启。
1.3.6.1.4.1.232.0.22023	没有足够的功率开启位于机架 SNMP Varbind 3 上的机柜 SNMP Varbind 5 中的刀片 SNMP Varbind 6。
1.3.6.1.4.1.232.0.22024	没有足够的功率开启位于机架 SNMP Varbind 3 上的机柜 SNMP Varbind 5 中的刀片 SNMP Varbind 6。
1.3.6.1.4.1.232.0.22025	没有足够的功率开启位于机架 SNMP Varbind 3 上的机柜 SNMP Varbind 5 中的刀片 SNMP Varbind 6。
1.3.6.1.4.1.232.0.22026	通过手动覆盖开启位于机架 SNMP Varbind 3 上的机柜 SNMP Varbind 5 中的刀片 SNMP Varbind 6。
1.3.6.1.4.1.232.0.22027	位于机架 SNMP Varbind 3 机柜 SNMP Varbind 5 中的保险丝 SNMP Varbind 6 发生熔断。

MIB ID	SNMP 陷阱描述
1.3.6.1.4.1.232.0.22028	已从机架 SNMP Varbind 3 机柜 SNMP Varbind 5 的位置 SNMP Varbind 7 除去 SNMP Varbind 6 中的服务器刀片。
1.3.6.1.4.1.232.0.22029	已在机架 SNMP Varbind 3 机柜 SNMP Varbind 5 的位置 SNMP Varbind 7 插入 SNMP Varbind 6 中的服务器刀片。
1.3.6.1.4.1.232.0.22030	机架 SNMP Varbind 3 上的机柜 SNMP Varbind 5 中的电源子系统负载不均衡。
1.3.6.1.4.1.232.0.22031	机架 SNMP Varbind 3 上的机柜 SNMP Varbind 5 中的电源子系统发生直流电问题。
1.3.6.1.4.1.232.0.22033	机架 SNMP Varbind 3 中耗电未知。
1.3.6.1.4.1.232.0.22032	机架 SNMP Varbind 3 上的机柜 SNMP Varbind 5 中的电源子系统超出了交流电输入功率。
1.3.6.1.4.1.232.0.22034	机架 SNMP Varbind 3 上的机柜 SNMP Varbind 5 中的电源子系统缺少负载均衡线缆。
1.3.6.1.4.1.232.0.22035	机架 SNMP Varbind 3 中的电源子系统包含过多电源柜 SNMP Varbind 5。
1.3.6.1.4.1.232.0.22036	机架 SNMP Varbind 3 上的机柜 SNMP Varbind 5 中的电源子系统未正确配置。
1.3.6.1.4.1.232.0.22037	机载管理器状态已设置为 “降级”。
1.3.6.1.4.1.232.0.22038	机载管理器状态已设置为 “正常”。
1.3.6.1.4.1.232.0.22039	机载管理器已卸除。
1.3.6.1.4.1.232.0.22042	服务器刀片 e-keying 已失败，并且在服务器 mezz 卡和位于机架 SNMP Varbind 3 机柜 SNMP Varbind 5 中的位置 SNMP Varbin 7 的刀片 SNMP Varbind 6 中的互联之间存在端口映射问题。
1.3.6.1.4.1.232.0.22040	机载管理器已插入。
1.3.6.1.4.1.232.0.22041	机架 SNMP Varbind 3 上的机柜 SNMP Varbind 5 中的机载管理器已取得主要角色。
1.3.6.1.4.1.232.0.22043	位于机架 SNMP Varbind 3 机柜 SNMP Varbind 5 的位置 SNMP Varbind 7 的刀片 SNMP Varbind 6 中的服务器刀片 e-keying 已恢复正常运行。
1.3.6.1.4.1.232.0.22044	已从机柜（位于机架 SNMP Varbind 3 机柜 SNMP Varbind 5 的位置 SNMP Varbind 7 的互联 SNMP Varbind 6 中）移除互联。
1.3.6.1.4.1.232.0.22045	互联已插入到机柜 （位于机架 SNMP Varbind 3 机柜 SNMP Varbind 5 中的位置 SNMP Varbind 7 的互联 SNMP Varbind 6 中）。
1.3.6.1.4.1.232.0.22046	位于机架 SNMP Varbind 3 机柜 SNMP Varbind 5 的位置 SNMP Varbind 7 的互联 SNMP Varbind 6 上的互联状态已设置为 “故障”。
1.3.6.1.4.1.232.0.22047	位于机架 SNMP Varbind 3 机柜 SNMP Varbind 5 的位置 SNMP Varbind 7 的互联 SNMP Varbind 6 上的互联状态已降级。

MIB ID	SNMP 陷阱描述
1.3.6.1.4.1.232.0.22048	位于机架 SNMP Varbind 3 机柜 SNMP Varbind 5 的位置 SNMP Varbind 7 的互联 SNMP Varbind 6 上的互联状态已设置为 “正常”。
1.3.6.1.4.1.232.0.22049	服务器刀片已请求降低功率
1.3.6.1.4.1.232.0.22050	服务器刀片已从机柜中卸除
1.3.6.1.4.1.232.0.22051	服务器刀片已插入到机柜
1.3.6.1.4.1.232.0.22052	cpqRackServerBladeStatusRepaired
1.3.6.1.4.1.232.0.22053	cpqRackServerBladeStatusDegraded
1.3.6.1.4.1.232.0.22054	cpqRackServerBladeStatusCritical
1.3.6.1.4.1.232.0.22055	cpqRackServerBladeGrpCapTimeout
1.3.6.1.4.1.232.0.22056	cpqRackServerBladeUnexpectedShutdown
1.3.6.1.4.1.232.0.22057	cpqRackServerBladeMangementControllerFirmwareUpdating
1.3.6.1.4.1.232.0.22058	cpqRackServerBladeMangementControllerFirmwareUpdateComplete
1.3.6.1.4.1.232.0.22059	cpqRackServerBladeSystemBIOSFirmwareUpdating
1.3.6.1.4.1.232.0.22060	cpqRackServerBladeSystemBIOSFirmwareUpdateCompleted
1.3.6.1.4.1.232.0.22061	cpqRackServerBladeFrontIOBlankingActive
1.3.6.1.4.1.232.0.22062	cpqRackServerBladeRemoteFrontIOBlankingInactive
1.3.6.1.4.1.232.0.22063	cpqRackServerBladeDiagnosticAdaptorInserted
1.3.6.1.4.1.232.0.22064	cpqRackServerBladeDiagnosticAdaptorRemoved
	cpqRackServerBladeDiagnosticAdaptorRemoved
1.3.6.1.4.1.232.0.22065	cpqRackServerBladeEnteredPXEBootMode
1.3.6.1.4.1.232.0.22066	cpqRackServerBladeExitedPXEBootMode
1.3.6.1.4.1.232.0.22067	cpqRackServerBladeWarmReset
1.3.6.1.4.1.232.0.22068	cpqRackServerBladePOSTCompleted
1.3.6.1.4.1.232.0.22069	cpqRackServerBladePoweredOn
1.3.6.1.4.1.232.0.22070	cpqRackServerBladePoweredOff
1.3.6.1.4.1.232.0.22071	cpqRackInformationalEAETrap
1.3.6.1.4.1.232.0.22072	cpqRackMinorEAETrap
1.3.6.1.4.1.232.0.22073	cpqRackMajorEAETrap
1.3.6.1.4.1.232.0.22074	cpqRackCriticalEAETrap
1.3.6.1.4.1.232.0.22075	cpqRackPowerMinorEAETrap
1.3.6.1.4.1.232.0.22076	cpqRackPowerMajorEAETrap
1.3.6.1.4.1.232.0.22077	cpqRackPowerCriticalEAETrap

对于以上每个 SNMP 陷阱，此策略均包含一条规则。问题解决之后，将自动确认之前的警报消息。

UPS 陷阱监视策略

SI-HPProLiant_CPQUPSTraps

SI-HPProLiant_CPQRackTraps 策略拦截与机架信息有关的关于温度、电源和状态的 SNMP 陷阱。每次生成陷阱后该策略便向 HPOM 控制台发送警报。

它将监视以下陷阱：

MIB ID	SNMP 陷阱描述
1.3.6.1.4.1.232.0.12001	UPS 报告交流电源故障。
1.3.6.1.4.1.232.0.12002	UPS 报告交流电源已恢复。
1.3.6.1.4.1.232.0.12003	UPS 已经启动服务器关闭。
1.3.6.1.4.1.232.0.12004	UPS 关闭之后，服务器能够正常运行。
1.3.6.1.4.1.232.0.12005	UPS 电池电量低，服务器即将断电。
1.3.6.1.4.1.232.0.12006	UPS 报告交流电源故障。
1.3.6.1.4.1.232.0.12007	UPS 报告交流电源已恢复。
1.3.6.1.4.1.232.0.12008	UPS 已经启动服务器关闭。
1.3.6.1.4.1.232.0.12009	UPS 关闭之后，服务器能够正常运行。
1.3.6.1.4.1.232.0.12010	UPS 电池电量低，服务器即将断电。
1.3.6.1.4.1.232.0.12011	UPS 已超载。
1.3.6.1.4.1.232.0.12012	UPS 电池将发生故障。
1.3.6.1.4.1.232.0.12013	cpqUpsGenericCritical
1.3.6.1.4.1.232.0.12014	cpqUpsGenericInfo

对于以上每个 SNMP 陷阱，此策略均包含一条规则。问题解决之后，将自动确认之前的警报消息。

刀片类型 2 陷阱监视策略

SI-HPProLiant_BladeType2Traps

SI-HPProLiant_BladeType2Traps 策略将拦截与刀片类型 2 相关的 SNMP 陷阱。该策略在每次生成陷阱后便向 HPOM 控制台发送警报。

它将监视以下陷阱：

MIB ID	SNMP 陷阱描述
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.1	bt2SwPrimaryPowerSupplyFailure
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.35	bt2SwUfdfoLtMUP
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.32	bt2SwFanFailure

MIB ID	SNMP 陷阱描述
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.48	bt2SwHotlinksBackupUp
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.46	bt2SwHotlinksMasterUp
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.17	bt2SwVrrpNewBackup
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.36	bt2SwUfdfoGlobalEna
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.28	bt2SwSaveComplete
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.37	bt2SwUfdfoGlobalDis
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.2	bt2SwDefGwUp
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.47	bt2SwHotlinksMasterDn
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.38	bt2SwUfdfoLtDAutoEna
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.5	bt2SwDefGwNotInService
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.41	bt2SwCubeRemoved
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.49	bt2SwHotlinksBackupDn
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.27	bt2SwApplyComplete
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.45	bt2SwCistTopologyChanged
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.16	bt2SwVrrpNewMaster
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.40	bt2SwCubeInserted
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.29	bt2SwFwDownloadSucess
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.18	bt2SwVrrpAuthFailure
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.34	bt2SwUfdfoLtMFailure
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.44	bt2SwStgTopologyChanged
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.3	bt2SwDefGwDown
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.4	bt2SwDefGwInService
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.42	bt2SwStgNewRoot
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.50	bt2SwHotlinksNone
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.22	bt2SwTempExceedThreshold
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.31	bt2SwTempReturnThreshold
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.39	bt2SwUfdfoLtDAutoDis
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.30	bt2SwFwDownloadFailure
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.33	bt2SwFanFailureFixed
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.43	bt2SwCistNewRoot
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.26	bt2SwRackLocationChange
1.3.6.1.4.1.11.2.3.7.11.33.1.2.7.19	bt2SwLoginFailure

对于以上每个 SNMP 陷阱，此策略均包含一条规则。问题解决之后，将自动确认之前的警报消息。

存储系统陷阱监视策略

SI-HPProLiant_CPQSSTraps

SI-HPProLiant_CPQSSTraps 策略拦截与存储系统相关的关于风扇状态、温度和电源的 SNMP 陷阱。每次生成陷阱后该策略便向 HPOM 控制台发送警报。

它将监视以下陷阱：

MIB ID	SNMP 陷阱描述
1.3.6.1.4.1.232.0.8001	存储系统风扇状态已更改为 “正常”，此状态包含在 SNMP Varbind 1 中。
	存储系统风扇状态已更改为 “故障”，此状态包含在 SNMP Varbind 1 中。
	存储系统风扇状态已更改为 “降级”，此状态包含在 SNMP Varbind 1 中。
	此单元不支持风扇监视，此状态包含在 SNMP Varbind 1 中。
1.3.6.1.4.1.232.0.8002	存储系统将由于温度故障而关闭。
1.3.6.1.4.1.232.0.8003	存储系统温度状态为 “降级”。
1.3.6.1.4.1.232.0.8004	存储系统温度 “正常”。
1.3.6.1.4.1.232.0.8005	存储系统侧面板已重新装到单元上。
1.3.6.1.4.1.232.0.8006	存储系统侧面板已从单元移除。
1.3.6.1.4.1.232.0.8007	存储系统电源单元已变为 “降级”。
1.3.6.1.4.1.232.0.8008	存储系统风扇状态已更改为 “正常”，此状态包含在 SNMP Varbind 3 中。
	存储系统风扇状态已更改为 “故障”，此状态包含在 SNMP Varbind 3 中。
	存储系统风扇状态已更改为 “降级”，此状态包含在 SNMP Varbind 3 中。
	存储系统风扇状态已更改为 “无风扇”，此状态包含在 SNMP Varbind 3 中。
1.3.6.1.4.1.232.0.8009	存储系统温度故障。
1.3.6.1.4.1.232.0.8010	存储系统温度状态为 “降级”。
1.3.6.1.4.1.232.0.8011	存储系统温度 “正常”。
1.3.6.1.4.1.232.0.8012	存储系统侧面板已重新装到单元上。
1.3.6.1.4.1.232.0.8013	存储系统侧面板已从单元移除。
1.3.6.1.4.1.232.0.8014	存储系统电源单元已变为 “降级”。
1.3.6.1.4.1.232.0.8015	存储系统电源单元已变为 “降级”。

MIB ID	SNMP 陷阱描述
1.3.6.1.4.1.232.0.8016	存储系统风扇状态已更改为 “未安装”，此状态包含在 SNMP Varbind 6 中。
	存储系统风扇状态已更改为 “正常”，此状态包含在 SNMP Varbind 6 中。
	存储系统风扇状态已更改为 “降级”，此状态包含在 SNMP Varbind 6 中。
	存储系统风扇状态已更改为 “故障”，此状态包含在 SNMP Varbind 6 中。
1.3.6.1.4.1.232.0.8017	存储系统电源状态已更改为 “未安装”，此状态包含在 SNMP Varbind 6 中。
	存储系统电源状态已更改为 “正常”，此状态包含在 SNMP Varbind 6 中。
	存储系统电源状态已更改为 “故障”，此状态包含在 SNMP Varbind 6 中。
	存储系统电源状态已更改为 “降级”，此状态包含在 SNMP Varbind 6 中。
1.3.6.1.4.1.232.0.8018	存储系统电源 UPS 状态已更改为 “正常”，此状态包含在 SNMP Varbind 6 中。
	存储系统电源 UPS 状态已更改为 “无 UPS”，此状态包含在 SNMP Varbind 6 中。
	存储系统电源 UPS 状态已更改为 “电源故障”，此状态包含在 SNMP Varbind 6 中。
	存储系统电源 UPS 状态已更改为 “电池电量低”，此状态包含在 SNMP Varbind 6 中。
1.3.6.1.4.1.232.0.8019	存储系统温度传感器状态已更改为 “正常”，此状态包含在 SNMP Varbind 6 中。
	存储系统温度传感器状态已更改为 “降级”，此状态包含在 SNMP Varbind 6 中。
	存储系统温度传感器状态已更改为 “故障”，此状态包含在 SNMP Varbind 6 中。
1.3.6.1.4.1.232.0.8020	存储系统风扇状态已更改为 “正常”，此状态包含在 SNMP Varbind 6 中。
	存储系统风扇状态已更改为 “未安装”，此状态包含在 SNMP Varbind 6 中。
	存储系统风扇状态已更改为 “降级”，此状态包含在 SNMP Varbind 6 中。
	存储系统风扇状态已更改为 “故障”，此状态包含在 SNMP Varbind 6 中。

MIB ID	SNMP 陷阱描述
1.3.6.1.4.1.232.0.8021	存储系统电源状态已更改为 “正常”，此状态包含在 SNMP Varbind 6 中。
	存储系统电源状态已更改为 “故障”，此状态包含在 SNMP Varbind 6 中。
	存储系统电源状态已更改为 “未安装”，此状态包含在 SNMP Varbind 6 中。
	存储系统电源状态已更改为 “降级”，此状态包含在 SNMP Varbind 6 中。
1.3.6.1.4.1.232.0.8022	存储系统风扇状态已更改为 “正常”，此状态包含在 SNMP Varbind 9 中。
	存储系统风扇状态已更改为 “降级”，此状态包含在 SNMP Varbind 9 中。
	存储系统风扇状态已更改为 “故障”，此状态包含在 SNMP Varbind 9 中。
	存储系统风扇状态已更改为 “不受支持”，此状态包含在 SNMP Varbind 9 中。
	存储系统风扇状态已更改为 “降级 - 风扇 1 故障”，此状态包含在 SNMP Varbin 9 中。
	存储系统风扇状态已更改为 “降级 - 风扇 2 故障”，此状态包含在 SNMP Varbin 9 中。
1.3.6.1.4.1.232.0.8023	存储系统温度状态已更改为 “正常”，此状态包含在 SNMP Varbind 9 中。
	存储系统温度状态已更改为 “降级”，此状态包含在 SNMP Varbind 9 中。
	存储系统温度状态已更改为 “故障”，此状态包含在 SNMP Varbind 9 中。
	存储系统温度状态已更改为 “无温度”，此状态包含在 SNMP Varbind 9 中。
	存储系统温度状态已更改为 “不受支持”，此状态包含在 SNMP Varbind 9 中。

MIB ID	SNMP 陷阱描述
1.3.6.1.4.1.232.0.8024	存储系统电源状态已更改为 “正常”，此状态包含在 SNMP Varbind 9 中。
	存储系统电源状态已更改为 “降级”，此状态包含在 SNMP Varbind 9 中。
	存储系统电源状态已更改为 “故障”，此状态包含在 SNMP Varbind 9 中。
	存储系统电源状态已更改为 “noFltTolPower”，此状态包含在 SNMP Varbind 9 中。
	存储系统电源状态已更改为 “不受支持”，此状态包含在 SNMP Varbind 9 中。
	存储系统电源状态已更改为 “noFltTolPower-Bay1Missing”，此状态包含在 SNMP Varbind 9 中。
	存储系统电源状态已更改为 “noFltTolPower-Bay2Missing”，此状态包含在 SNMP Varbind 9 中。
	存储系统电源状态已更改为 “正常”，此状态包含在 SNMP Varbind 9 中。
1.3.6.1.4.1.232.8.0.1	存储系统风扇状态已更改为 “正常”，此状态包含在 SNMP Varbind 1 中。
	存储系统风扇状态已更改为 “故障”，此状态包含在 SNMP Varbind 1 中。
	存储系统风扇状态已更改为 “降级”，此状态包含在 SNMP Varbind 1 中。

MIB ID	SNMP 陷阱描述
1.3.6.1.4.1.232.0.8025	存储系统的恢复服务器选项状态已更改为 “守护程序关闭 - 已禁用”，此状态包含在 SNMP Varbind 5 中。
	存储系统的恢复服务器选项状态已更改为 “正常”，此状态包含在 SNMP Varbind 5 中。
	存储系统的恢复服务器选项状态已更改为 “守护程序关闭 - 活动”，此状态包含在 SNMP Varbind 5 中。
	存储系统的恢复服务器选项状态已更改为 “无辅助服务器”，此状态包含在 SNMP Varbind 5 中。
	存储系统的恢复服务器选项状态已更改为 “守护程序关闭 - 无辅助服务器”，此状态包含在 SNMP Varbind 5 中。
	存储系统的恢复服务器选项状态已更改为 “链接关闭”，此状态包含在 SNMP Varbind 5 中。
	存储系统的恢复服务器选项状态已更改为“守护程序关闭 - 链接关闭”，此状态包含在 SNMP Varbind 5 中。
	存储系统的恢复服务器选项状态已更改为 “辅助服务器正在运行 - 自动”，此状态包含在 SNMP Varbind 5 中。
	存储系统的恢复服务器选项状态已更改为 “辅助服务器正在运行 - 用户”，此状态包含在 SNMP Varbind 5 中。
	存储系统的恢复服务器选项状态已更改为 “未配置”，此状态包含在 SNMP Varbind 5 中。
	存储系统的恢复服务器选项状态已更改为 “不受支持”，此状态包含在 SNMP Varbind 5 中。
	存储系统的恢复服务器选项状态已更改为 “已禁用”，此状态包含在 SNMP Varbind 5 中。
	存储系统的恢复服务器选项状态已更改为 “evTimeOutError”，此状态包含在 SNMP Varbind 5 中。
1.3.6.1.4.1.232.0.8026	存储系统风扇状态已更改为 “正常”，此状态包含在 SNMP Varbind 9 中。
	存储系统风扇状态已更改为 “故障”，此状态包含在 SNMP Varbind 9 中。
	存储系统风扇状态已更改为 “降级”，此状态包含在 SNMP Varbind 9 中。
	存储系统风扇状态已更改为 “无风扇”，此状态包含在 SNMP Varbind 9 中。

MIB ID	SNMP 陷阱描述
1.3.6.1.4.1.232.0.8027	存储系统温度状态为 “降级”，此状态包含在 SNMP Varbind 9 中。
	存储系统温度状态为 “故障”，此状态包含在 SNMP Varbind 9 中。
	存储系统温度状态为 “正常”，此状态包含在 SNMP Varbind 9 中。
	存储系统温度状态已更改为 “无温度”，此状态包含在 SNMP Varbind 9 中。
1.3.6.1.4.1.232.0.8028	存储系统电源部件状态为 “降级”，此状态包含在 SNMP Varbind 9 中
	存储系统电源部件状态为 “故障”，此状态包含在 SNMP Varbind 9 中。
	存储系统电源单元状态为 “正常”，此状态包含在 SNMP Varbind 9 中。
	存储系统电源单元状态为 “noFltTolPower”，此状态包含在 SNMP Varbind 9 中。
1.3.6.1.4.1.232.0.8029	存储系统风扇状态已更改为 “正常”，此状态包含在 SNMP Varbind 9 中。
	存储系统风扇状态已更改为 “故障”，此状态包含在 SNMP Varbind 9 中。
	存储系统风扇状态已更改为 “降级”，此状态包含在 SNMP Varbind 9 中。
	存储系统风扇状态已更改为 “无风扇”，此状态包含在 SNMP Varbind 9 中。
1.3.6.1.4.1.232.0.8030	存储系统温度状态已更改为 “正常”，此状态包含在 SNMP Varbind 9 中。
	存储系统温度状态已更改为 “降级”，此状态包含在 SNMP Varbind 9 中。
	存储系统温度状态已更改为 “故障”，此状态包含在 SNMP Varbind 9 中。
	存储系统温度状态已更改为 “无温度”，此状态包含在 SNMP Varbind 9 中。
1.3.6.1.4.1.232.0.8031	存储系统电源状态已更改为 “降级”，此状态包含在 SNMP Varbind 9 中。
	存储系统电源状态已更改为 “故障”，此状态包含在 SNMP Varbind 9 中。
	存储系统电源状态已更改为 “noFltTolPower”，此状态包含在 SNMP Varbind 9 中。

对于以上每个 SNMP 陷阱，此策略均包含一条规则。问题解决之后，将自动确认之前的警报消息。

虚拟连接模块陷阱监视策略

SI-HPProLiant_VCModuleTraps

SI-HPProLiant_VCModuleTraps 策略拦截与虚拟连接模块有关的 SNMP 陷阱。每次生成陷阱后该策略便向 HPOM 控制台发送警报。

它将监视以下陷阱：

MIB ID	SNMP 陷阱描述
1.3.6.1.4.1.11.5.7.5.2.3.2.11	vcModPortInputUtilizationUp

对于此 SNMP 陷阱，此策略包含一条规则。问题解决之后，将自动确认之前的警报消息。

SIM 代理程序进程监视策略

SI-SIMAgentProcessMonitor

SI-SIMAgentProcessMonitor 策略是检查 IM 代理程序是否已安装的测量阈值策略。该策略每 5 分钟运行一次，如果 IM 代理程序未安装或已关闭就向 HPOM 控制台发送消息。

容量策略

容量监视可用于提供所需服务级别和成本的性能。它确保 IT 基础结构的容量能与不断发展的业务需求相对应。还可识别出利用不足和利用过度的资源。监视一段时间内这些方面的变化情况有助于了解它们对 IT 资源利用率的影响。您可以分析系统资源的当前和历史性能，以准确预测未来的容量需求。这些策略的默认策略组为：

基础结构管理 → < *语言* > → **系统基础结构** → **容量**

磁盘容量监视策略

SI-DiskCapacityMonitor

此策略将监视被管节点上磁盘的容量参数。对于每个磁盘，此策略会检查空间利用率和可用空间，以及 Linux 节点上的索引节点利用率。当可用空间、空间利用率或索引节点利用率超出指定的阈值时，此策略将向 HPOM 控制台发送警报。

使用的度量	• FS_MAX_SIZE • FS_SPACE_USED • FS_SPACE_UTIL • FS_DIRNAME • FS_INODE_UTIL （不适用于 Windows）
支持的平台	• Microsoft Windows • Red Hat Enterprise Linux • Suse Linux Enterprise Server • HP-UX • IBM AIX • Oracle Solaris

脚本参数	**描述**
SpaceUtilCriticalThreshold	此阈值表示磁盘上已利用的空间。将此阈值设置为将收到严重性为 “严重”的消息的值。
SpaceUtilMajorThreshold	将此阈值设置为将收到严重性为 “主要”的消息的值。
SpaceUtilMinorThreshold	将此阈值设置为将收到严重性为 “轻微”的消息的值。
SpaceUtilWarningThreshold	将此阈值设置为将收到严重性为 “警告”的消息的值。
InodeUtilCriticalThreshold	此阈值是 Linux 系统上索引节点的利用率百分比 （0 到 100%）。将此阈值设置为将收到严重性为 “严重”的消息的值。
InodeUtilMajorThreshold	将此阈值设置为将收到严重性为 “重大”的消息的节点的最小利用空间值。
InodeUtilMinorThreshold	将此阈值设置为将收到严重性为 “轻微”的消息的值。
InodeUtilWarningThreshold	将此阈值设置为将收到严重性为 “警告”的消息的值。
FreeSpaceCriticalThreshold	此阈值表示磁盘 / 文件系统上的可用空间 （以 MB 为单位）。将此阈值设置为磁盘的最小可用空间值，低于该值便会收到严重性为 “严重”的消息。
FreeSpaceMajorThreshold	将此阈值设置为磁盘的最小可用空间值，低于该值便会收到严重性为 “重大”的消息。
FreeSpaceMinorThreshold	将此阈值设置为磁盘的最小可用空间值，低于该值便会收到严重性为 “轻微”的消息。

FreeSpaceWarningThreshold	将此阈值设置为磁盘的最小可用空间值，低于该值便会收到严重性为 “警告”的消息。
MessageGroup	传出消息的消息组。
Debug	将此值设为 **0** 可禁用跟踪消息，设为 **1** 可在控制台接收跟踪消息，设为 **2** 可在被管节点上的跟踪文件中记录跟踪消息。有关详细信息，请参阅跟踪。

您可以为被管节点上的驱动器 / 文件系统设置不同的阈值。设置这些阈值时，策略参数可以采用多个以逗号分隔的值，如下例所示：

- **FreeSpaceMinorThreshold 45**

在此示例中，被管节点上所有磁盘 / 文件系统的阈值均设置为 45 MB。如果磁盘 / 文件系统的可用空间低于阈值，则策略将发送严重性为 “轻微”的警报。

- **SpaceUtilCriticalThreshold /=65,95,c:=65**

在此示例中，“/”和 “*C:*”驱动器的阈值设置为 65%，而被管节点上的所有其他驱动器 / 文件系统的阈值设置为 95%。如果这些驱动器 / 文件系统的系统利用率超过阈值，则策略将发送严重警报。

- **InodeUtilCriticalThreshold /opt=85,/=88**

在此示例中，“*/opt*”驱动器的阈值设置为 85%，“/”驱动器的阈值设置为 88%。如果索引节点利用率超过阈值，则策略将发送严重警报。此策略将不会监视被管节点上其余的驱动器 / 文件系统。

- **FreeSpaceMajorThreshold E:=200,256,F:=512,c:=1024,/=1024**

在此示例中，“*E:*”驱动器的阈值设置为 200，“*F:*”驱动器的阈值设置为 512，“*C:*”驱动器的阈值设置为 1024，“/”驱动器的阈值设置为 1024，而被管节点上的其余驱动器的阈值设置为 256。如果可用空间低于阈值，则策略将发送严重性为 “重大”的警报。

- **InodeUtilCriticalThreshold <null>**

  InodeUtilMajorThreshold <null>

  InodeUtilMinorThreshold <null>

  InodeUtilWarningThreshold <null>

在此示例中，没有为驱动器 / 文件系统设置阈值。此策略将不会监视任何驱动器 / 文件系统的索引节点利用率。

交换空间容量监视策略

SI-SwapCapacityMonitor

此策略将监视系统的交换空间利用率。

使用的度量	• GBL_SWAP_SPACE_AVAIL • GBL_SWAP_SPACE_UTIL • GBL_SWAP_SPACE_USED
支持的平台	• Microsoft Windows • Red Hat Enterprise Linux • Suse Linux Enterprise Server • HP-UX • IBM AIX • Oracle Solaris

脚本参数	**描述**
SwapSpaceUtilCriticalThreshold	此阈值是节点上交换空间的利用率百分比 （0 到 100%）。将此阈值设置为将收到严重性为 “严重” 的消息的磁盘最小可用交换空间值。
SwapSpaceUtilMajorThreshold	将此阈值设置为将收到严重性为 “重大” 的消息的节点最小利用交换空间值。
SwapSpaceUtilMinorThreshold	将此阈值设置为将收到严重性为 “轻微” 的消息的节点最小利用空间值。
SwapSpaceUtilWarningThreshold	将此阈值设置为将收到严重性为 “警告” 的消息的节点最小利用空间值。
FreeSwapSpaceAvailCriticalThreshold	此阈值表示磁盘 / 文件系统上的可用交换空间 （以 MB 为单位）。将此阈值设置为将收到严重性为 “严重” 的消息的磁盘最小可用空间值。
FreeSwapSpaceAvailMajorThreshold	将此阈值设置为将收到严重性为 “重大” 的消息的磁盘最小可用交换空间值。
FreeSwapSpaceAvailMinorThreshold	将此阈值设置为将收到严重性为 “轻微” 的消息的磁盘最小可用交换空间值。
FreeSwapSpaceAvailWarningThreshold	将此阈值设置为将收到严重性为 “警告” 的消息的磁盘最小可用交换空间值。
MessageGroup	传出消息的消息组。
Debug	将此值设为 **0** 可禁用跟踪消息，设为 **1** 可在控制台接收跟踪消息，设为 **2** 可在被管节点上的跟踪文件中记录跟踪消息。有关详细信息，请参阅跟踪。

内存利用率监视策略

SI-MemoryUtilization-AT

此策略将监视操作系统的总体内存利用率。此策略使用自动确定阈值的方式，根据之前日期的内存利用率自动计算阈值。

此策略依赖于历史数据。要得到精确结果，请在 Performance Agent 收集到一周的数据之后再部署策略。

使用的度量	GBL_MEM_UTIL
支持的平台	• Microsoft Windows • Red Hat Enterprise Linux • Suse Linux Enterprise Server • HP-UX • IBM AIX • Oracle Solaris
脚本参数	**描述**
MessageApplication	输入一个合适的值，帮助识别策略向管理控制台发送的消息。
DataSource	将 HP 嵌入式性能组件 (EPC) 数据源名称显示为 CODA。
DataObject	将 HP 嵌入式性能组件 (EPC) 数据对象名称显示为 Global。
DataMetric	将 HP 嵌入式性能组件 (EPC) 度量名称显示为 GBL_MEM_UTIL。
BaselinePeriod	输入要定义为基线期的时间段，例如 “3600 秒”。此时间段会随当前时间变化，最近的 3600 秒 （1 小时）会成为当前的基线期。
MinimumValue	显示度量所表示的内存消耗的最小值。
MaximumValue	显示度量所表示的内存消耗的最大值。
WarningDeviations	显示不在正常范围内的标准偏差数量，策略会向 HPOM 控制台发送严重性为 “警告” 的消息。为此参数设置一个合适的值。要禁用此参数，请将值设置为 *5*。
MinorDeviations	显示不在正常范围内的标准偏差数量，策略会向 HPOM 控制台发送严重性为 “轻微” 的消息。为此参数设置一个大于 WarningDeviations 指定值的合适值。要禁用此参数，请将值设置为 *5*。

MajorDeviations	显示不在正常范围内的标准偏差数量，策略会向 HPOM 控制台发送严重性为 “重大” 的消息。为此参数设置一个大于 MinorDeviations 指定值的合适值。要禁用此参数，请将值设置为 *5*。
WarningHighSeverity	显示当前数据符合或超过 *WarningDeviations* 中指定值的样本数据平均值时，发送到 HPOM 控制台的警报消息的严重性。要禁用此参数，请将值设置为 *none*。
MinorHighSeverity	显示当前数据符合或超过 *MinorDeviations* 中指定值的样本数据平均值时，发送到 HPOM 控制台的警报消息的严重性。要禁用此参数，请将值设置为 *none*。
MajorHighSeverity	显示当前数据符合或超过 *MajorDeviations* 中指定值的样本数据平均值时，发送到 HPOM 控制台的警报消息的严重性。要禁用此参数，请将值设置为 *none*。
WarningLowSeverity	显示当前数据符合或低于 *WarningDeviations* 中指定值的样本数据平均值时，发送到 HPOM 控制台的警报消息的严重性。要禁用此参数，请将值设置为 *none*。
MinorLowSeverity	显示当前数据符合或低于 *MinorDeviations* 中指定值的样本数据平均值时，发送到 HPOM 控制台的警报消息的严重性。要禁用此参数，请将值设置为 *none*。
MajorLowSeverity	显示当前数据符合或低于 *MajorDeviations* 中指定值的样本数据平均值时，发送到 HPOM 控制台的警报消息的严重性。要禁用此参数，请将值设置为 *none*。
InstanceSource	请勿编辑此参数值。
MemUtilCutOff	请设置一个值，低于此值便不再监视内存利用率。
DebugLevel	将此值设为 **0** 可禁用跟踪消息，设为 **1** 可在控制台接收跟踪消息，设为 **2** 可在被管节点上的跟踪文件中记录跟踪消息。有关详细信息，请参阅跟踪。
MessageGroup	传出消息的消息组。

交换利用率监视策略

SI-SwapUtilization-AT

此策略将监视被管节点上系统使用的总体交换空间。此策略使用自动确定阈值的方式，根据之前日期的交换空间利用率自动计算阈值。

此策略依赖于历史数据。要得到精确结果，请在 Performance Agent 收集到一周的数据之后再部署策略。

使用的度量	GBL_SWAP_SPACE_USED
支持的平台	• Microsoft Windows • Red Hat Enterprise Linux • Suse Linux Enterprise Server • HP-UX • IBM AIX • Oracle Solaris
脚本参数	**描述**
MessageApplication	输入一个合适的值，帮助识别策略向管理控制台发送的消息。
DataSource	将 HP 嵌入式性能组件 (EPC) 数据源名称显示为 CODA。
DataObject	将 HP 嵌入式性能组件 (EPC) 数据对象名称显示为 Global。
DataMetric	将 HP 嵌入式性能组件 (EPC) 度量名称显示为 GBL_SWAP_SPACE_USED。
BaselinePeriod	输入要定义为基线期的时间段，例如 “3600 秒”。此时间段会随当前时间变化，最近的 3600 秒 （1 小时）会成为当前的基线期。
MinimumValue	显示度量所表示的最小交换空间利用率。
MaximumValue	显示度量所表示的最大交换空间利用率。
WarningDeviations	显示不在正常范围内的标准偏差数量，策略会向 HPOM 控制台发送严重性为 “警告” 的消息。为此参数设置一个合适的值。要禁用此参数，请将值设置为 *5*。
MinorDeviations	显示不在正常范围内的标准偏差数量，策略会向 HPOM 控制台发送严重性为 “轻微” 的消息。为此参数设置一个大于 WarningDeviations 指定值的合适值。要禁用此参数，请将值设置为 *5*。

MajorDeviations	显示不在正常范围内的标准偏差数量，策略会向 HPOM 控制台发送严重性为 “重大” 的消息。为此参数设置一个大于 MinorDeviations 指定值的合适值。要禁用此参数，请将值设置为 *5*。
WarningHighSeverity	显示当前数据符合或超过 *WarningDeviations* 中指定值的样本数据平均值时，发送到 HPOM 控制台的警报消息的严重性。要禁用此参数，请将值设置为 *none*。
MinorHighSeverity	显示当前数据符合或超过 *MinorDeviations* 中指定值的样本数据平均值时，发送到 HPOM 控制台的警报消息的严重性。要禁用此参数，请将值设置为 *none*。
MajorHighSeverity	显示当前数据符合或超过 *MajorDeviations* 中指定值的样本数据平均值时，发送到 HPOM 控制台的警报消息的严重性。要禁用此参数，请将值设置为 *none*。
WarningLowSeverity	显示当前数据符合或低于 *WarningDeviations* 中指定值的样本数据平均值时，发送到 HPOM 控制台的警报消息的严重性。要禁用此参数，请将值设置为 *none*。
MinorLowSeverity	显示当前数据符合或低于 *MinorDeviations* 中指定值的样本数据平均值时，发送到 HPOM 控制台的警报消息的严重性。要禁用此参数，请将值设置为 *none*。
MajorLowSeverity	显示当前数据符合或低于 *MajorDeviations* 中指定值的样本数据平均值时，发送到 HPOM 控制台的警报消息的严重性。要禁用此参数，请将值设置为 *none*。
InstanceSource	请勿编辑此参数值。
DebugLevel	将此值设为 **0** 可禁用跟踪消息，设为 **1** 可在控制台接收跟踪消息，设为 **2** 可在被管节点上的跟踪文件中记录跟踪消息。有关详细信息，请参阅跟踪。
MessageGroup	传出消息的消息组。
SwapUtilCutOff	请设置一个值，低于此值便不再监视交换空间利用率。

每个 CPU 利用率监视策略

SI-PerCPUUtilization-AT

此策略将监视被管节点上每个 CPU 的利用率，将在每个间隔内单独处理每个 CPU 实例。此策略使用自动确定阈值的方式，根据之前日期的 CPU 利用率自动计算阈值。

此策略依赖于历史数据。要得到精确结果，请在 Performance Agent 收集到一周的数据之后再部署策略。

使用的度量	BYCPU_CPU_TOTAL_UTIL
支持的平台	• Microsoft Windows • Red Hat Enterprise Linux • Suse Linux Enterprise Server • HP-UX • IBM AIX • Oracle Solaris
脚本参数	**描述**
MessageApplication	输入一个合适的值，帮助识别策略向管理控制台发送的消息。
DataSource	将 HP 嵌入式性能组件 (EPC) 数据源名称显示为 CODA。
DataObject	将 HP 嵌入式性能组件 (EPC) 数据对象名称显示为 Global。
DataMetric	将 HP 嵌入式性能组件 (EPC) 度量名称显示为 BYCPU_CPU_TOTAL_UTIL。
BaselinePeriod	输入要定义为基线期的时间段，例如 “3600 秒”。此时间段会随当前时间变化。最近的 3600 秒 （1 小时）会成为当前的基线期。
MinimumValue	显示度量所表示的 CPU 消耗的最小值。
MaximumValue	显示度量所表示的 CPU 消耗的最大值。
WarningDeviations	显示不在正常范围内的标准偏差数量，策略会向 HPOM 控制台发送严重性为 “警告” 的消息。为此参数设置一个合适的值。要禁用此参数，请将值设置为 *5*。
MinorDeviations	显示不在正常范围内的标准偏差数量，策略会向 HPOM 控制台发送严重性为 “轻微” 的消息。为此参数设置一个大于 WarningDeviations 指定值的合适值。要禁用此参数，请将值设置为 *5*。

MajorDeviations	显示不在正常范围内的标准偏差数量，策略会向 HPOM 控制台发送严重性为 “重大” 的消息。为此参数设置一个大于 MinorDeviations 指定值的合适值。要禁用此参数，请将值设置为 *5*。
WarningHighSeverity	显示当前数据符合或超过 *WarningDeviations* 中指定值的样本数据平均值时，发送到 HPOM 控制台的警报消息的严重性。要禁用此参数，请将值设置为 *none*。
MinorHighSeverity	显示当前数据符合或超过 *MinorDeviations* 中指定值的样本数据平均值时，发送到 HPOM 控制台的警报消息的严重性。要禁用此参数，请将值设置为 *none*。
MajorHighSeverity	显示当前数据符合或超过 *MajorDeviations* 中指定值的样本数据平均值时，发送到 HPOM 控制台的警报消息的严重性。要禁用此参数，请将值设置为 *none*。
WarningLowSeverity	显示当前数据符合或低于 *WarningDeviations* 中指定值的样本数据平均值时，发送到 HPOM 控制台的警报消息的严重性。要禁用此参数，请将值设置为 *none*。
MinorLowSeverity	显示当前数据符合或低于 *MinorDeviations* 中指定值的样本数据平均值时，发送到 HPOM 控制台的警报消息的严重性。要禁用此参数，请将值设置为 *none*。
MajorLowSeverity	显示当前数据符合或低于 *MajorDeviations* 中指定值的样本数据平均值时，发送到 HPOM 控制台的警报消息的严重性。要禁用此参数，请将值设置为 *none*。
InstanceSource	请勿编辑此参数值。
DebugLevel	将此值设为 **0** 可禁用跟踪消息，设为 **1** 可在控制台接收跟踪消息，设为 **2** 可在被管节点上的跟踪文件中记录跟踪消息。有关详细信息，请参阅跟踪。
MessageGroup	传出消息的消息组。
CPUUtilCutOff	请设置一个值，低于此值便不再监视 CPU 利用率。

远程驱动器空间利用率监视策略

SI-MSWindowsRemoteDriveSpaceUtilization

SI-MSWindowsRemoteDriveSpaceUtilization 策略将监视 Microsoft Windows 平台上远程驱动器的空间利用率级别。此策略的默认策略组为：

基础结构管理 → *< 语言 >* → 系统基础结构 → 容量 → Windows

源类型	WMI
支持的平台	Microsoft Windows
脚本参数	**描述**
SpaceUtilCriticalThreshold	此阈值是所监视远程驱动器上的空间利用率百分比（0 到 100%）。将此阈值设置为将收到严重性为 “严重” 的消息的驱动器最小可用空间值。
SpaceUtilMajorThreshold	将此阈值设置为将收到严重性为 “重大” 的消息的驱动器最小可用空间值。
SpaceUtilMinorThreshold	将此阈值设置为将收到严重性为 “轻微” 的消息的驱动器最小可用空间值。
SpaceUtilWarningThreshold	将此阈值设置为将收到严重性为 “警告” 的消息的驱动器最小可用空间值。
MessageGroup	传出消息的消息组。
Debug	将此值设为 0 可禁用跟踪消息，设为 1 可在控制台接收跟踪消息，设为 2 可在被管节点上的跟踪文件中记录跟踪消息。有关详细信息，请参阅跟踪。
AssignMessageToRemoteHost	可以将此值设置为 1，将警报消息的源显示为远程主机。默认情况下消息会分配到发出消息的被管节点。

NFS 文件系统的远程驱动器空间利用率监视策略

SI-LinuxNfsUtilizationMonitor

SI-LinuxNfsUtilizationMonitor 策略将监视 Linux 平台上 NFS 远程文件系统的空间利用率级别。此策略的默认策略组为：

基础结构管理 → *< 语言 >* → 系统基础结构 → 容量 → Linux

支持的平台	• Red Hat Enterprise Linux • Suse Linux Enterprise Server
脚本参数	**描述**
SpaceUtilCriticalThreshold	此阈值是所监视远程文件系统上的空间利用率百分比 （0 到 100%）。将此阈值设置为将收到严重性为 “严重” 的消息的文件系统最小可用空间值。

SpaceUtilMajorThreshold	将此阈值设置为将收到严重性为 “重大”的消息的文件系统最小可用空间值。
SpaceUtilMinorThreshold	将此阈值设置为将收到严重性为 “轻微”的消息的文件系统最小可用空间值。
SpaceUtilWarningThreshold	将此阈值设置为将收到严重性为 “警告”的消息的文件系统最小可用空间值。
NfsFileSystemType	指定要监视空间利用率级别的文件系统类型。例如，如果指定 NFS，则此策略将监视所有 NFS 远程文件系统的空间利用率级别。
AssignMessageToRemoteHost	可以将此值设置为 1，将警报消息的源显示为远程主机。默认情况下消息会分配到发出消息的被管节点。
MessageGroup	传出消息的消息组。
Debug	将此值设为 0 可禁用跟踪消息，设为 1 可在控制台接收跟踪消息，设为 2 可在被管节点上的跟踪文件中记录跟踪消息。有关详细信息，请参阅跟踪。

CIFS 文件系统的远程驱动器空间利用率监视策略

SI-LinuxCifsUtilizationMonitor

SI-LinuxCifsUtilizationMonitor 策略将监视 Linux 平台上 CIFS 远程文件系统的空间利用率级别。此策略的默认策略组为：

基础结构管理 → < *语言* > → 系统基础结构 → 容量 → Linux

支持的平台	• Red Hat Enterprise Linux • Suse Linux Enterprise Server
脚本参数	**描述**
SpaceUtilCriticalThreshold	此阈值是所监视远程文件系统上的空间利用率百分比 （0 到 100%）。将此阈值设置为将收到严重性为 “严重”的消息的文件系统最小可用空间值。
SpaceUtilMajorThreshold	将此阈值设置为将收到严重性为 “重大”的消息的文件系统最小可用空间值。
SpaceUtilMinorThreshold	将此阈值设置为将收到严重性为 “轻微”的消息的文件系统最小可用空间值。

SpaceUtilWarningThreshold	将此阈值设置为将收到严重性为 “警告” 的消息的文件系统最小可用空间值。
CifsFileSystemType	指定要监视空间利用率级别的文件系统类型。例如，如果指定 CIFS，则此策略将监视所有 CIFS 远程文件系统的空间利用率级别。此策略可用于监视 *cifs* 和 *smb* 文件系统类型。
AssignMessageToRemoteHost	可以将此值设置为 1，将警报消息的源显示为远程主机。默认情况下消息会分配到发出消息的被管节点。
MessageGroup	传出消息的消息组。
Debug	将此值设为 0 可禁用跟踪消息，设为 1 可在控制台接收跟踪消息，设为 2 可在被管节点上的跟踪文件中记录跟踪消息。有关详细信息，请参阅跟踪。

分页和未分页池利用率策略

SI-MSWindowsPagedPoolUtilization 和 SI-MSWindowsNonPagedPoolUtilization

SI-MSWindowsPagedPoolUtilization 策略将监视注册表数据写入到分页文件时的内存，而 SI-MSWindowsNonPagedPoolUtilization 策略将监视系统无法处理页面错误时存储数据的内存。此策略的默认策略组为：

基础结构管理 → *< 语言 >* → 系统基础结构 → 容量 → Windows

使用的度量	• GBL_MEM_PAGED_POOL_BYTES • GBL_MEM_NONPAGED_POOL_BYTES
支持的平台	Microsoft Windows
脚本参数	**描述**
BaselinePeriod	输入要定义为基线期的时间段，例如 “900 秒”。此时间段会随当前时间变化，最近的 900 秒会成为当前的基线期。

WarningDeviations	显示不在正常范围内的标准偏差数量，策略会向 HPOM 控制台发送严重性为 “警告” 的消息。为此参数设置一个合适的值。要禁用此参数，请将值设置为 *4.5*。
MinorDeviations	显示不在正常范围内的标准偏差数量，策略会向 HPOM 控制台发送严重性为 “轻微” 的消息。为此参数设置一个大于 WarningDeviations 指定值的合适值。要禁用此参数，请将值设置为 *5.5*。
MajorDeviations	显示不在正常范围内的标准偏差数量，策略会向 HPOM 控制台发送严重性为 “重大” 的消息。为此参数设置一个大于 MinorDeviations 指定值的合适值。要禁用此参数，请将值设置为 *7.5*。

日志监视策略

系统基础结构 SPI 提供了日志文件策略，可监视被管节点的关键日志。这些策略的默认策略组为：

基础结构管理 → < *语言* > → 系统基础结构 → 日志

Linux 系统服务日志文件策略

Linux 系统服务日志文件策略将监视 Red Hat 和 Suse enterprise Linux 版本的关键系统服务日志。这些策略的默认策略组为：

基础结构管理 → < *语言* > → 系统基础结构 → 日志 → Linux

启动日志策略

SI-LinuxBootLog

此策略将监视启动日志文件 `/var/log/boot.log`，并在出现系统启动错误时发出警报。默认的轮询间隔是 5 分钟。

此策略将检查以下条件：

条件	描述
服务启动失败	查找与 <*> <@.service> 匹配的错误条件：启动日志文件中的 <@.daemon> 启动失败模式。如果发现匹配，则此条件将向 HPOM 控制台发送严重性为 “轻微” 的消息，其中含有相应的消息属性。
服务失败	查找与 <*> <@.service> 匹配的错误条件：日志文件中的 <*.msg> 失败模式。如果发现匹配，则此条件将向 HPOM 控制台发送严重性为 “严重” 的消息，其中含有相应的消息属性。

安全日志策略

SI-LinuxSecureLog

此策略将监视 /var/log/secure 和 /var/log/messages 中的日志文件，并在出现安全登录失败时发出警报。默认的轮询间隔是 5 分钟。

此策略将检查以下条件：

条件	描述
身份验证失败	查找与 <*> sshd\[<#>\] 匹配的错误条件：安全日志文件中来自 <*.host> 端口 <#> ssh2 的 <@.user> 模式的密码错误。如果发现匹配，则此条件将向 HPOM 控制台发送严重性为 “轻微” 的消息，其中含有相应的消息属性。

内核日志策略

SI-LinuxKernelLog

此策略将监视内核日志文件 /var/log/messages，并在出现内核服务失败时发出警报。默认的轮询间隔是 5 分钟。

此策略将检查以下条件：

条件	描述
内核服务故障	查找与 <*> 内核匹配的错误条件：<@.service>：内核日志文件中的 <*.msg> 失败模式。如果发现匹配，则此条件将向 HPOM 控制台发送严重性为 “轻微” 的消息，其中含有相应的消息属性。

Windows 系统服务日志文件策略

Windows Server 日志文件策略将监视 Microsoft Windows 2008 或更高版本的关键系统服务日志。这些策略的默认策略组为：

基础结构管理 → *< 语言 >* → 系统基础结构 → 日志 → MS Windows Server

NFS 日志策略

SI-MSWindowsServer_NFSWarnError

此策略将监视 NFS 服务器进程的 NFS 日志文件，并将严重性为 “警告” 或 “错误” 的错误消息转发到 HPOM 控制台。默认的轮询间隔是 1 分钟。此策略将查找 NFS 日志文件中所记录的以下错误：

- NFS 服务器检测到磁盘空间较小，已停止记录审计。
- 审计日志已达到其最大文件大小。
- NFS 服务器无法注册到 RPC 端口映射器。
- NFS 驱动程序在第 2 阶段初始化期间失败。

DNS 日志策略

SI-MSWindowsServer_DNSWarnError

此策略将监视 Microsoft DNS 服务器服务及其相应进程的日志文件，并将严重性为 “警告” 或 “错误” 的错误日志条目转发到 HPOM 控制台。默认的轮询间隔是 1 分钟。此策略将查找 DNS 日志文件中所记录的以下错误：

- DNS 服务器无法为资源记录分配内存。
- DNS 服务器由于缺少可用内存而无法响应客户端请求。
- DNS 服务器无法创建区域传输线程。
- DNS 服务器在写入文件时遇到错误。
- DNS 服务器无法初始化 Remote Procedure Call (RPC) 服务。

Windows 登录策略

SI-MSWindowsServer_WindowsLogonWarnError

此策略将监视 Windows 登录和初始化事件日志，并将严重性级别为 “警告” 或 “错误” 的错误日志条目转发到 HPOM 控制台。默认的轮询间隔是 1 分钟。此策略将查找 Windows 日志文件中所记录的以下错误：

- Windows 许可证无效
- 激活 Windows 许可证失败
- Windows 登录进程未能切换桌面
- Windows 登录进程意外终止
- Windows 登录进程未能生成用户应用程序
- Windows 登录进程未能终止当前已登录用户的进程
- Windows 登录进程未能断开用户会话的连接

终端服务日志策略

SI-MSWindowsServer_TerminalServiceWarnError

此策略将监视 Windows 终端服务及其相应进程的日志文件，并将严重性为 “警告”或 “错误”的错误日志条目转发到 HPOM 控制台。默认的轮询间隔是 1 分钟。此策略将查找 Windows 终端服务日志文件中所记录的以下错误：

- 由于终端服务器当前配置为不接受任何连接，因此已拒绝连接请求
- 因为身份验证失败，自动重新连接未能将用户重新连接到会话
- 终端服务未能启动
- 终端服务器接收到大量未完成连接

Windows Server DHCP 错误

SI-MSWindowsServer_DHCPWarnError

此策略将监视 DHCP 服务器与客户端服务及其相应进程的日志文件，并将严重性为 “警告”或 “错误”的错误日志条目转发到 HPOM 控制台。默认的轮询间隔是 1 分钟。此策略将查找 Windows 终端服务日志文件中所记录的以下错误：

- Iashlpr 无法联系 NPS 服务
- 作用域或超级作用域中没有 BOOTP 客户端的可用 IP 地址
- DHCP 服务器无法到达 NPS 服务器以确定客户端的 NAP 访问状态
- 作用域或超级作用域中没有可用于租用的 IP 地址
- 本地计算机上的 DHCP/BINL 服务已确定自身未获准启动
- DHCP 服务无法初始化审计日志
- 此工作组服务器中的 DHCP/BINL 服务遇到另一个带有 IP 地址的服务器
- DHCP 服务无法恢复 DHCP 注册表配置
- DHCP 服务无法从注册表读取全局 BOOTP 文件名
- DHCP 服务无法为任何客户端提供服务，因为没有任何活动接口
- 没有任何静态 IP 地址绑定到 DHCP 服务器
- DHCP 服务器服务无法注册到服务控制器
- DHCP 服务器服务无法初始化其注册表参数

AIX 系统日志文件监视策略

AIX 系统日志文件监视策略将监视关键系统错误。这些策略的默认策略组为：

基础结构管理 → < *语言* > → 系统基础结构 → 日志 → AIX

ERRPT 日志监视策略

SI-AIXErrptLog

“errpt”命令的输出作为系统错误存储在 `errpt.log` 文件中。 SI-AIXErrptLog 策略将监视日志文件，并将日志条目发送到 HPOM 控制台作为严重性为 “警告”的消息。警报内容包含错误代码、类和中断。

性能策略

性能监视可帮助预测性能故障，并在基础结构问题威胁到服务质量之前确定这些问题。收集的性能数据可用于在服务器、操作系统、网络设备和应用程序的整个基础结构之间关联事件，以阻止发展中的性能问题并确定其根本原因。

这些策略的默认策略组为：

基础结构管理 → *< 语言 >* → 系统基础结构 → 性能

磁盘性能策略

SI-PerDiskAvgServiceTime-AT

此策略将监视被管节点上的磁盘性能，并在磁盘读写服务时间违反阈值级别时发出警报。此策略要求在被管节点上运行 Performance Agent。

此策略依赖于历史数据。要得到精确结果，请在 Performance Agent 收集到一周的数据之后再部署策略

使用的度量	BYDSK_AVG_SERVICE_TIME
支持的平台	• Microsoft Windows • Red Hat Enterprise Linux • Suse Linux Enterprise Server • HP-UX • IBM AIX • Oracle Solaris
脚本参数	**描述**
MessageApplication	输入一个合适的值，帮助识别 SI-PerDiskAvgServiceTime-AT 策略向管理控制台发送的消息。
DataSource	将 HP 嵌入式性能组件 (EPC) 数据源名称显示为 SCOPE。
DataObject	将 HP 嵌入式性能组件 (EPC) 数据对象名称显示为 DISK。
DataMetric	将 HP 嵌入式性能组件 (EPC) 度量名称显示为 BYDSK_AVG_SERVICE_TIME。
BaselinePeriod	输入要定义为基线期的时间段，例如 “3600 秒”。此时间段会随当前时间变化。最近的 3600 秒 （1 小时）会成为当前的基线期。
MinimumValue	显示度量所表示的处理每个读写磁盘请求所用的最少平均时间。

MaximumValue	显示度量所表示的处理每个读写磁盘请求所用的最多平均时间。
WarningDeviations	显示不在正常范围内的标准偏差数量，策略会向 HPOM 控制台发送严重性为 “警告” 的消息。为此参数设置一个合适的值。要禁用此参数，请将值设置为 *5*。
MinorDeviations	显示不在正常范围内的标准偏差数量，策略会向 HPOM 控制台发送严重性为 “轻微” 的消息。为此参数设置一个大于 WarningDeviations 指定值的合适值。要禁用此参数，请将值设置为 *5*。
MajorDeviations	显示不在正常范围内的标准偏差数量，策略会向 HPOM 控制台发送严重性为 “重大” 的消息。为此参数设置一个大于 MinorDeviations 指定值的合适值。要禁用此参数，请将值设置为 *5*。
WarningHighSeverity	显示当前数据符合或超过 *WarningDeviations* 中指定值的样本数据平均值时，发送到 HPOM 控制台的警报消息的严重性。要禁用此参数，请将值设置为 *none*。
MinorHighSeverity	显示当前数据符合或超过 *MinorDeviations* 中指定值的样本数据平均值时，发送到 HPOM 控制台的警报消息的严重性。要禁用此参数，请将值设置为 *none*。
MajorHighSeverity	显示当前数据符合或超过 *MajorDeviations* 中指定值的样本数据平均值时，发送到 HPOM 控制台的警报消息的严重性。要禁用此参数，请将值设置为 *none*。
WarningLowSeverity	显示当前数据符合或低于 *WarningDeviations* 中指定值的样本数据平均值时，发送到 HPOM 控制台的警报消息的严重性。要禁用此参数，请将值设置为 *none*。
MinorLowSeverity	显示当前数据符合或低于 *MinorDeviations* 中指定值的样本数据平均值时，发送到 HPOM 控制台的警报消息的严重性。要禁用此参数，请将值设置为 *none*。

MajorLowSeverity	显示当前数据符合或低于 *MajorDeviations* 中指定值的样本数据平均值时，发送到 HPOM 控制台的警报消息的严重性。要禁用此参数，请将值设置为 *none*。
InstanceSource	请勿编辑此参数值。
DebugLevel	将此值设为 `0` 可禁用跟踪消息，设为 `1` 可在控制台接收跟踪消息，设为 `2` 可在被管节点上的跟踪文件中记录跟踪消息。有关详细信息，请参阅跟踪。
MessageGroup	传出消息的消息组。
DiskIOCutOff	请设置一个值，低于此值便不再监视磁盘读写服务时间。

全局 CPU 利用率监视策略

SI-GlobalCPUUtilization-AT

此策略将监视被管节点上的 CPU 性能，并在所有 CPU 中利用率违反阈值级别时发出警报。

此策略依赖于历史数据。要得到精确结果，请在 Performance Agent 收集到一周的数据之后再部署策略

使用的度量	GBL_CPU_TOTAL_UTIL
支持的平台	• Microsoft Windows • Red Hat Enterprise Linux • Suse Linux Enterprise Server • HP-UX • IBM AIX • Oracle Solaris
脚本参数	**描述**
MessageApplication	输入一个合适的值，帮助识别 SI-GlobalCPUUtilization-AT 策略向管理控制台发送的消息。
DataSource	将 HP 嵌入式性能组件 (EPC) 数据源名称显示为 CODA。
DataObject	将 HP 嵌入式性能组件 (EPC) 数据对象名称显示为 GLOBAL。
DataMetric	将 HP 嵌入式性能组件 (EPC) 度量名称显示为 GBL_CPU_TOTAL_UTIL。

BaselinePeriod	输入要定义为基线期的时间段，例如 “3600 秒”。此时间段会随当前时间变化。最近的 3600 秒 （1 小时）会成为当前的基线期。
MinimumValue	显示度量所表示的 CPU 非空闲时间的最小百分比。
MaximumValue	显示度量所表示的 CPU 非空闲时间的最大百分比。
WarningDeviations	显示不在正常范围内的标准偏差数量，策略会向 HPOM 控制台发送严重性为 “警告”的消息。为此参数设置一个合适的值。要禁用此参数，请将值设置为 *5*。
MinorDeviations	显示不在正常范围内的标准偏差数量，策略会向 HPOM 控制台发送严重性为 “轻微”的消息。为此参数设置一个大于 WarningDeviations 指定值的合适值。要禁用此参数，请将值设置为 *5*。
MajorDeviations	显示不在正常范围内的标准偏差数量，策略会向 HPOM 控制台发送严重性为 “重大”的消息。为此参数设置一个大于 MinorDeviations 指定值的合适值。要禁用此参数，请将值设置为 *5*。
WarningHighSeverity	显示当前数据符合或超过 *WarningDeviations* 中指定值的样本数据平均值时，发送到 HPOM 控制台的警报消息的严重性。要禁用此参数，请将值设置为 *none*。
MinorHighSeverity	显示当前数据符合或超过 *MinorDeviations* 中指定值的样本数据平均值时，发送到 HPOM 控制台的警报消息的严重性。要禁用此参数，请将值设置为 *none*。
MajorHighSeverity	显示当前数据符合或超过 *MajorDeviations* 中指定值的样本数据平均值时，发送到 HPOM 控制台的警报消息的严重性。要禁用此参数，请将值设置为 *none*。
WarningLowSeverity	显示当前数据符合或低于 *WarningDeviations* 中指定值的样本数据平均值时，发送到 HPOM 控制台的警报消息的严重性。要禁用此参数，请将值设置为 *none*。

MinorLowSeverity	显示当前数据符合或低于 *MinorDeviations* 中指定值的样本数据平均值时，发送到 HPOM 控制台的警报消息的严重性。要禁用此参数，请将值设置为 *none*。
MajorLowSeverity	显示当前数据符合或低于 *MajorDeviations* 中指定值的样本数据平均值时，发送到 HPOM 控制台的警报消息的严重性。要禁用此参数，请将值设置为 *none*。
InstanceSource	请勿编辑此参数值。
DebugLevel	将此值设为 `0` 可禁用跟踪消息，设为 `1` 可在控制台接收跟踪消息，设为 `2` 可在被管节点上的跟踪文件中记录跟踪消息。有关详细信息，请参阅跟踪。
MessageGroup	传出消息的消息组。

运行队列长度监视策略

SI-RunQueueLengthMonitor-AT

此策略将监视 CPU 运行队列中等待的进程数量，并在运行队列中的进程数量违反阈值级别时发出警报。

此策略依赖于历史数据。要得到精确结果，请在 Performance Agent 收集到一周的数据之后再部署策略。

使用的度量	GBL_RUN_QUEUE
支持的平台	• Microsoft Windows • Red Hat Enterprise Linux • Suse Linux Enterprise Server • HP-UX • IBM AIX • Oracle Solaris
脚本参数	**描述**
MessageApplication	输入一个合适的值，帮助识别策略向管理控制台发送的消息。
DataSource	将 HP 嵌入式性能组件 (EPC) 数据源名称显示为 CODA。
DataObject	将 HP 嵌入式性能组件 (EPC) 数据对象名称显示为 GLOBAL。
DataMetric	将 HP 嵌入式性能组件 (EPC) 度量名称显示为 GBL_RUN_QUEUE。

BaselinePeriod	输入要定义为基线期的时间段，例如 “3600 秒”。此时间段会随当前时间变化。最近的 3600 秒 （1 小时）会成为当前的基线期。
MinimumValue	显示度量所表示的在间隔期间运行队列中等待线程 / 进程的最小平均数量。
MaximumValue	显示度量所表示的在间隔期间运行队列中等待线程 / 进程的最大平均数量。
WarningDeviations	显示不在正常范围内的标准偏差数量，策略会向 HPOM 控制台发送严重性为 “警告”的消息。为此参数设置一个合适的值。要禁用此参数，请将值设置为 *5*。
MinorDeviations	显示不在正常范围内的标准偏差数量，策略会向 HPOM 控制台发送严重性为 “轻微”的消息。为此参数设置一个大于 WarningDeviations 指定值的合适值。要禁用此参数，请将值设置为 *5*。
MajorDeviations	显示不在正常范围内的标准偏差数量，策略会向 HPOM 控制台发送严重性为 “重大”的消息。为此参数设置一个大于 MinorDeviations 指定值的合适值。要禁用此参数，请将值设置为 *5*。
WarningHighSeverity	显示当前数据符合或超过 *WarningDeviations* 中指定值的样本数据平均值时，发送到 HPOM 控制台的警报消息的严重性。要禁用此参数，请将值设置为 *none*。
MinorHighSeverity	显示当前数据符合或超过 *MinorDeviations* 中指定值的样本数据平均值时，发送到 HPOM 控制台的警报消息的严重性。要禁用此参数，请将值设置为 *none*。
MajorHighSeverity	显示当前数据符合或超过 *MajorDeviations* 中指定值的样本数据平均值时，发送到 HPOM 控制台的警报消息的严重性。要禁用此参数，请将值设置为 *none*。
WarningLowSeverity	显示当前数据符合或低于 *WarningDeviations* 中指定值的样本数据平均值时，发送到 HPOM 控制台的警报消息的严重性。要禁用此参数，请将值设置为 *none*。

MinorLowSeverity	显示当前数据符合或低于 *MinorDeviations* 中指定值的样本数据平均值时，发送到 HPOM 控制台的警报消息的严重性。要禁用此参数，请将值设置为 *none*。
MajorLowSeverity	显示当前数据符合或低于 *MajorDeviations* 中指定值的样本数据平均值时，发送到 HPOM 控制台的警报消息的严重性。要禁用此参数，请将值设置为 *none*。
InstanceSource	请勿编辑此参数值。
DebugLevel	将此值设为 `0` 可禁用跟踪消息，设为 `1` 可在控制台接收跟踪消息，设为 `2` 可在被管节点上的跟踪文件中记录跟踪消息。有关详细信息，请参阅跟踪。
MessageGroup	传出消息的消息组。

网络利用率和性能策略

SI-NetworkUsageAndPerformance

此策略将监视系统的网络利用率并显示错误率和冲突，帮助识别可能的网络瓶颈。SI-NetworkUsageAndPerformance 策略只监视 vMA 计算机的物理 NIC。

此策略不会监视 Windows 操作系统上包冲突的性能数据，因为 Windows 操作系统上无法使用 BYNETIF_COLLISION 度量。

此策略中使用的以下度量要求在被管节点上运行 HP Performance Agent：BYNETIF_UTIL 和 BYNETIF_QUEUE。

使用的度量	• BYNETIF_IN_PACKET • BYNETIF_ID • BYNETIF_OUT_PACKET • BYNETIF_ERROR • BYNETIF_COLLISION • BYNETIF_OUT_BYTE_RATE • BYNETIF_IN_BYTE_RATE • BYNETIF_UTIL • BYNETIF_QUEUE • BYNETIF_NAME
支持的平台	• Microsoft Windows • Red Hat Enterprise Linux • Suse Linux Enterprise Server • HP-UX • IBM AIX • Oracle Solaris *以下脚本参数均适用于上述所有平台，参数描述中另有明确规定的除外。*
脚本参数	**描述**
NICByteRateCriticalThreshold	此参数将监视每秒传输的平均字节数，并在此值超过阈值时发送严重性为 “严重”的消息。可以设置接收此消息的阈值。
NICByteRateMajorThreshold	可以为每秒传输的平均字节数设置一个阈值，达到该阈值便会发送严重性为 “重大”的消息。
NICByteRateMinorThreshold	可以为每秒传输的平均字节数设置一个阈值，达到该阈值便会发送严重性为 “轻微”的消息。
NICByteRateWarningThreshold	可以为每秒传输的平均字节数设置一个阈值，达到该阈值便会发送严重性为 “警告”的消息。
NICErrPktRatePctCriticalThreshold	包错误率是未成功传输的包数量与发送的总包数量之间的百分比。此参数将监视包错误率，并在此值超过阈值时发出严重性为 “严重”的消息。
NICErrPktRatePctMajorThreshold	可以为包错误率设置一个阈值，达到该阈值便会发送严重性为 “重大”的消息。

NICErrPktRatePctMinorThreshold	可以为包错误率设置一个阈值，达到该阈值便会发送严重性为 “轻微”的消息。
NICErrPktRatePctWarningThreshold	可以为包错误率设置一个阈值，达到该阈值便会发送严重性为 “警告”的消息。
NICCollisionRatePctCriticalThreshold	此参数将监视冲突包数量与传输的总包数量之间的百分比。可以为冲突错误率设置一个阈值，达到该阈值便会发送严重性为 “严重”的消息。 *此参数不适用于 Windows。*
NICCollisionRatePctMajorThreshold	可以为冲突错误率设置一个阈值，达到该阈值便会发送严重性为 “重大”的消息。 *此参数不适用于 Windows。*
NICCollisionRatePctMinorThreshold	可以为冲突错误率设置一个阈值，达到该阈值便会发送严重性为 “轻微”的消息。 *此参数不适用于 Windows。*
NICCollisionRatePctWarningThreshold	可以为冲突错误率设置一个阈值，达到该阈值便会发送严重性为 “警告”的消息。 *此参数不适用于 Windows。*
NICOutBoundQueueLengthCriticalThreshold	此参数表示所有网络接口的出站队列中等待的包数量。可以为出站队列长度设置一个阈值，达到该阈值便会发送严重性为 “严重”的消息。 *此参数仅适用于 HP-UX 和 Windows。*
NICOutBoundQueueLengthMajorThreshold	可以为出站队列长度设置一个阈值，达到该阈值便会发送严重性为 “重大”的消息。 *此参数仅适用于 HP-UX 和 Windows。*
NICOutBoundQueueLengthMinorThreshold	可以为出站队列长度设置一个阈值，达到该阈值便会发送严重性为 “轻微”的消息。 *此参数仅适用于 HP-UX 和 Windows。*
NICOutBoundQueueLengthWarningThreshold	可以为出站队列长度设置一个阈值，达到该阈值便会发送严重性为 “警告”的消息。 *此参数仅适用于 HP-UX 和 Windows。*

NICBandwidthUtilCriticalThreshold	此参数表示已使用带宽与总可用带宽之间的百分比。可以为带宽利用率设置一个阈值，达到该阈值便会发送严重性为 “严重” 的消息。 *此参数仅适用于 HP-UX、AIX 和 Windows。*
NICBandwidthUtilMajorThreshold	可以为带宽利用率设置一个阈值，达到该阈值便会发送严重性为 “重大” 的消息。 *此参数仅适用于 HP-UX、AIX 和 Windows。*
NICBandwidthUtilMinorThreshold	可以为带宽利用率设置一个阈值，达到该阈值便会发送严重性为 “轻微” 的消息。 *此参数仅适用于 HP-UX、AIX 和 Windows。*
NICBandwidthUtilWarningThreshold	可以为带宽利用率设置一个阈值，达到该阈值便会发送严重性为 “警告” 的消息。 *此参数仅适用于 HP-UX、AIX 和 Windows。*
MessageGroup	输入一个合适的值，帮助识别此策略发送的消息。一旦违反了阈值，策略会在消息中附加此参数的值，然后再向管理控制台发送此消息。
Debug	将此值设为 **0** 可禁用跟踪消息，设为 **1** 可在控制台接收跟踪消息，设为 **2** 可在被管节点上的跟踪文件中记录跟踪消息。有关详细信息，请参阅跟踪。

内存瓶颈诊断策略

SI-MemoryBottleneckDiagnosis

此策略将监视物理内存利用率和瓶颈。当内存利用率较高而可用内存较少时，就会产生内存瓶颈，这将导致系统速度降低，从而影响总体性能。内存消耗较高会导致过多的页面调出以及较高的页面扫描速率、换出字节率和页面请求速度，最终导致系统速度降低。

此策略会首先检查是否存在违反内存瓶颈阈值的情况，若不存在则检查是否存在违反内存利用率阈值的情况。如果内存瓶颈和内存利用率的条件均未达到，则策略将检查是否存在可用页表。默认情况下，可用页表阈值包括 Microsoft 对 Windows 系统的建议值。如果同时违反了多个阈值，则表示利用率过高，策略将向 HPOM 控制台发送一条消息，其中含有相应的消息属性。消息中还会显示内存占用量排名前 10 位的进程的列表。

用于评估内存瓶颈条件的多个度量在不同平台上使用不同的阈值。要为特定平台启用正确的阈值，请在被管节点上部署阈值覆盖策略。

ThresholdOverrides_Linux 定义 Linux 平台上内存度量的相应阈值。

ThresholdOverrides_Windows 定义 Windows 平台上内存度量的相应阈值。

使用的度量	• GBL_MEM_UTIL • GBL_MEM_PAGEOUT_RATE • GBL_MEM_PAGEOUT_BYTE_RATE • GBL_MEM_PAGE_REQUEST_RATE* • GBL_MEM_CACHE_FLUSH_RATE * • GBL_MEM_PG_SCAN_RATE • GBL_MEM_PHYS * 仅当被管节点上安装了 HP performance Agent 时，才使用以上度量。
支持的平台	• Microsoft Windows • Red Hat Enterprise Linux • Suse Linux Enterprise Server • HP-UX • IBM AIX • Oracle Solaris
脚本参数	**描述**
MemPageOutRateCriticalThreshold	此阈值表示每秒钟从物理内存换出到磁盘的总页面数。将此阈值设置为将收到严重性为 “严重” 的消息的换出页面数。
MemPageOutRateMajorThreshold	将此阈值设置为将收到严重性为 “重大” 的消息的换出页面数。
MemPageOutRateMinorThreshold	将此阈值设置为将收到严重性为 “轻微” 的消息的换出页面数。
MemPageOutRateWarningThreshold	将此阈值设置为将收到严重性为 “警告” 的消息的换出页面数。
MemUtilCriticalThreshold	此阈值是节点上物理内存的利用率百分比 （0 到 100%）。将此阈值设置为将收到严重性为 “严重” 的消息的磁盘最小使用内存值。
MemUtilMajorThreshold	将此阈值设置为将收到严重性为 “重大” 的消息的节点最小使用内存值。

MemUtilMinorThreshold	将此阈值设置为将收到严重性为 “轻微”的消息的节点最小使用内存值。
MemUtilWarningThreshold	将此阈值设置为将收到严重性为 “警告”的消息的节点最小使用内存值。
MemPageScanRateCriticalThreshold	此阈值表示每秒钟从物理内存换入到磁盘的总页面数。将此阈值设置为将收到严重性为 “严重”的消息的换入页面数。
MemPageScanRateMajorThreshold	将此阈值设置为将收到严重性为 “重大”的消息的换入页面数。
MemPageScanRateMinorThreshold	将此阈值设置为将收到严重性为 “轻微”的消息的换入页面数。
MemPageScanRateWarningThreshold	将此阈值设置为将收到严重性为 “警告”的消息的换入页面数。
MemPageReqRateHighThreshold	将此阈值设置为每秒钟磁盘的页面请求数量。
MemCacheFlushRateHighThreshold	将此阈值设置为文件系统缓存将内容刷新到磁盘的速率。
FreeMemAvailCriticalThreshold	此阈值表示磁盘 / 文件系统上的可用物理内存 （以 MB 为单位）。将此阈值设置为将收到严重性为 “严重”的消息的磁盘最小可用内存值。
FreeMemAvailMajorThreshold	将此阈值设置为将收到严重性为 “重大”的消息的磁盘最小可用内存值。
FreeMemAvailMinorThreshold	将此阈值设置为将收到严重性为 “轻微”的消息的磁盘最小可用内存值。
FreeMemAvailWarningThreshold	将此阈值设置为将收到严重性为 “警告”的消息的磁盘最小可用内存值。
MemSwapoutByteRateCriticalThreshold	此阈值表示页面调出守护程序每秒扫描的页面数量（以 MB 为单位）。将此阈值设置为将收到严重性为 “严重”的消息的磁盘最小可用内存值。
MemSwapoutByteRateMajorThreshold	将此阈值设置为将收到严重性为 “重大”的消息的磁盘最小可用内存值。

MemSwapoutByteRateMinorThreshold	将此阈值设置为将收到严重性为 “轻微”的消息的磁盘最小可用内存值。
MemSwapoutByteRateWarningThreshold	将此阈值设置为将收到严重性为 “警告”的消息的磁盘最小可用内存值。
FreePageTableCriticalThreshold	此阈值表示系统上可用页表的数量。将此阈值设置为将收到严重性为 “严重”的消息的磁盘最小可用页表值。 *此参数仅适用于 Windows。*
FreePageTableMajorThreshold	将此阈值设置为将收到严重性为 “重大”的消息的磁盘最小可用页表值。 *此参数仅适用于 Windows。*
FreePageTableMinorThreshold	将此阈值设置为将收到严重性为 “轻微”的消息的磁盘最小可用页表值。 *此参数仅适用于 Windows。*
FreePageTableWarningThreshold	将此阈值设置为将收到严重性为 “警告”的消息的磁盘最小可用页表值。 *此参数仅适用于 Windows。*
MessageGroup	输入一个合适的值，帮助识别此策略发送的消息。一旦违反了阈值，策略会在消息中附加此参数的值，然后再向管理控制台发送此消息。
Debug	将此值设为 `0` 可禁用跟踪消息，设为 `1` 可在控制台接收跟踪消息，设为 `2` 可在被管节点上的跟踪文件中记录跟踪消息。有关详细信息，请参阅跟踪。

CPU 峰值检查策略

SI-CPUSpikeCheck

此策略是处理器性能监视策略。当 CPU 利用率出现明显升高后又立即下降时，即表明系统经历了一次 CPU 峰值。 SI-CPUSpikeCheck 策略将监视系统模式下每段 CPU 忙碌时间的 CPU 峰值和用户模式下每段 CPU 忙碌时间的峰值，以及每个 CPU 的总忙碌时间。

使用的度量	• BYCPU_CPU_USER_MODE_UTIL • BYCPU_CPU_SYS_MODE_UTIL • BYCPU_ID • BYCPU_CPU_TOTAL_UTIL
支持的平台	• Microsoft Windows • Red Hat Enterprise Linux • Suse Linux Enterprise Server • HP-UX • IBM AIX • Oracle Solaris

脚本参数	**描述**
CpuUtilCriticalThreshold	此阈值表示 CPU 忙碌时的总 CPU 时间，即总 CPU 利用时间。包括用户模式和系统模式下所用的总 CPU 时间。将此阈值设置为将收到严重性为 “严重” 的消息的总 CPU 利用时间最小值。
CpuUtilMajorThreshold	将此阈值设置为将收到严重性为 “重大” 的消息的总 CPU 利用时间最小值。
CpuUtilMinorThreshold	将此阈值设置为将收到严重性为 “轻微” 的消息的总 CPU 利用时间最小值。
CpuUtilWarningThreshold	将此阈值设置为将收到严重性为 “警告” 的消息的总 CPU 利用时间最小值。
CpuUtilUsermodeCriticalThreshold	此阈值是用户模式下 CPU 忙碌时的 CPU 时间百分比（0 到 100%）。将此阈值设置为将收到严重性为 “严重” 的消息的 CPU 忙碌时间最小值。
CpuUtilUsermodeMajorThreshold	将此阈值设置为将收到严重性为 “重大” 的消息的用户模式下 CPU 忙碌时间最小值。
CpuUtilUsermodeMinorThreshold	将此阈值设置为将收到严重性为 “轻微” 的消息的用户模式下 CPU 忙碌时间最小值。
CpuUtilUsermodeWarningThreshold	将此阈值设置为将收到严重性为 “警告” 的消息的用户模式下 CPU 忙碌时间最小值。

CpuUtilSysmodeCriticalThreshold	此阈值是系统模式下 CPU 忙碌时的 CPU 时间百分比（0 到 100%）。将此阈值设置为将收到严重性为 “严重”的消息的 CPU 忙碌时间最小值。
CpuUtilSysmodeMajorThreshold	将此阈值设置为将收到严重性为 “重大”的消息的系统模式下 CPU 忙碌时间最小值。
CpuUtilSysmodeMinorThreshold	将此阈值设置为将收到严重性为 “轻微”的消息的系统模式下 CPU 忙碌时间最小值。
CpuUtilSysmodeWarningThreshold	将此阈值设置为将收到严重性为 “警告”的消息的系统模式下 CPU 忙碌时间最小值。
InterruptRateCriticalThreshold	此阈值表示采样间隔期间 CPU 每秒设备中断的平均次数。将此阈值设置为将收到严重性为 “严重”的消息的 CPU 中断率最小值。
InterruptRateMajorThreshold	将此阈值设置为将收到严重性为 “重大”的消息的 CPU 中断率最小值。
InterruptRateMinorThreshold	将此阈值设置为将收到严重性为 “轻微”的消息的 CPU 中断率最小值。
InterruptRateWarningThreshold	将此阈值设置为将收到严重性为 “警告”的消息的 CPU 中断率最小值。
MessageGroup	传出消息的消息组。
Debug	将此值设为 `0` 可禁用跟踪消息，设为 `1` 可在控制台接收跟踪消息，设为 `2` 可在被管节点上的跟踪文件中记录跟踪消息。有关详细信息，请参阅跟踪。

CPU 瓶颈诊断策略

SI-CPUBottleneckDiagnosis

此策略将检测 CPU 利用率百分比、处理器队列长度、系统上的 CPU 总数以及操作系统数超过阈值之类的 CPU 瓶颈。

如果违反了 CPU 利用率阈值以及队列中等待 CPU 时间的进程数量阈值，则策略将向 HPOM 控制台发送一条消息，其中含有相应的消息属性。消息中还会显示 CPU 占用量排名前 10 位的进程的列表。

策略在 HPOM for Linux/HPOM for Solaris 上检测到的第一个 CPU 瓶颈实例将不会被报告。对于此后出现的瓶颈，策略将向控制台发送警报消息，显示 CPU 占用量排名前 10 位的进程的列表。

使用的度量	• GBL_CPU_TOTAL_UTIL • GBL_RUN_QUEUE • GBL_NUM_CPU • GBL_OSNAME • GBL_INTERRUPT_RATE • GBL_CSWITCH_RATE* * 仅当被管节点上安装了 HP Performance Agent 时，才使用本策略
支持的平台	• Microsoft Windows • Red Hat Enterprise Linux • Suse Linux Enterprise Server • HP-UX • IBM AIX • Oracle Solaris

脚本参数	**描述**
GlobalCpuUtilCriticalThreshold	此阈值表示汇总的 CPU 利用率。将此阈值设置为将收到严重性为 “严重” 的消息的汇总 CPU 利用率最小值。
GlobalCpuUtilMajorThreshold	将此阈值设置为将收到严重性为 “重大” 的消息的汇总 CPU 利用率最小值。
GlobalCpuUtilMinorThreshold	将此阈值设置为将收到严重性为 “轻微” 的消息的汇总 CPU 利用率最小值。
GlobalCpuUtilWarningThreshold	将此阈值设置为将收到严重性为 “警告” 的消息的汇总 CPU 利用率最小值。
RunQueueLengthCriticalThreshold	此阈值表示进程队列长度，即等待 CPU 时间的进程数量。将此阈值设置为将收到严重性为 “严重” 的消息的队列中进程数量最小值。
RunQueueLengthMajorThreshold	将此阈值设置为将收到严重性为 “重大” 的消息的队列中进程数量最小值。

RunQueueLengthMinorThreshold	将此阈值设置为将收到严重性为 “轻微” 的消息的队列中进程数量最小值。
RunQueueLengthWarningThreshold	将此阈值设置为将收到严重性为 “警告” 的消息的队列中进程数量最小值。
ContextSwitchRateCriticalThreshold	此阈值表示系统中上下文切换总数的比率。将此阈值设置为将收到严重性为 “严重” 的消息的上下文切换总数。
ContextSwitchRateMajorThreshold	将此阈值设置为将收到严重性为 “重大” 的消息的上下文切换总数。
ContextSwitchRateMinorThreshold	将此阈值设置为将收到严重性为 “轻微” 的消息的上下文切换总数。
ContextSwitchRateWarningThreshold	将此阈值设置为将收到严重性为 “警告” 的消息的上下文切换总数。
InterruptRateCriticalThreshold	此阈值表示采样间隔期间 CPU 每秒处理器中断的平均次数。将此阈值设置为将收到严重性为 “严重” 的消息的 CPU 中断率最小值。
InterruptRateMajorThreshold	将此阈值设置为将收到严重性为 “重大” 的消息的 CPU 中断率最小值。
InterruptRateMinorThreshold	将此阈值设置为将收到严重性为 “轻微” 的消息的 CPU 中断率最小值。
InterruptRateWarningThreshold	将此阈值设置为将收到严重性为 “警告” 的消息的 CPU 中断率最小值。
MessageGroup	输入一个合适的值，帮助识别此策略发送的消息。一旦违反了阈值，策略会在消息中附加此参数的值，然后再向管理控制台发送此消息。
Debug	将此值设为 **0** 可禁用跟踪消息，设为 **1** 可在控制台接收跟踪消息，设为 **2** 可在被管节点上的跟踪文件中记录跟踪消息。有关详细信息，请参阅跟踪。

每个磁盘 Utilization-AT 策略

SI-PerDiskUtilization-AT

此策略将监视被管节点上每个磁盘的利用率，将在每个间隔内单独处理每个磁盘实例。此策略使用自动确定阈值的方式，根据之前日期的磁盘利用率自动计算阈值。此策略要求在被管节点上运行 Performance Agent。

此策略依赖于历史数据。要得到精确结果，请在 Performance Agent 收集到一周的数据之后再部署策略。

使用的度量	BYDSK_UTIL
支持的平台	• Microsoft Windows • Red Hat Enterprise Linux • Suse Linux Enterprise Server • HP-UX • IBM AIX • Oracle Solaris
脚本参数	**描述**
MessageApplication	输入一个合适的值，帮助识别 SI-PerDiskUtilization-AT 策略向管理控制台发送的消息。
DataSource	将 HP 嵌入式性能组件 (EPC) 数据源名称显示为 SCOPE。
DataObject	将 HP 嵌入式性能组件 (EPC) 数据对象名称显示为 DISK。
DataMetric	将 HP 嵌入式性能组件 (EPC) 度量名称显示为 BYDSK_UTIL。
BaselinePeriod	输入要定义为基线期的时间段，例如 “3600 秒”。此时间段会随当前时间变化。最近的 3600 秒 （1 小时）会成为当前的基线期。
MinimumValue	显示度量所表示的磁盘利用率的最小值。
MaximumValue	显示度量所表示的磁盘利用率的最大值。
WarningDeviations	显示不在正常范围内的标准偏差数量，策略会向 HPOM 控制台发送严重性为 “警告” 的消息。为此参数设置一个合适的值。要禁用此参数，请将值设置为 *5*。
MinorDeviations	显示不在正常范围内的标准偏差数量，策略会向 HPOM 控制台发送严重性为 “轻微” 的消息。为此参数设置一个大于 WarningDeviations 指定值的合适值。要禁用此参数，请将值设置为 *5*。

MajorDeviations	显示不在正常范围内的标准偏差数量，策略会向 HPOM 控制台发送严重性为 “重大” 的消息。为此参数设置一个大于 MinorDeviations 指定值的合适值。要禁用此参数，请将值设置为 *5*。
WarningHighSeverity	显示当前数据符合或超过 *WarningDeviations* 中指定值的样本数据平均值时，发送到 HPOM 控制台的警报消息的严重性。要禁用此参数，请将值设置为 *none*。
MinorHighSeverity	显示当前数据符合或超过 *MinorDeviations* 中指定值的样本数据平均值时，发送到 HPOM 控制台的警报消息的严重性。要禁用此参数，请将值设置为 *none*。
MajorHighSeverity	显示当前数据符合或超过 *MajorDeviations* 中指定值的样本数据平均值时，发送到 HPOM 控制台的警报消息的严重性。要禁用此参数，请将值设置为 *none*。
WarningLowSeverity	显示当前数据符合或低于 *WarningDeviations* 中指定值的样本数据平均值时，发送到 HPOM 控制台的警报消息的严重性。要禁用此参数，请将值设置为 *none*。
MinorLowSeverity	显示当前数据符合或低于 *MinorDeviations* 中指定值的样本数据平均值时，发送到 HPOM 控制台的警报消息的严重性。要禁用此参数，请将值设置为 *none*。
MajorLowSeverity	显示当前数据符合或低于 *MajorDeviations* 中指定值的样本数据平均值时，发送到 HPOM 控制台的警报消息的严重性。要禁用此参数，请将值设置为 *none*。
InstanceSource	请勿编辑此参数值。
Debug	将此值设为 **0** 可禁用跟踪消息，设为 **1** 可在控制台接收跟踪消息，设为 **2** 可在被管节点上的跟踪文件中记录跟踪消息。有关详细信息，请参阅跟踪。
MessageGroup	传出消息的消息组。
DiskUtilCutOff	请设置一个值，低于此值便不再监视磁盘利用率。

网络接口传出字节速率策略

SI-PerNetifOutbyteBaseline-AT

此策略将监视给定间隔内网络接口的传出字节速率，会分别监视被管节点上每个网络接口的传出字节。此策略将在每个间隔内单独处理每个网络接口实例。此策略使用自动确定阈值的方式，根据之前日期的网络接口传出字节速率自动计算阈值。

此策略依赖于历史数据。要得到精确结果，请在 Performance Agent 收集到一周的数据之后再部署策略。该策略并不监视 vMA 计算机的物理 NIC。

使用的度量	BYNETIF_OUT_BYTE_RATE
支持的平台	• Microsoft Windows • Red Hat Enterprise Linux • Suse Linux Enterprise Server • HP-UX • IBM AIX • Oracle Solaris
脚本参数	**描述**
MessageApplication	输入一个合适的值，帮助识别 SI-PerNetifOutbyteBaseline-AT 策略向管理控制台发送的消息。
DataSource	将 HP 嵌入式性能组件 (EPC) 数据源名称显示为 CODA。
DataObject	将 HP 嵌入式性能组件 (EPC) 数据对象名称显示为 NETIF。
DataMetric	将 HP 嵌入式性能组件 (EPC) 度量名称显示为 BYNETIF_OUT_BYTE_RATE。
BaselinePeriod	输入要定义为基线期的时间段，例如 “3600 秒”。此时间段会随当前时间变化。最近的 3600 秒 （1 小时）会成为当前的基线期。
MinimumValue	显示度量所表示的网络接口传出字节速率的最小值。
MaximumValue	显示度量所表示的网络接口传出字节速率的最大值。
WarningDeviations	显示不在正常范围内的标准偏差数量，策略会向 HPOM 控制台发送严重性为 “警告” 的消息。为此参数设置一个合适的值。要禁用此参数，请将值设置为 *5*。
MinorDeviations	显示不在正常范围内的标准偏差数量，策略会向 HPOM 控制台发送严重性为 “轻微” 的消息。为此参数设置一个大于 WarningDeviations 指定值的合适值。要禁用此参数，请将值设置为 *5*。

MajorDeviations	显示不在正常范围内的标准偏差数量，策略会向 HPOM 控制台发送严重性为 “重大” 的消息。为此参数设置一个大于 MinorDeviations 指定值的合适值。要禁用此参数，请将值设置为 *5*。
WarningHighSeverity	显示当前数据符合或超过 *WarningDeviations* 中指定值的样本数据平均值时，发送到 HPOM 控制台的警报消息的严重性。要禁用此参数，请将值设置为 *none*。
MinorHighSeverity	显示当前数据符合或超过 *MinorDeviations* 中指定值的样本数据平均值时，发送到 HPOM 控制台的警报消息的严重性。要禁用此参数，请将值设置为 *none*。
MajorHighSeverity	显示当前数据符合或超过 *MajorDeviations* 中指定值的样本数据平均值时，发送到 HPOM 控制台的警报消息的严重性。要禁用此参数，请将值设置为 *none*。
WarningLowSeverity	显示当前数据符合或低于 *WarningDeviations* 中指定值的样本数据平均值时，发送到 HPOM 控制台的警报消息的严重性。要禁用此参数，请将值设置为 *none*。
MinorLowSeverity	显示当前数据符合或低于 *MinorDeviations* 中指定值的样本数据平均值时，发送到 HPOM 控制台的警报消息的严重性。要禁用此参数，请将值设置为 *none*。
MajorLowSeverity	显示当前数据符合或低于 *MajorDeviations* 中指定值的样本数据平均值时，发送到 HPOM 控制台的警报消息的严重性。要禁用此参数，请将值设置为 *none*。
Debug	将此值设为 **0** 可禁用跟踪消息，设为 **1** 可在控制台接收跟踪消息，设为 **2** 可在被管节点上的跟踪文件中记录跟踪消息。有关详细信息，请参阅跟踪。
MessageGroup	传出消息的消息组。
ByNetifOutByteCutOff	请设置一个值，低于此值便不再监视传出字节速率。

网络接口传入字节速率策略

SI-PerNetifInbyteBaseline-AT

此策略将监视给定间隔期间网络接口的传入字节速率，会分别监视被管节点上每个网络接口的传入字节。此策略将在每个间隔内单独处理每个网络接口实例。此策略使用自动确定阈值的方式，根据之前日期的网络接口传入字节速率自动计算阈值。

此策略依赖于历史数据。要得到精确结果，请在 Performance Agent 收集到一周的数据之后再部署策略。该策略并不监视 vMA 计算机的物理 NIC。

使用的度量	BYNETIF_IN_BYTE_RATE
支持的平台	• Microsoft Windows • Red Hat Enterprise Linux • Suse Linux Enterprise Server • HP-UX • IBM AIX • Oracle Solaris
脚本参数	**描述**
MessageApplication	输入一个合适的值，帮助识别策略向管理控制台发送的消息。
DataSource	将 HP 嵌入式性能组件 (EPC) 数据源名称显示为 CODA。
DataObject	将 HP 嵌入式性能组件 (EPC) 数据对象名称显示为 NETIF。
DataMetric	将 HP 嵌入式性能组件 (EPC) 度量名称显示为 BYNETIF_IN_BYTE_RATE。
BaselinePeriod	输入要定义为基线期的时间段，例如 “3600 秒”。此时间段会随当前时间变化。最近的 3600 秒 （1 小时）会成为当前的基线期。
MinimumValue	显示度量所表示的网络接口传入字节速率的最小值。
MaximumValue	显示度量所表示的网络接口传入字节速率的最大值。
WarningDeviations	显示不在正常范围内的标准偏差数量，策略会向 HPOM 控制台发送严重性为 “警告” 的消息。为此参数设置一个合适的值。要禁用此参数，请将值设置为 *5*。
MinorDeviations	显示不在正常范围内的标准偏差数量，策略会向 HPOM 控制台发送严重性为 “轻微” 的消息。为此参数设置一个大于 WarningDeviations 指定值的合适值。要禁用此参数，请将值设置为 *5*。

MajorDeviations	显示不在正常范围内的标准偏差数量，策略会向 HPOM 控制台发送严重性为 “重大” 的消息。为此参数设置一个大于 MinorDeviations 指定值的合适值。要禁用此参数，请将值设置为 *5*。
WarningHighSeverity	显示当前数据符合或超过 *WarningDeviations* 中指定值的样本数据平均值时，发送到 HPOM 控制台的警报消息的严重性。要禁用此参数，请将值设置为 *none*。
MinorHighSeverity	显示当前数据符合或超过 *MinorDeviations* 中指定值的样本数据平均值时，发送到 HPOM 控制台的警报消息的严重性。要禁用此参数，请将值设置为 *none*。
MajorHighSeverity	显示当前数据符合或超过 *MajorDeviations* 中指定值的样本数据平均值时，发送到 HPOM 控制台的警报消息的严重性。要禁用此参数，请将值设置为 *none*。
WarningLowSeverity	显示当前数据符合或低于 *WarningDeviations* 中指定值的样本数据平均值时，发送到 HPOM 控制台的警报消息的严重性。要禁用此参数，请将值设置为 *none*。
MinorLowSeverity	显示当前数据符合或低于 *MinorDeviations* 中指定值的样本数据平均值时，发送到 HPOM 控制台的警报消息的严重性。要禁用此参数，请将值设置为 *none*。
MajorLowSeverity	显示当前数据符合或低于 *MajorDeviations* 中指定值的样本数据平均值时，发送到 HPOM 控制台的警报消息的严重性。要禁用此参数，请将值设置为 *none*。
Debug	将此值设为 **0** 可禁用跟踪消息，设为 **1** 可在控制台接收跟踪消息，设为 **2** 可在被管节点上的跟踪文件中记录跟踪消息。有关详细信息，请参阅跟踪。
MessageGroup	传出消息的消息组。
ByNetifInByteCutOff	请设置一个值，低于此值便不再监视传入字节速率。

样本性能策略

系统基础结构 SPI 提供了样本性能策略，可用于监视系统上所运行进程的性能。您可以根据需要，将这些策略用作模版来创建副本和进行修改。

脚本参数	描述
ProcessName	输入要监视的进程的名称。
ProcessArguments	输入进程参数 （若有）。
MessageGroup	传出消息的消息组。
CPUUsageHighWaterMark 或 *MemoryUsageHighWaterMark*	为进程的 CPU 或内存利用率设置阈值，高于该值便会接收警报。
Debug	将此值设为 `0` 可禁用跟踪消息，设为 `1` 可在控制台接收跟踪消息，设为 `2` 可在被管节点上的跟踪文件中记录跟踪消息。有关详细信息，请参阅跟踪。

提供的样本策略有：

- **SI-JavaProcessMemoryUsageTracker** 策略将监视系统上运行的 Java 进程的内存利用率。此策略的默认策略组为：

  基础结构管理 → < *语言* > → 系统基础结构 → 性能 → 进程资源利用率监视样本

- **SI-JavaProcessCPUUsageTracker** 策略将监视系统上运行的 Java 进程的 CPU 利用率。此策略的默认策略组为：

  基础结构管理 → < *语言* > → 系统基础结构 → 性能 → 进程资源利用率监视样本

- **SI-MSWindowsSvchostCPUUsageTracker** 策略将监视系统上运行的 svchost 进程的 CPU 利用率。此策略的默认策略组为：

  基础结构管理 → < *语言* > → 系统基础结构 → 性能 → 进程资源利用率监视样本 → Windows

- **SI-MSWindowsSvchostMemoryUsageTracker** 策略将监视系统上运行的 svchost 进程的内存利用率。此策略的默认策略组为：

  基础结构管理 → < *语言* > → 系统基础结构 → 性能 → 进程资源利用率监视样本 → Windows

安全策略

假设有未经授权的用户通过输入用户名和密码的不同组合 （或部署一个自动脚本执行此操作）来尝试侵入您的系统，则这样的尝试会导致大量登录失败。要识别和预防这种风险，可以部署系统基础结构安全策略以定期检查系统的登录失败次数。例如，这些策略可收集登录失败数据，并在尝试次数过多时发出警报。

部署安全收集器策略之后，请确保策略至少运行 5 分钟以便收集所需数据。

Windows 的登录失败收集器策略

SI-MSWindowsFailedLoginsCollector

此策略是检查 Microsoft Windows 上登录尝试失败次数的计划任务策略。此策略会检查被管节点上是否存在未知用户名或密码不正确所造成的无效登录，并且每隔一定的时间就将失败登录的每个实例记录到嵌入式性能组件 (EPC) 的 GBL_NUM_FAILED_LOGINS 度量中。默认情况下，时间间隔为 1 小时。 EPC 中存储的记录信息可用于向控制台发送警报，也可用于生成有关一段时期内无效登录次数的报告。此策略的默认策略组为：

基础结构管理 → *< 语言 >* → 系统基础结构 → 安全性 → Windows

Windows 的最后登录收集器策略

SI-MSWindowsLastLogonsCollector

这是检查 Microsoft Windows 上所有活动本地用户帐户的登录详细信息的计划任务策略。并且每隔一定的时间就将用户登录的每个实例记录到嵌入式性能组件 (EPC) 的 SECONDS_SINCE_LASTLOGIN 度量中。默认情况下，时间间隔为 1 小时。 EPC 中存储的记录信息可用于向控制台发送警报，也可用于生成有关一段时期内用户登录次数的报告。此策略的默认策略组为：

基础结构管理 → *< 语言 >* → 系统基础结构 → 安全性 → Windows

Linux 的登录失败收集器策略

SI-UNIXFailedLoginsCollector

这是检查 RHEL 和 SLES Linux 系统、HP-UX、AIX 以及 Solaris 上登录尝试失败次数的计划任务策略。此策略会检查被管节点上是否存在未知用户名或密码不正确所造成的无效登录，并且每隔一定的时间就将失败登录的每个实例记录到嵌入式性能组件 (EPC) 的 GBL_NUM_FAILED_LOGINS 度量中。默认情况下，时间间隔为 1 小时。 EPC 中存储的记录信息可用于向控制台发送警报，也可用于生成有关一段时期内无效登录次数的报告。此策略的默认策略组为：

- **基础结构管理 → *< 语言 >* → 系统基础结构 → 安全性 → Linux**
- **基础结构管理 → *< 语言 >* → 系统基础结构 → 按供应商分组的策略 → *< 操作系统 >* - 快速入门**

  在这个实例中， ***< 操作系统 >*** 可以是 AIX、 HP-UX、 SLES、 RHEL 或 Solaris

确保 SI-UNIXFailedLoginsCollector 策略部署到 Solaris 节点后能够正常运行的先决条件有：

- Solaris 节点上的 `/etc/default/login` 文件必须进行以下设置：

  `SYSLOG=YES`

  `SYSLOG_FAILED_LOGINS=1`

- 在 `/etc/syslog.conf` 文件中对以下行取消注释，如果不存在则添加该行。

  `auth.notice ifdef(`LOGHOST', /var/log/authlog, @loghost)`

- 使用以下命令刷新 `syslogd`：

  `svcadm refresh system/system-log`

部署在其他节点上的 SI-UNIXFailedLoginsCollector 策略

节点	用于显示失败登录的命令 / 日志文件
Solaris	`/var/log/authlog`
Linux	`lastb` 命令
HP-UX	`lastb` 命令
AIX	`/etc/security/failedlogin` 日志

Linux 的最后登录收集器策略

SI-LinuxLastLogonsCollector

这是检查 RHEL 和 SLES Linux 系统上所有活动本地用户帐户的登录详细信息的计划任务策略。并且每隔一定的时间就将用户登录的每个实例记录到嵌入式性能组件 (EPC) 的 SECONDS_SINCE_LASTLOGIN 度量中。默认情况下，时间间隔为 1 小时。EPC 中存储的记录信息可用于向控制台发送警报，也可用于生成有关一段时期内用户登录次数的报告。此策略的默认策略组为：

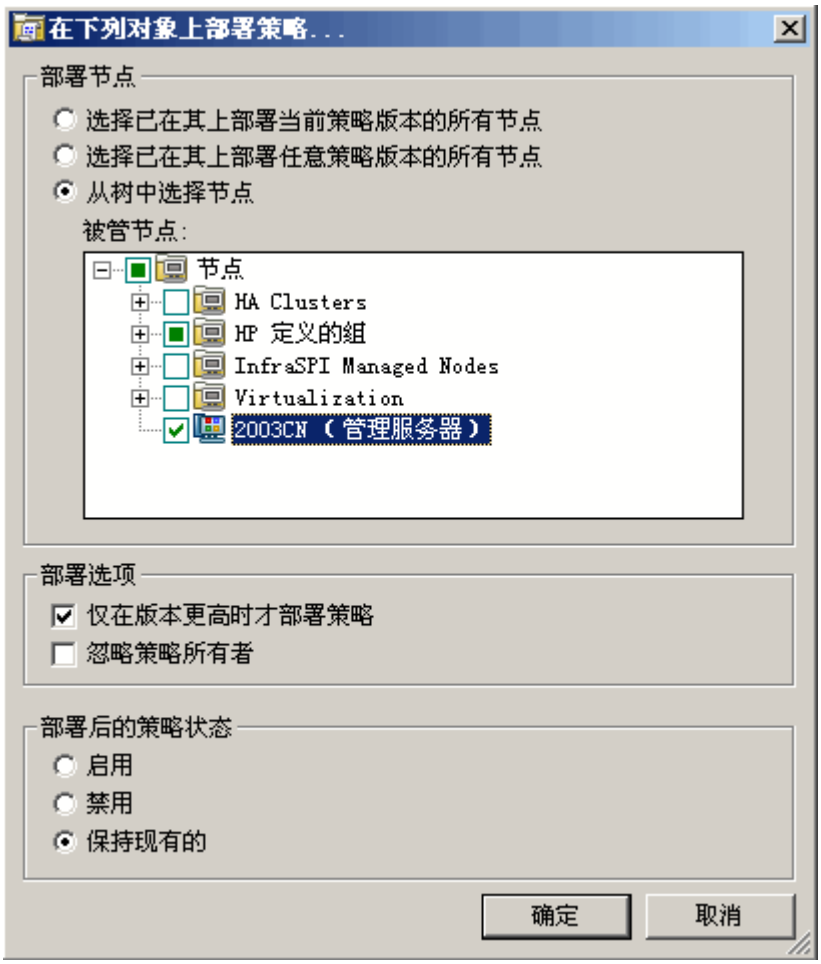
基础结构管理 → < *语言* > → 系统基础结构 → 安全性 → Linux

从 HPOM for Windows 管理服务器部署 SI SPI

要从管理服务器手动部署策略，请执行以下步骤：

1. 右键单击要部署的策略。
2. 从菜单中选择**所有任务**。
3. 选择**部署位置**。此时将打开 “在下列对象上部署策略” 对话框。
4. 选择**从树中选择节点**选项。从被管节点的列表中选择要部署策略的节点。
5. 单击**确定**。

图 3　　在下列对象上部署策略对话框



从 HPOM for UNIX 管理服务器部署 SI SPI 策略

在部署策略之前，请先确保节点已添加到管理服务器，并已安装了 HP Operations Agent 软件。有关如何将节点添加到管理服务器的详细信息，请参阅 《HP Operations Manager for Unix 联机帮助》。

要从 HPOM for UNIX （HP-UX、 Linux 或 Solaris）的管理服务器部署策略，请执行以下步骤：

任务 1：　分配策略或策略组

1　以管理员身份登录到 HPOM。此时将显示 HPOM 管理 UI。

2　单击 “对象库” 类别下的**策略库**。此时将打开 “策略库” 窗口。

3　在 “策略库” 窗口中，选择要分配到节点或节点组的策略或策略组。

4　从**选择操作**下拉框中选择**分配到节点 / 节点组 ...**，并单击 “提交”。

此时将打开选择窗口。

5　选择节点或节点组，然后单击**确定**。

所选策略将分配到这些节点。

任务 2： 部署策略

1 在 HPOM 管理 UI 中单击 “对象库” 类别下的**节点库**。此时将打开 “节点库” 窗口。

2 在 “节点库” 窗口中，选择要部署策略的节点或节点组。

3 从**选择操作**下拉框中选择**部署配置 ...**，并单击 “提交”。

此时将打开选择窗口。

4 选中**分发策略**复选框，并单击**确定**。

策略将在所选节点上部署。

系统基础结构 SPI 工具

使用工具可以管理被管节点上的服务，并查看为特定被管节点收集的数据列表。

要访问 HPOM for Windows 上的系统基础结构工具，请选择：

工具 → 系统基础结构

要访问 HPOM for UNIX/HPOM for Linux 的控制台或管理 UI 上的工具，请选择：

工具库 → 系统基础结构

用户最后登录工具

在被管节点上启动此工具后，将显示所有活动用户及其最后登录详细信息的列表。在启动工具之前，请确保已部署相应的最后登录收集器策略。有关最后登录收集器策略的详细信息，请参阅 Windows 的最后登录收集器策略和 Linux 的最后登录收集器策略。

要从 HPOM for Windows 管理服务器启动此工具，请执行以下步骤：

1 从控制台树的**工具**文件夹中选择**系统基础结构**文件夹。

2 在详细信息窗格中选择**用户最后登录**工具，并右键单击以打开快捷方式菜单。

3 选择**所有任务 → 启动工具 ...**，打开**选择启动此工具的位置**对话框。

对话框将显示可以启动所选工具的被管节点列表。

4 选中要应用工具的每个节点对应的复选框。选择**节点**文件夹将选中此文件夹包含的整个工具组。

5 单击**启动**。

工具状态对话框将打开，显示启动操作的结果。

您可以保存应用工具操作的结果。在**启动的工具**框中选择一行或多行，并单击**保存**。这样即会以文本格式保存输出。

要从 HPOM for UNIX 管理服务器启动工具，请执行以下步骤：

1 在 Java UI 中选择**工具 → 系统基础结构**。

2 右键单击 < *工具名称* > 工具，选择**启动自定义**。

此时将打开**启动工具 - 自定义向导**窗口。

3 在节点列表中选择要启动工具的节点。

4 在向导上，单击**获取选择项**。

节点便添加到 “选定节点” 列表。

5 单击**下一步**。

在 “指定运行工具所需的其他信息” 页面上，可以指定其他信息或将字段留空。

6 单击**完成**。

此时将显示工具输出。

5 系统基础结构 SPI 报告和图形

您可以将系统基础结构 SPI 与 HP Reporter 集成，以生成基于被管节点所收集的度量数据的报告。报告描述了系统资源。还可生成用于分析所收集度量数据的图形。要生成和查看由系统基础结构 SPI 所收集数据的报告和图形，请将 HPOM 与 HP Reporter 和 HP Performance Manager 一起使用。

系统基础结构 SPI 报告

报告全面描述了系统资源。您可以将系统基础结构 SPI 与 HP Reporter 集成，以生成基于被管节点所收集的度量数据的报告。

您可以从 HPOM for Windows 控制台访问系统基础结构 SPI 报告。要为系统基础结构 SPI 安装 HP Reporter 包，请参阅 《HP Operations 基础结构 SPI 安装指南》。

要从 HPOM for Windows 查看系统基础结构 SPI 的报告，请展开控制台树中的**报告 → 系统基础结构**。要显示某个报告，请选择所需的报告，单击右键，然后选择**显示报告**。

如果 HP Reporter 安装在 HPOM 管理服务器上，则可以直接在管理服务器上查看报告。

如果 HP Reporter 安装在与 HPOM 管理服务器连接的独立系统上，则可以在 HP Reporter 系统上查看报告。有关 HP Reporter 与 HPOM 集成的详细信息，请参阅 《HP Reporter 安装和特殊配置指南》。下图是报告示例。

图 4　　系统基础结构 SPI 报告的示例

Unused Logins

for Group Systems Infrastructure

This report was prepared: 8/11/2009, 3:00:53 AM

This report shows the login information for all the managed nodes.

aspint7-sol.ov.test

Login Name	Dates in Database	Last Login Date	Day Since Login (DD:HH:MM:SS)
root	08/09/2009 - 07/29/2009	8/4/2009 11:59:32PM	2:13:30:28

Never Logged in User List

halt
netdump
news
opc_op
shutdown
sync
vi-user

btovm555.ov.test

Login Name	Dates in Database	Last Login Date	Day Since Login (DD:HH:MM:SS)
vi-admin	08/08/2009 - 07/29/2009	8/5/2009 11:59:05PM	0:19:05:55

Never Logged in User List

halt
netdump
news
opc_op
shutdown
sync
vi-user

系统基础结构 SPI 提供了以下报告：

报告 / 报告标题	用途
系统最后登录	此报告将显示被管节点上最后一次登录的日期，以及从未登录的用户列表。这些信息按照日期和时间排序。可以使用此信息识别未使用或废弃的用户帐户。
系统登录失败	此报告将显示一个列表，列出被管节点上所有失败的登录尝试。可以使用此信息识别多次尝试登录到被管节点的未经授权用户。
系统可用性	此报告将显示系统的可用性信息。可以使用此信息了解数据库中某日期范围内 （不含非轮换运行时间、周末和节假日）的系统运行时间百分比和系统故障时间。
CPU 占用量排名靠前的进程	此报告将显示 CPU 占用量高的系统。可以使用此信息分析报告间隔内 CPU 周期占用量多的系统。
内存占用量排名靠前的进程	此报告将显示内存占用量高的系统。可以使用此信息分析报告间隔内内存占用量多的系统。

系统基础结构 SPI 图形

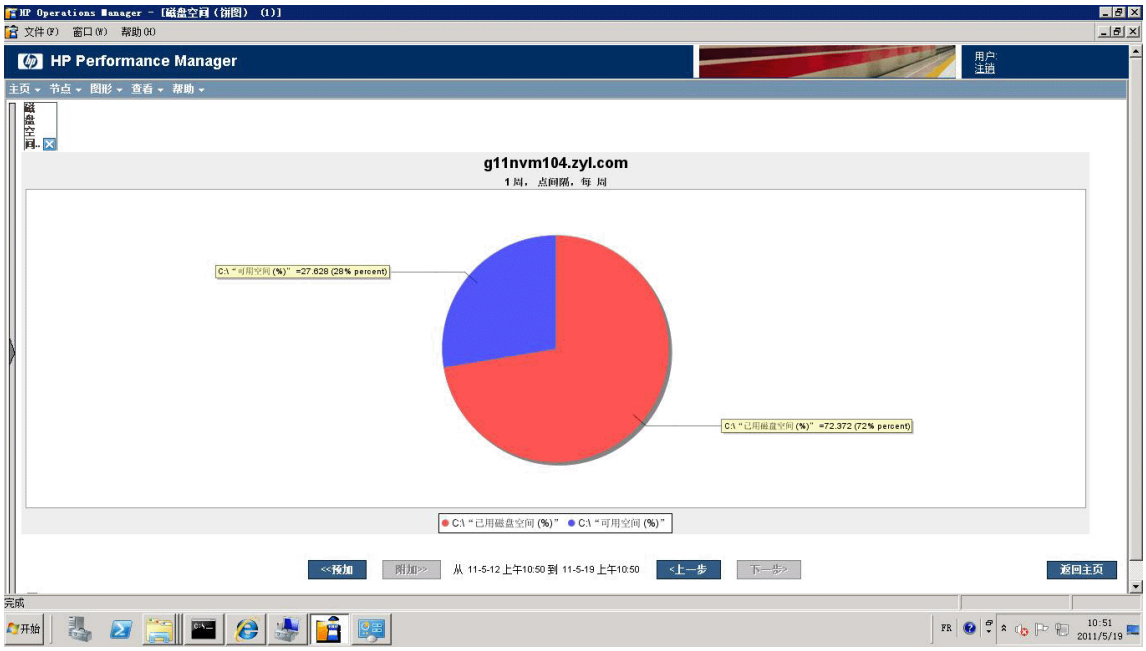
可以使用 HP Performance Manager 针对从被管节点收集的近似实时数据生成图形。如果 HPOM 管理服务器上已安装了 HP Performance Manager，则可以从 HPOM 控制台访问这些图形。

系统基础结构 SPI 提供一组预配置的图形，位于 HPOM 控制台树中的 “图形” 文件夹中。仅在 HPOM 管理服务器上安装 HP Performance Manager 后，才可以访问此 “图形” 文件夹。下图是图形示例。

要访问 HPOM for Windows 上的图形，请选择**图形** → **基础结构性能**。

要访问 HPOM for UNIX/Linux/Solaris 上的图形，请选择活动消息，打开 “消息属性” 窗口，并单击**操作**。在 “操作员启动的操作” 部分下面，单击**执行**。或者可以，右键单击活动消息，选择**执行 / 停止操作**，并单击**执行操作员启动的操作**。

图 5　　系统基础结构 SPI 图形的示例



系统基础结构 SPI 提供了以下图形：

图形	图形配置
磁盘	• 磁盘利用率 • 磁盘摘要 • 磁盘吞吐量 • 磁盘空间 • 磁盘空间 （饼图） • 磁盘详细信息
全局性能	• 全局历史记录 • 全局运行队列基线 • 全局详细信息 • 多个全局预测

图形	图形配置
CPU	• CPU 摘要 • CPU 利用率摘要 • 单个 CPU • CPU 比较 • CPU 计量 • CPU 详细信息 • 全局 CPU 预测 • 季节性 CPU 预测
网络	• 网络摘要 • 单个网络 • 网络接口详细信息
内存	• 内存摘要 • 物理内存利用率
配置	• 配置详细信息 • 系统配置
事务数	• 事务运行状况 • 事务历史记录 • 事务详细信息 • 事务响应预测
文件系统	• 文件系统详细信息
应用程序	• 应用程序 CPU 计量 • 应用程序 CPU 预测 • 应用程序历史记录 • 应用程序详细信息
进程	• 进程详细信息

6 疑难解答

本章介绍了 SI SPI 的基本疑难解答方案。

问题	硬件监视策略并不发送任何警报。
原因	-
解决方案	• 如果 snmpd 服务已停止，请启动。 **# /etc/init.d/snmpd start** • 确保 opctrapi 正在侦听端口号 162。

问题	客体虚拟机自动添加失败。
原因	InfraSPI-ServerSettings 策略中的 AutoAdd_Guests 参数默认情况下设置为 False。这是为了避免由于自动添加大量客体虚拟机而引起控制台 GUI 冻结。
解决方案	可以在 InfraSPI-ServerSettings 策略中设置参数 **AutoAdd_Guests=true**，然后重新部署策略。要访问该策略，选择**基础结构管理 → 设置和阈值 → 代理程序设置**。

问题	HPOM 控制台上显示以下警告 / 错误消息： An error occurred in the processing of the policy 'SI-PerDiskUtilization-AT'. Please check the following errors and take corrective actions. (OpC30-797) Initialization of collection source "DoNotRename" failed. (OpC30-724) Cannot find object 'DISK' in Coda object list. (OpC30-761) Searching for 'data source: SCOPE' in the DataSourceList failed. (OpC30-766))
原因	当将 SI-PerDiskUtilization-AT 策略部署到未安装 HP Performance Agent 的节点时，将发生此错误。 SI-PerDiskUtilization-AT 策略需使用 SCOPE 提供的度量进行计算，并需要 HP Performance Agent 才能正常运行。
解决方案	在被管节点上安装 HP Performance Agent，使策略正常运行。

问题	HPOM for UNIX 管理员 GUI 中修改的高级监视策略在部署到被管节点后无法运行。

原因	在 HPOM for UNIX 策略编辑器的 GUI 模式中编辑高级监视策略时，会将语法错误引入到 Perl 代码模块中。这会导致策略无法执行，将显示如下错误：
	`An error occurred in the processing of the policy 'SI-LinuxSshdProcessMonitor'. Please check the following errors and take corrective actions. (OpC30-797)`
	`Error during evaluation of threshold level "Processes - Fill Instance list" (OpC30-728)`
	`Execution of instance filter script failed. (OpC30-714)`
	`Perl Script execution failed: syntax error at PerlScript line 11, near "1`
	
	`#BEGIN_PROCESSES_LIST`
	`#ProcName=/usr/sbin/sshd`
	`#Params=`
	`#Params=`
	`#MonMode=>=`
	`#ProcNum=1`
	`#END_PROCESSES_LIST`
	`@ProcNames"`
	`Missing right curly or square bracket at PerlScript line 17, within string`
	`syntax error at PerlScript line 17, at EOF`
	`. (OpC30-750)`
	从 HPOM for UNIX 部署时，未编辑的高级监视策略 （度量阈值类型）运行正常。

解决方案	要编辑度量阈值策略中的设置，请使用 HPOM for UNIX 管理员 GUI 的“以原始模式编辑”功能更改策略内容。此功能需要您了解策略数据文件的语法。

问题	在 HPOM for UNIX （版本 9.00）操作员控制台中，操作员启动的命令未能启动系统基础结构 SPI 图形。
原因	-
解决方案	在 HPOM 服务器上运行以下命令： **`/opt/OV/contrib/OpC/OVPM/install_OVPM.sh <OMU 服务器名称>:8081`**

问题	发现过程和数据收集对非英文名称报错。
原因	尽管系统基础结构 SPI 可以在非英文 HP Operations Manager 上成功部署，但在系统中使用非英文名称会导致错误。这是因为 HP Operations Agent 中存储收集的 PERL API 无法识别非英文名称。
解决方案	确保群集和资源组均以英文命名。

问题	系统发现自动添加节点时出现警报消息。
原因	当自动为群集和虚拟环境添加节点时，系统发现策略会生成正常严重性的警报消息。对这些消息的确认需要一些时间，因为此策略的自动添加功能需要时间来填充节点库。
解决方案	禁用自动添加功能，这可通过更改 XPL 配置参数中的以下默认值来实现： • *AutoAdd_ClusterNode*：默认值为 True。将它改为 False。 • *AutoAdd_Cluster_RG_IP*：默认值为 True。将它改为 False。 • *AutoAdd_HypervisorNode*：默认值为 True。将它改为 False。 • *AutoAdd_Guests*：默认值为 False。将它改为 True。

We appreciate your feedback!

If an email client is configured on this system, by default an email window opens when you click on the bookmark “Comments”.

In case you do not have the email client configured, copy the information below to a web mail client, and send this email to **docfeedback@hp.com**

Product name:

Document title:

Version number:

Feedback: